7 FEHLER, DIE MAN BEI DER AUSWAHL EINER SSE-LÖSUNG VERMEIDEN SOLLTE

Aufbau der Security Service Edge (SSE) auf Grundlage von Zero Trust

Von:

Sanjit Ganguli
VP Transformation Strategy/Field CTO bei Zscaler

Nathan Howe
VP Emerging Technology & 5G bei Zscaler

Gesponsert von:

zscaler™

7 Fehler, die man bei der Auswahl einer SSE-Lösung vermeiden sollte

Inhaltsverzeichnis

SSE: Was ist das und was bedeutet es für IT-Architekten?

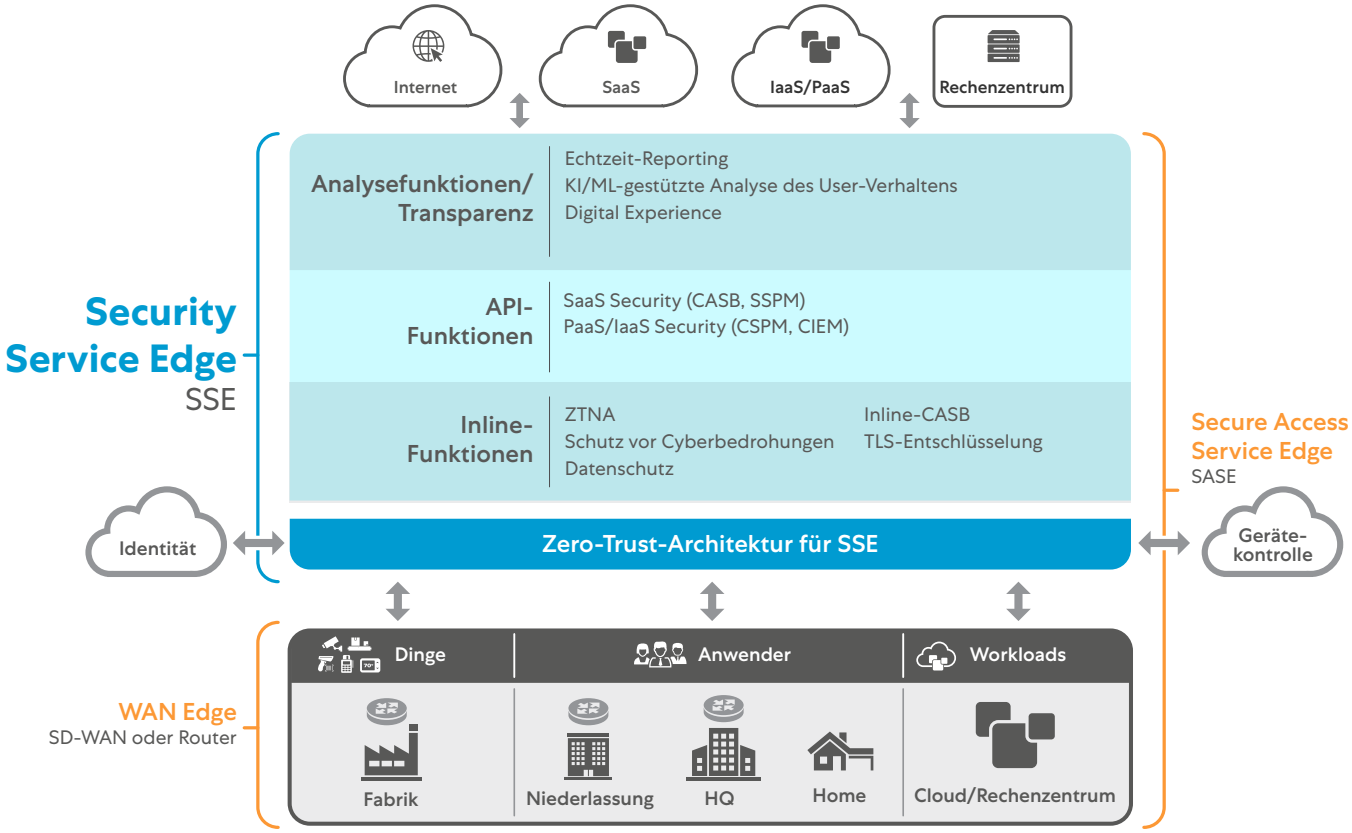

Abb. 1: Im SASE-Framework (Secure Access Service Edge) ist SSE als Komponente für die Durchsetzung von Richtlinien bzw. Richtlinienentscheidungen inbegriffen. SASE erfordert den Einsatz dedizierter Konnektivitätslösungen zwischen der Entität, von der die Anfrage ausgeht, und der Security Edge, wo die Unternehmensrichtlinien durchgesetzt werden.

Security Service Edge (SSE) wurde von Gartner als Komponente definiert, die im Rahmen des SASE-Frameworks (Secure Access Service Edge) für die Durchsetzung von Richtlinien bzw. Richtlinienentscheidungen zuständig ist. SSE ermöglicht die Konsolidierung und Vereinfachung von Cloud-basierter Sicherheit und Konnektivität.

Eine möglichst unkomplizierte IT-Architektur bringt eindeutige Vorteile – das gilt erst recht, wenn sie zum Abbau technischer Schulden und zur Beschleunigung von Transaktionen und Betriebsabläufen beiträgt. Im Umkehrschluss wird Sicherheit jedoch in vielen Unternehmen als lästiges Hindernis wahrgenommen, das Engpässe verursacht, die Agilität einschränkt und dem Geschäftserfolg im Weg steht. SSE ist ein überzeugendes Argument zur Entkräftung solcher Vorurteile. Im Rahmen einer SSE-Umgebung fungieren Sicherheitslösungen ganz im Gegenteil als Treiber des Geschäftserfolgs, indem sie zuverlässigen Schutz gewährleisten und dem Unternehmen die komplette Kontrolle geben.

Um kurz auf die Hintergründe einzugehen: Das SASE-Framework wurde 2019 konzipiert und soll Unternehmen bei der Digitalisierung – sprich: der Umstellung auf Cloud und Mobilität – unterstützen. SASE kombiniert Netzwerkzugang und Sicherheit und stellt beides an der (geografisch distributierten) Cloud-Edge bereit **(siehe Abb. 1)**. Dadurch gewährleistet das Framework, dass Sicherheit nicht mehr zentral bereitgestellt werden muss, und ermöglicht sichere Verbindungen von und zu jedem beliebigen Standort.

Ein Handy lässt sich mit ganz unterschiedlichen Mobilfunk- und drahtlosen Netzwerken verbinden. Obwohl es keine dedizierte Netzwerk-Routing-Lösung gibt, muss der Traffic zwischen der Entität, von der die Anfrage ausgeht, und dem Verbindungsziel trotzdem durch Sicherheitskontrollen geschützt werden. Analog sollte es auch bei der Absicherung des Unternehmens-Traffics keine Rolle spielen, zu welcher Edge, welchem Netzwerk oder welchem Standort die Verbindung hergestellt wird. Mit SSE wird das möglich.

Cybersicherheitsanbieter sind sehr schnell auf den SASE-Zug aufgesprungen. Teilweise wurde der Begriff von Marketing-Profis zweckentfremdet, die ihr Produkt als SASE-konform anpriesen, nur weil es einen Netzwerkzugang bereitstellt.

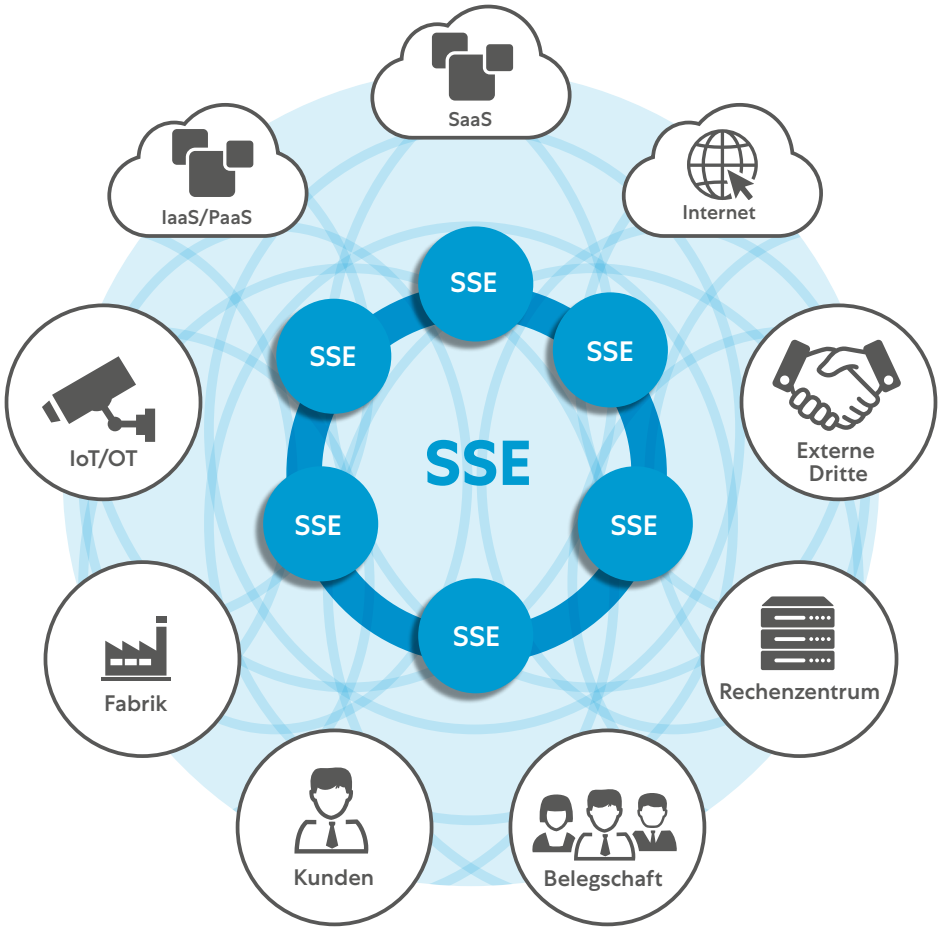

Abb. 2: Mit SSE können Unternehmen endlich auf Firewalls und VPNs verzichten. Basierend auf Identitätsprüfungen und Unternehmensrichtlinien wird der Direktzugriff zwischen zwei Entitäten an der Edge vermittelt. Damit lässt sich Sicherheit ohne Performance-Beeinträchtigungen in unmittelbarer User-Nähe bereitstellen.

SSE ist eine Sammelbezeichnung für die Suite von SASE-Services, die zum Schutz des Unternehmens-Traffics eingesetzt werden. Eine SSE-Lösung gewährleistet, dass befugte User (bzw. Workloads) Zugriff auf die jeweils benötigten Anwendungen und Services erhalten – dabei kann es sich um Workloads in IaaS- oder PaaS-Umgebungen, SaaS-Anwendungen oder auch um Internet-Services wie LinkedIn oder YouTube handeln. Die Zugriffsberechtigung muss aufgrund von ZTA-Kontrollen (Zero Trust Access) gewährt werden (siehe dazu die ausführlichen Erläuterungen im Abschnitt zum **2. häufigen Fehler**).

Um diese hochgesteckten Ziele zu erfüllen, müssen SSE-Anbieter eine globale, hochverfügbare, skalierbare und netzwerkunabhängige Lösung bereitstellen, die konsistente Richtlinien, Zero-Trust-Zugriff und reibungslose Anwendererfahrungen gewährleistet.

Nur so kann standortunabhängig ein gleichermaßen hohes Schutzniveau bei zuverlässiger Verfügbarkeit garantiert werden **(siehe Abb. 2).** Im Unterschied zum SASE-Framework legt SSE keine Verbindungs- oder Zugriffsmethode fest. Stattdessen wird von der Prämisse ausgegangen, dass der Zugriff auf genehmigte Services über ein beliebiges Netzwerk erfolgen kann und durch entsprechende Kontrollen abgesichert werden muss.

Hinter dem SASE-Framework steht der Gedanke, Konnektivität und Sicherheit miteinander zu verbinden. Damit das in der Unternehmenspraxis funktionieren kann, muss der gesamte Vorgang für die Mitarbeiter als Enduser transparent sein. Voraussetzung dafür sind Direktverbindungen – zwischen User und Anwendung, Anwendung-zu-Anwendung, Workload-zu-Workload, X-zu-Y. User dürfen niemals das Gefühl haben, dass sie sich erst mit dem Netzwerk verbinden müssen, bevor sie arbeiten können. Stattdessen sollen sie mit der Mentalität herangehen, dass sie direkt ihre Arbeit erledigen können.

In Unternehmensumgebungen, die auf einer Legacy-Infrastruktur basieren, lässt sich diese reibungslose Integration zwischen Netzwerkzugriff und Sicherheit nicht realisieren. Dieses veraltete Modell beruhte auf einer zentralen Bereitstellung der Sicherheit – somit musste der gesamte Datenverkehr zunächst über das Unternehmensnetzwerk mit dem physischen Standort der hardwarebasierten Sicherheitskontrollen verbunden (und durch die Kontrollen geroutet) werden. Dies galt unabhängig vom Standort (also auch für Remote-User bzw. Zweigstellen), der Entität, von der die Anfrage ausgeht (User, Anwendung oder Workload), und dem Verbindungsziel (Internet, Cloud, Rechenzentrum).

Der Geschäftsnutzen einer SSE-basierten digitalen Transformation

Die Umstellung auf SSE macht in vielen Fällen eine umfangreiche digitale Unternehmenstransformation erforderlich. Unternehmen, die sich aktiv auf diesen Wandel einlassen, profitieren jedoch oft von handfesten Vorteilen:

Kontrolle:

SSE beginnt mit Zero. SSE unterzieht sämtliche User, Geräte, Workloads, Netzwerke und Edges einer Identitätsprüfung. Zugriffsberechtigungen werden ausschließlich identitätsbasiert und kontextbezogen gewährleistet, wobei die Kontextdaten aus Verhaltensanalysen bezogen werden. Damit behält das Unternehmen jederzeit die komplette Kontrolle darüber, welcher User bzw. welche Entität auf einzelne Services innerhalb seiner IT-Infrastruktur zugreifen kann.

Direktverbindungen:

SSE-Lösungen setzen Richtlinien inline durch, also zwischen der Entität, von der die Anfrage ausgeht, und dem Verbindungsziel. Zugriffsberechtigungen werden niemals auf Netzwerkebene, sondern immer nur für einzelne Anwendungen gewährt.

Unternehmensspezifische Sicherheitsrichtlinien:

Richtlinien, die festlegen, welche Entitäten auf welche Services zugreifen dürfen, basieren auf dem Prinzip der minimalen Rechtevergabe. User, Geräte, Workloads usw. erhalten ausschließlich im Rahmen dieser Berechtigungen Zugriff auf Services. Andere Verbindungen sind nicht verfügbar, und der Zugriff auf alle anderen Services wird blockiert.

Global Enforcement:

Die SSE-Lösung muss Richtlinien global durchsetzen, sodass für alle Entitäten auf allen Verbindungswegen identische Kontrollen gelten. Diese Kontrollen basieren auf Kontextdaten, die aus Richtlinien, Analyse-Engines und anderen Tools (Threat Monitoring, Deception Technology usw.) gewonnen werden. Diese Durchsetzungsmechanismen müssen sich entsprechend den jeweiligen Anforderungen des Unternehmens skalieren lassen.

Ganzheitlicher Funktionsumfang:

SSE gewährleistet auch bei hohen Datenvolumen eine gründliche Inline-Überprüfung des gesamten Traffics. SSE unterstützt Unternehmen bei der Abwehr komplexer Bedrohungen, schützt geschäftskritische Ressourcen (nicht nur) in der Cloud, verhindert Datenverluste und stellt Inline-Kontrollen bereit. Bei Bedarf sollte die Lösung die Kontrolle über Inhalte ermöglichen, die in Cloud-Services gespeichert sind.

Minimale Angriffsfläche:

SSE verhindert unerwünschte Zugriffe auf und Exposition von Unternehmensressourcen, indem die Angriffsfläche minimiert wird. Ressourcen, die nicht zugänglich sind, können auch nicht angegriffen werden.

Standortunabhängige Konnektivität:

SSE stellt diese Konnektivität für sämtliche Unternehmensbereiche und für Verbindungen von beliebigen Standorten bereit. SSE schützt und verbindet eine flexible User-Basis und gewährleistet, dass Workloads und Geräte auch bei Verlagerung oder anderen Veränderungen unter der Kontrolle des Unternehmens bleiben.

Durch die zuverlässige Absicherung sämtlicher Geschäftsprozesse kann SSE als Katalysator für den positiven Wandel wirken. Zwischen den SSE-Lösungen verschiedener Anbieter bestehen jedoch deutliche Qualitätsunterschiede. Im Vorfeld einer geplanten Umstellung auf SSE sollten IT-Verantwortliche die unterschiedlichen Angebote gründlich evaluieren und eine Lösung wählen, mit der das Unternehmen Sicherheit ohne unnötige Komplikationen gewährleisten kann.

Bei der Auswahl eines geeigneten SSE-Anbieters, dessen Aufgabe es ist, das Unternehmen zuverlässig durch die digitale Transformation zu führen, ist Vorsicht und gründliche Recherche geboten. Im Folgenden wird auf sieben häufige Fehler eingegangen, die IT-Führungskräfte bei der Entscheidung für die richtige Kombination aus Services, Architektur und Funktionen unbedingt vermeiden sollten, um den Geschäftsnutzen von SSE in vollem Umfang zu realisieren. Diese Umstellung beinhaltet auch eine Abkehr von altbewährten Methoden, die der erfolgreichen Transformation im Wege stehen. Dazu zählt etwa das Festhalten an Netzwerken oder die Vergabe pauschaler Zugriffsberechtigungen auf Services.

1. Fehler:
Die ausgewählte SSE-Lösung hat keine nachgewiesene Erfolgsbilanz beim Betrieb einer globalen Cloud-Plattform mit skalierbarer Performance und Verfügbarkeit

2. Fehler:
Die ausgewählte SSE-Lösung basiert nicht auf einer Zero-Trust-Architektur

3. Fehler:
Die ausgewählte SSE-Lösung stellt vermeintlich Advanced Threat Protection und erweiterte DLP bereit, kann aber bei hohen Datenvolumen nicht den gesamten verschlüsselten Traffic überprüfen

4. Fehler:
Die ausgewählte SSE-Lösung ist eine Allzwecklösung ohne flexible, skalierbare und vielseitige Bereitstellungs- und Verwaltungsoptionen

5. Fehler:
Auswahl einer SSE-Lösung, die eine mittelmäßige Anwendererfahrung bietet, da die Anwendungskonnektivität nicht optimiert wird oder Beeinträchtigungen der Anwendererfahrung nicht diagnostiziert werden

6. Fehler:
Die ausgewählte SSE-Lösung lässt sich nur eingeschränkt mit Drittanbieterlösungen integrieren und orchestrieren

7. Fehler:
Der Geschäftsnutzen der ausgewählten SSE-Lösung lässt sich in einer Testumgebung schwer nachweisen

An wen richtet sich dieser Ratgeber?

Bei der Umstellung auf SSE geht es um mehr als nur die Transformation der Sicherheit. Entsprechend betrifft sie neben **Sicherheitsarchitekten** einen weiteren Personenkreis. Die Handlungsempfehlungen in diesem E-Book richten sich sowohl an **Sicherheitsarchitekten** als auch an **Netzwerkarchitekten**, **Systemarchitekten**, **Cloud-Architekten** und **Anwendungsarchitekten**.

#1 Fehler

Die ausgewählte SSE-Lösung hat keine nachgewiesene Erfolgsbilanz beim Betrieb einer globalen Cloud-Plattform mit skalierbarer Performance und Verfügbarkeit

Stattdessen empfiehlt sich die Auswahl einer Lösung, die folgende Voraussetzungen erfüllt:

- Sie bietet vielseitige, globale Edges zur Richtliniendurchsetzung bei Public Service Edges mit durch SLAs gesicherter Leistung, Verfügbarkeit, Durchsatz und Funktionalität. Richtlinien werden direkt an den Standorten der Kunden durchgesetzt.
- Es handelt sich um eine Cloud-native SSE-Lösung, die durch erstklassige Leistung in den Bereichen Ausfallsicherheit, Infrastruktur, geografische Reichweite, Funktionsumfang und User Experience überzeugt. SSE-Services werden nicht über einen Managed-Cloud- oder Rechenzentrumsanbieter am Zielort, sondern inline in Carrier-neutralen Rechenzentren bereitgestellt.
- Skalierbarkeit, Wachstumspotenzial und Bereitstellungsmöglichkeiten sind durch Kundenreferenzen, vorliegende Berichte, unabhängige Zertifizierungen und externe Open-Source-Datenspeicher (https://www.peeringdb.com/org/12297) nachgewiesen.

Umsetzung durch kompetente SSE-Anbieter:

Bei der Einrichtung und Verwaltung einer SSE-Plattform, die Milliarden von Transaktionen verarbeiten soll, kommt es keineswegs nur auf die Rechenkapazität an. **Die SSE-Lösung soll die Sicherheit, Konnektivität und Produktivität des Unternehmens gewährleisten.** Entsprechend muss sie in der Lage sein, sämtliche im Funktionsumfang inbegriffenen Services im gesamten Unternehmen einheitlich und zeitnah bereitzustellen.

Eine geeignete SSE-Lösung stellt die im Funktionsumfang inbegriffenen Services über eine global distribuierte Plattform bereit. Für die Bereitstellung hat sich eine Proxy-basierte Architektur als effektivstes Modell erwiesen. Ein Proxy-basierter Service für die Absicherung des Anwendungszugriffs mit SSE ist nicht im Netzwerk verankert und ermöglicht die Inline-Überprüfung des gesamten Traffics sowie weitere Analysefunktionen direkt über die Plattform **(siehe den Abschnitt zum 3. Fehler)**.

Der Aufbau einer echten Proxy-Architektur ist mit beträchtlichem F&E-Aufwand verbunden und erfordert jahrelange Weiterentwicklung, um den Skalierungsanforderungen zukunftsfähiger Unternehmen gerecht zu werden. Ein geeigneter SSE-Anbieter kann anhand zahlreicher Fallbeispiele nachweisen, dass seine Proxy-Architektur für große Installationen skalierbar ist.

Dieser Service muss über einheitliche Policy-Edges bereitgestellt werden, damit sämtliche Datenübertragungsfunktionen des Unternehmens geschützt sind. Dabei kommt es nicht nur auf die Anzahl der Nodes an, sondern eher darauf, wie viele Standorte die vom Kunden benötigten Services bereitstellen. Insbesondere ist darauf zu achten, dass die Bereitstellung an allen Standorten durch SLAs garantiert wird. Der SSE-Anbieter darf öffentliche Präsenzpunkte nur in Regionen bereitstellen, in denen er die Verfügbarkeit der Services durch einen SLA garantieren kann. Ist dies – aufgrund unzureichender Peering-Vereinbarungen oder aus anderen Gründen – nicht möglich, sollten auch keine Präsenzpunkte angeboten werden.

Die Umstellung auf SSE bedeutet auch, dass das Unternehmen seine Sicherheit, Konnektivität und Kontrolle konsolidiert und stärkt und die Verantwortung mit einem vertrauenswürdigen Anbieter teilt. Durch diese gemeinsame Verantwortung lässt sich die Bereitstellung von Schutzmechanismen und Konnektivität für alle User, Workloads, Services und Zweigstellen vereinfachen. Der SSE-Anbieter muss dabei die Einhaltung einer Reihe feststehender SLAs nachweisen, um das Funktionieren des Unternehmens und die Bereitstellung der Schutzmechanismen zu gewährleisten.

Für die Verbindung des Unternehmensservice zu einer Zielfunktion ist ein effektiver Pfad erforderlich. Dies lässt sich nur über eine SSE-Lösung mit hochgradig effektivem Peering in Carrier-neutralen Rechenzentren gewährleisten. Entsprechend müssen Kontrollen inline zwischen Ausgangspunkt und Verbindungsziel angewendet werden, und zwar unabhängig von deren jeweiligen Standorten.

Lösungen, die den Sicherheitsservice in zentralen Computing-Clouds hosten (häufig innerhalb eines Hyperscalers) und über Ingress-Gateways verfügen wie in Abb. 3 dargestellt (auch als Onramp-Services bezeichnet), haben zwar geografisch distribuierte Eintrittspunkte, jedoch werden die Kontrolle und Anwendung von Richtlinien zentral verarbeitet, was zu unerwünschten Latenzen und Beeinträchtigungen der User Experience führt.

SSE-Anbieter müssen nachweislich über eine komplette, umfangreiche und skalierbare Cloud-Plattform verfügen. Neben SLAs sollte der SSE-Anbieter auch Nachweise für die Skalierbarkeit, Stabilität, Verfügbarkeit, geografisch distribuierte Bereitstellung usw. erbringen. Zur Validierung dieser Nachweise empfiehlt es sich, öffentlich zugängliche historische Daten einzusehen und Erfahrungsberichte von Kunden einzuholen.

Einheitliche Richtliniendurchsetzung an der Edge

Die Durchsetzung von Richtlinien muss direkt an den Service Edges des SSE-Anbieters erfolgen: Diese dürfen nicht lediglich zur Umleitung des Traffics an die zentrale Infrastruktur innerhalb eines größeren Cloud-basierten Netzwerks dienen. Solche Onramp-Services verfehlen den Zweck der Bereitstellung leistungsstarker Services mit geringer Latenz.

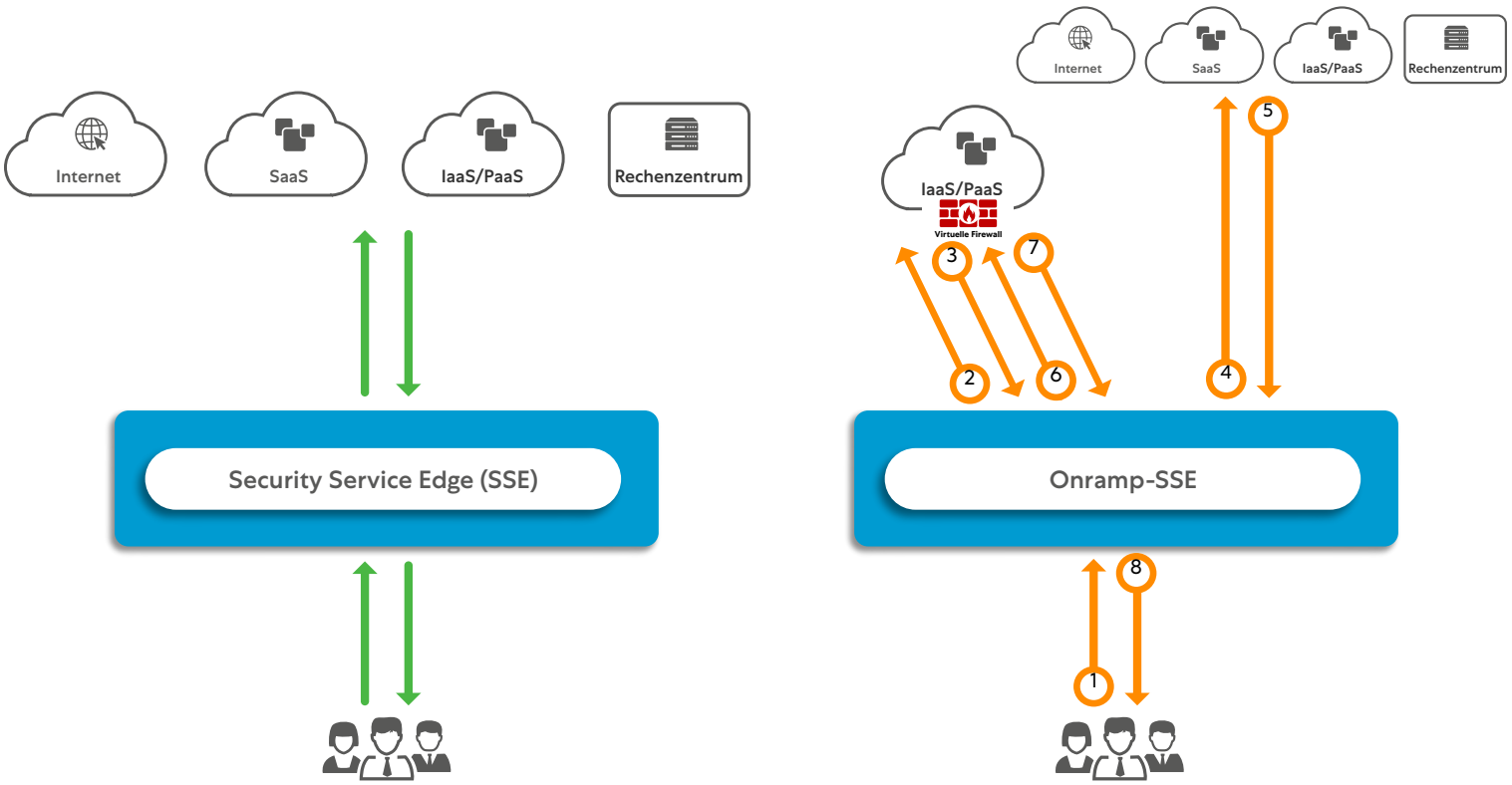

Abb. 3: Bei Inline-SSE-Services (links) werden Sicherheitskontrollen direkt auf den Traffic angewendet. Onramp-Sicherheitskontrollen (rechts) stellen zwar Ingress-Gateways in der Edge bereit, leiten den Traffic jedoch an eine zentrale in einer Computing-Cloud gehostete Kontrollstelle weiter, was zu zusätzlichen Latenzen und Ineffizienz führt und die User Experience beeinträchtigt.

Die SSE-Lösung muss folgende Designkriterien erfüllen:

- Edges müssen an wichtigen Peering-Standorten in Carrier-neutralen Rechenzentren gehostet werden, um minimale Latenzzeiten zwischen Ausgangspunkt und Verbindungsziel zu gewährleisten. Bei der Bewertung des SSE-Anbieters sollten Daten aus öffentlichen Quellen wie PeeringDB und Partner-Implementierungen **(weitere Informationen zu Partner-Integrationen im Abschnitt zum 6. Fehler)** herangezogen werden.
- Die Lösung muss durch einen robusten SLA gesichert werden. Dadurch wird die Stabilität der geschäftskritischen Funktionen gewährleistet und versichert, dass der SSE-Anbieter in den jeweiligen Regionen tätig ist, für die die SLAs gelten.
- An Standorten, an denen aufgrund lokaler Bedingungen differenzierte Bereitstellungsoptionen erforderlich sind – z. B. On-Premise oder innerhalb eines Edge-Computing-Node –, muss eine private Bereitstellung auf kundenspezifischer Basis möglich sein **(weitere Informationen im Abschnitt zum 4. Fehler)**.
- Die Fähigkeit zur Durchsatzsteigerung muss anhand einer positiven Verlaufskurve nachgewiesen werden.
- Edges müssen fehlertolerant sein und im Aktiv/Aktiv-Modus bereitgestellt werden, um Verfügbarkeit und Redundanz zu gewährleisten. (Public Service Edges werden vom Anbieter überwacht und gewartet, um kontinuierliche Verfügbarkeit sicherzustellen.)
- Datenschutz gewährleisten, damit Kunden-Traffic nicht an andere Komponenten innerhalb der Infrastruktur weitergegeben wird und keine Daten auf der Festplatte gespeichert werden
- Einheitliche Kontrollen für Unternehmensressourcen an allen Edges bereitstellen – ohne Routing oder Weiterleiten zwischen Remote-Edges und zentralen Standorten
- Umfassende globale Schutzmaßnahmen durchsetzen, um alle Unternehmensservices zu schützen, sobald eine Bedrohung erkannt wird

⚠ Worauf sollte man achten?

- Public Edges, die keine Durchsetzung bieten. Stattdessen wird Traffic in größere Rechenzentren mit Computing-Ressourcen weitergeleitet.
- Behauptungen, dass Hunderte von Public Edges vorhanden wären, ohne Informationen zu Funktionsumfang und Kapazität jedes Edges
- Edges ohne SLAs für Verfügbarkeit, Durchsatz und Resilienz
- Edge-Services ohne Mandantenfähigkeit und Routing/Weiterleiten von Traffic an andere Standorte
- SSE-Services, die nicht nachweislich von Großkunden eingesetzt wurden
- Services ohne öffentlich zugängliche Informationen zu Stabilität und Verfügbarkeit des Services

Ergebnisse:

Es ist entscheidend, eine SSE-Lösung auszuwählen, die für das heutige Unternehmen aber auch hinsichtlich zukünftiger Ziele skalierbar ist. Skalierbarkeit ist nicht einfach nur ein Prozess zur Größenveränderung. Vor allem sollte Skalierbarkeit bedeuten, dass die Anforderungen eines Unternehmens erfüllt werden können, ohne die Funktionalität, Stabilität und Sicherheit des Unternehmens zu beeinträchtigen. Deshalb sollte man bei der Auswahl einer SSE-Lösung folgende Kriterien beachten:

- Die Lösung wird nachweislich weltweit von unterschiedlichen Kunden eingesetzt.
- Sie beinhaltet schriftlich festgehaltene und validierte SLAs, die bei Verlust oder Verschlechterung der SSE-Services greifen.
- Sie wurde von einer Vielzahl von Kunden mit ähnlicher Unternehmensgröße und -komplexität implementiert.
- Mithilfe öffentlich zugänglicher Tools (z. B. PeeringDB) kann man Informationen zu allen PoPs abrufen.
- Alle kritischen Funktionen werden an allen Standorten ohne Hairpinning von Traffic zur Verfügung gestellt.
- Sie bietet Inline-Schutz zwischen Quelle und Ziel.
- Sie ist für die Infrastruktur sowie betriebliche und funktionale Resilienz konzipiert.
- Sie kann in verschiedenen Formen an verschiedenen Standorten verwendet werden.

#2 Fehler

Auswahl einer SSE-Lösung, die nicht auf einer Zero-Trust-Architektur basiert

Stattdessen sollte man bei der Auswahl einer SSE-Lösung folgende Kriterien beachten:

- Eine Lösung, die unabhängig vom Standort/Netzwerk Zugriffsberechtigungen nur aufgrund einer kontextbezogenen Identitätsprüfung gewährt. Dieses Prinzip der minimalen Rechtevergabe sollte nicht nur für User, sondern für alle Services gelten. Indem Verbindungen ausschließlich über die entsprechenden SSE-Kontrollen zwischen befugten Quellen und gültigen Zielen hergestellt werden, minimieren Unternehmen die laterale Bewegungsfreiheit innerhalb des Netzwerks, die oft von Bedrohungen ausgenutzt wird.
- Eine Lösung, die ausschließlich Verbindungen für dynamische Zugriffe auf Sitzungsbasis herstellt. Firewalls, SD-WAN und andere Netzwerkservices beinhalten kein Zero Trust. Es muss sich um ein netzwerkunabhängiges Overlay handeln.
- Unbefugte Quellen sollten niemals auf Unternehmensressourcen zugreifen können. Deshalb muss die Angriffsfläche minimiert werden und es ist sicherzustellen, dass die richtigen Kontrollen auf alle Services angewendet werden.

Umsetzung durch kompetente SSE-Anbieter:

Zero Trust für die gesamte Unternehmenskommunikation bedeutet, dass keine Quelle (einschließlich User, Dritte, Netzwerke usw.) ohne ausdrückliche Berechtigung und Genehmigung auf ein Ziel zugreifen darf.

Die Bereitstellung von Zero Trust innerhalb eines Unternehmens ist bislang eine Herausforderung, da die Verbindung zwischen Quelle und Ziel über ein gemeinsames Netzwerk erfolgt und dazu entweder ein physischer oder logischer Netzwerkpfad erforderlich ist. Abbildung 4 verdeutlicht dieses Problem. Mit SD-WANs oder Firewalls kann man keine Zero-Trust-Architektur aufbauen oder der bestehenden Architektur hinzufügen.

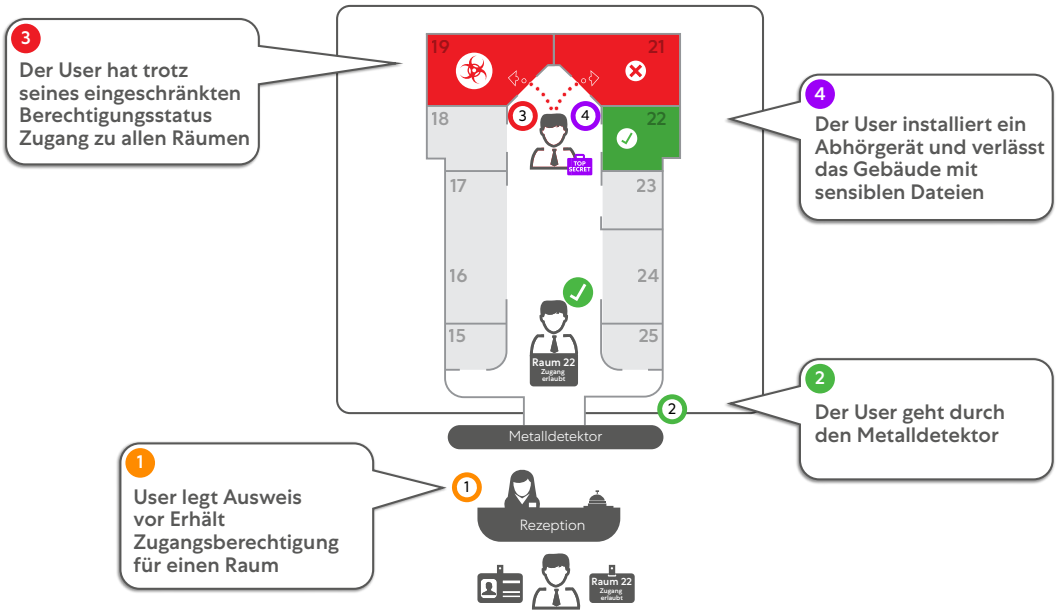

Abbildung 4: Wie Zugriffe nicht erfolgen sollten – Analogie zur herkömmlichen Netzwerksicherheit. Wenn sich User einfach mit dem Unternehmensnetzwerk verbinden können, ist es so, als würde man unbeaufsichtigten Besuchern erlauben, im Firmensitz herumzulaufen und möglicherweise sensible Daten zu stehlen.

Mit SSE können unternehmensweiter User-Zugriff und Einschränkungen für Workloads durchgesetzt werden. Indem man diese Maßnahmen nicht nur auf Mitarbeiter anwendet, lässt sich ein Unternehmen vor Risiken wie einer ungeschützten Angriffsfläche und lateraler Ausbreitung von Bedrohungen schützen.

Unter anderem setzt eine Zero-Trust-Architektur granulare Kontrollen durch, die sicherstellen, dass ein User bei jeder Anfrage mit dem richtigen Ziel kommuniziert – dies erfolgt auf Sitzungsbasis (siehe Abbildung 5). Um solche Regeln zu erstellen, muss man über Kenntnisse zu beiden Entitäten (Quelle und Ziel) verfügen. Deshalb beginnen viele Unternehmen mit ihrer User-Basis, wenn sie auf Zero Trust (und SSE) umsteigen. Usern wird oft eine Identität zugewiesen, anhand derer sie von verschiedenen Services unterschieden werden. Da die Netzwerke jedoch flach, ungeschützt und offen sind, können User Zugriff auf mehr Informationen haben, nur weil es sich um ein gemeinsam genutztes Netzwerk handelt. Dies stellt ein erhebliches Risiko für die Unternehmensstabilität dar.

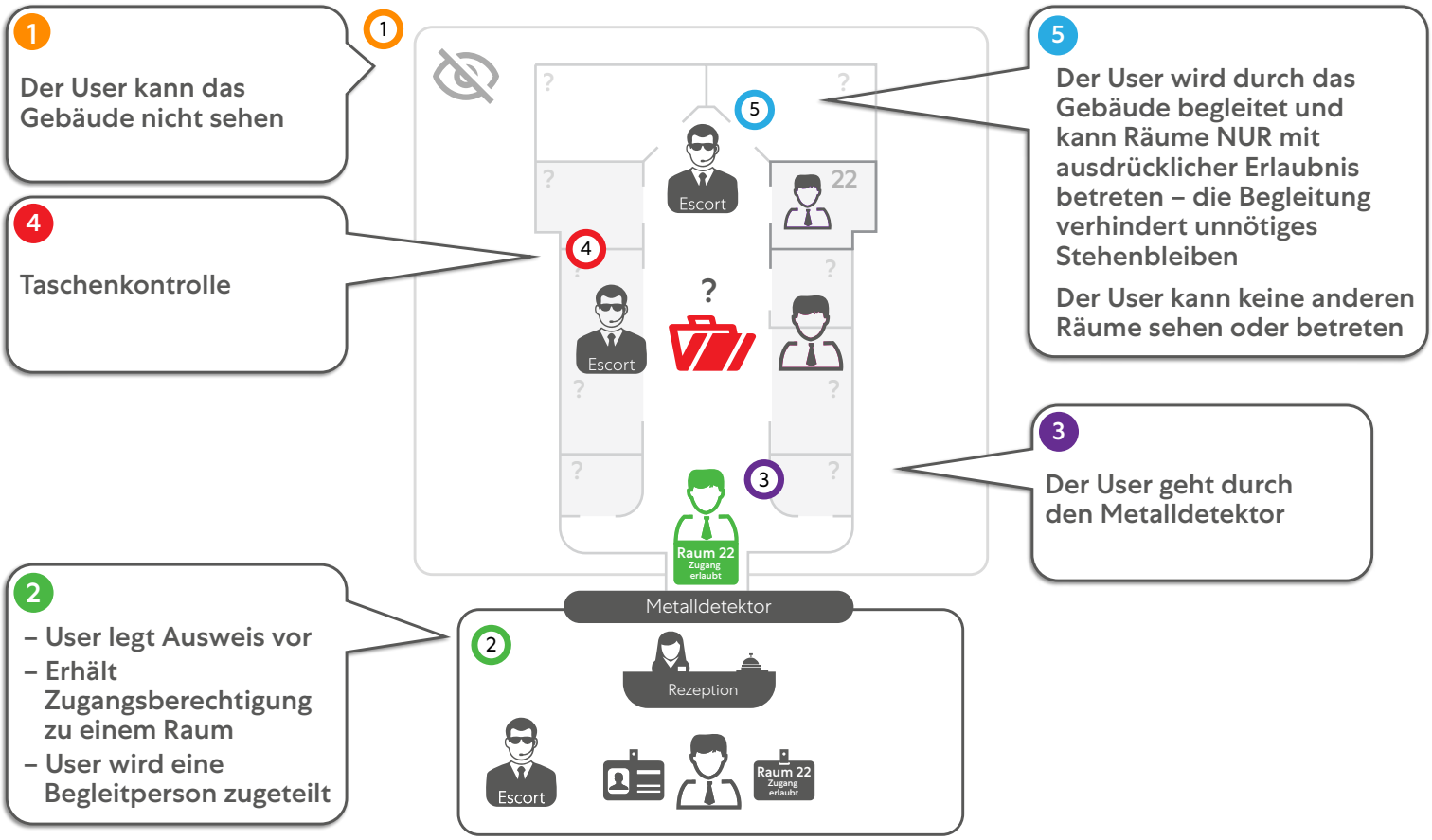

Abbildung 5: Zugriffe sollten mit durchgehender Kontrolle erfolgen. Zero-Trust-Zugriff funktioniert nach folgendem Prinzip: Man begleitet eine Besucherin mit verbundenen Augen zu einer Besprechung in den Firmensitz und danach begleitet man sie wieder hinaus. Die Besucherin kann sich nicht unbeaufsichtigt bewegen oder an geheime Informationen gelangen.

Alle geschäftlichen Anwendungsfälle, wie z. B. der Schutz von Usern und wichtigen Unternehmensressourcen, sollten berücksichtigt und SSE-Kontrollen auf den gesamten Traffic angewendet werden. Verbindungen sollten erst hergestellt werden, wenn das Risiko der folgenden Aspekte dynamisch und kontextbezogen bewertet wurde (siehe Abbildung 6):

Initiator der Verbindung

Welche Identität und welchen Vertrauenstatus hat der User/das Gerät/das Netzwerk? Darf diese Identität auf diese Quelle zugreifen und unter welchen Bedingungen?

Beispiel: Sarah aus der Personalabteilung benötigt Zugriff auf das in der Cloud gehostete HR-System sowie auf das intern gehostete Kostensystem. Der Zugriff wird über die SSE-Plattform gewährt, sofern ihre Identität und der Vertrauensstatus ihres Geräts die erforderlichen Berechtigungen aufweisen.

Richtlinienüberprüfung

Wo und wie werden welche Kontrollen durchgeführt? Kriterien für die Kontrolle sind u. a. die Effektivität des Pfades, das Risiko und der Vertrauensstatus des Initiators, die Funktion des angeforderten Ziels und die Unternehmensrichtlinien.

Beispiel: Pierre hat eine gültige Identität, um auf Salesforce zuzugreifen, aber sein Unternehmen möchte, dass er die Daten nur ansehen, aber nicht herunterladen oder bearbeiten kann. Die SSE-Lösung gewährt Pierre daher ausschließlich Zugriff, um die Inhalte der Anwendung anzusehen.

Ziel der Verbindung

Auf welchen Service wird zugegriffen? Handelt es sich um öffentliche SaaS oder um eine interne Workload? Welche Kontrollen sollen durchgeführt werden? Der Zugriff kann sich je nach Kontext der Identitäts- und Kontrollrichtlinie ändern.

Beispiel: Ein gültiger Initiator kann die Genehmigung haben, auf einen bestimmten Cloud-PaaS-Service zuzugreifen. Wenn es sich um einen Cloud-Service handelt, überprüft die SSE-Lösung die Workload, um sicherzustellen, dass keine vertraulichen Informationen preisgegeben werden. Der Initiator kann dann mit einem internen Service mit ähnlichem Vertrauensstatus kommunizieren und so einfach eine Verbindung zwischen Initiator und Service herstellen, ohne dass zusätzliche Kontrollen erforderlich sind.

Herstellung der Verbindung

Schließlich werden die vorherigen Eingaben, die bedingten Einblicke in Workloads, Netzwerk oder Edge-Kapazitäten und unternehmensspezifische Richtlinien usw. herangezogen und der Zugriff hergestellt. Die SSE-Lösung sollte Abweichungen wie z. B. einen neuen Standort erkennen und den Zugriff über den geeignetsten Pfad gewähren.

Beispiel: Sobald Quelle, Kontrolle und Ziele validiert sind, wird die Verbindung ausschließlich für diese Sitzung hergestellt. Der lückenlose Ablauf der Durchsetzung auf Sitzungsbasis ist in Abbildung 6 dargestellt.

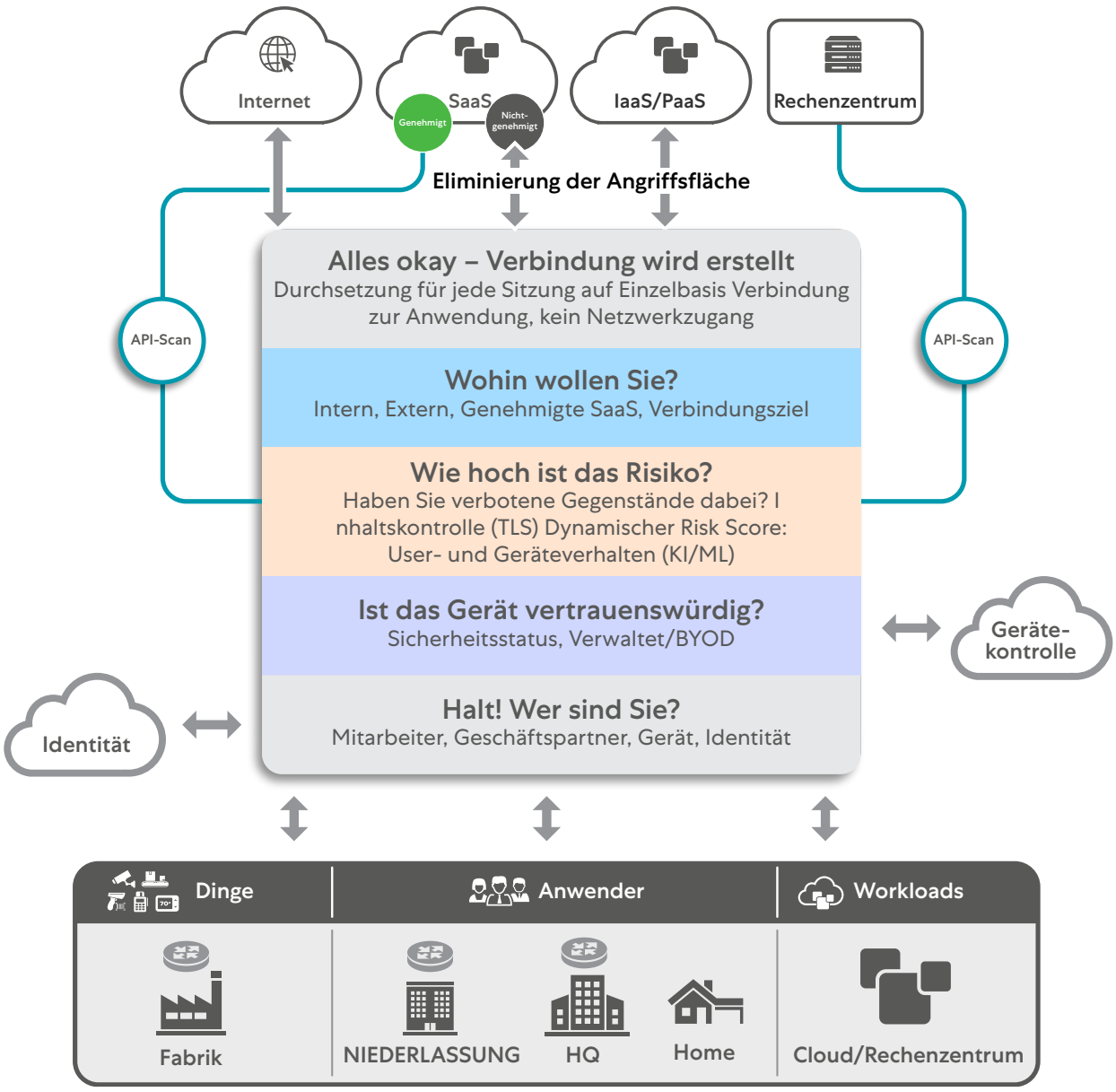

Abbildung 6: Phasen einer Zero-Trust-Architektur – Richtlinienüberprüfung und -durchsetzung in jeder Phase

Indem man die Verbindungskontrollen innerhalb einer SSE-Lösung definiert, **stellt man sicher, dass nur die richtige Quelle über die richtige SSE-Lösung auf das richtige Ziel** zugreifen kann. Diese Nutzung von SSE mit minimaler Rechtevergabe bietet einem Unternehmen mehrere Vorteile, darunter:

- Die richtigen SSE-Kontrollen können auf die richtige Quelle angewendet werden
- SSE-geschützte Services sind für unbefugte Quellen nicht zugänglich, wodurch Cybersicherheitsrisiken reduziert werden
- Es werden weniger unnötige Verbindungen hergestellt, z. B. keine Verbindung zwischen einem Linux-Server und einem Windows-Patch-System
- Granulare Transparenz und Erlernen von Abläufen – pro Zugriffsanfrage, nicht von Netzwerk-IP zu IP
- Konsolidierung des Zugriffs auf Grundlage der Identität und nicht des Netzwerks, wodurch Netzwerkfunktionen (und Infrastruktur) rationalisiert werden können

Der Weg zu SEE mit Zero Trust:

Durch die Auswahl einer SSE-Lösung, die User-basierte Kontrollen in den folgenden Anwendungsfällen bietet, können Schutzmaßnahmen auf alle Geschäftsbereiche ausgeweitet werden (siehe Abbildung 7):

User zu Workloads

Wenn Unternehmen User-Zugriff auf Workloads ermöglichen, bedeutet das, dass das Netzwerk bei solche Zugriffen keine Rolle mehr spielt. Gleichzeitig erhält man Transparenz über die Workloads, auf die User zugreifen. Dieses Konzept bietet in der Regel den schnellsten Mehrwert.

Granulare Kontrollen für User in der gesamten Anwendungslandschaft sollten in Betracht gezogen werden. Beispielsweise können Internetservices wie YouTube auf das PR-Team eines Unternehmens beschränkt werden.

So können mehr Unternehmensservices entwickelt und detailliertere Regeln, z. B. für den Zugriff auf isolierte OT- und R&D-Plattformen, erstellt werden, ohne dass der User-Basis das gesamte Ökosystem zugänglich gemacht wird.

Zugriff für externe Dritte

Werden herkömmliche Modelle für den Zugriff externer User verwendet, führt dies zu einer riskanten Verbindung mit dem Netzwerk und zu einer ungeschützten Angriffsfläche. Durch die Implementierung des Zero-Trust-Zugriffs entfallen diese Risikofaktoren. Mithilfe des Zero-Trust-Prinzips der minimalen Rechtevergabe können Unternehmen festlegen, dass Partner über nicht vertrauenswürdige oder private Geräte nur auf bestimmte Anwendungen zugreifen können. Gleichzeitig erhalten sie einen besseren Überblick darüber, worauf externe User zugreifen.

Kontrollen einer SSE-Lösung für externe User sollten mehrere Mechanismen für die Zugriffskontrolle umfassen. Zu den Optionen zählen autorisierter Client-Zugriff von mehreren Identitätsanbietern, Zugriff auf bestimmte Anwendungen, isolierter Browser-Zugriff oder ausschließlich Zugriff auf ein gerendertes Bild, das externen Usern präsentiert wird (Streaming von Pixeln an das Gerät des Users wie BYOD).

Zwischen Workloads

Kontrollen zwischen Workloads sind Zugriffsanfragen auf Anwendungen und Services. Im Allgemeinen fordert ein Windows-Rechner Windows- und nicht Linux-Patches an. Daher ist es entscheidend, dass ein Unternehmen festlegt, welche Systeme auf welche Entitäten zugreifen können.

Wie bei User-Kontrollen muss auch bei Workload-Kontrollen eine gültige Identität angegeben werden, um einen Service nutzen zu können. Wenn die Workload öffentliche Ressourcen wie PaaS-basierte IoT/OT-Dienste nutzt, muss die Security Edge den Kontext validieren und erfassen sowie jeden versuchten Missbrauch blockieren.

Sollte die Workload hingegen auf einen lokalen, privaten Service zugreifen, kann dies nur durch Inline-SSE-Kontrollen erfolgen, nachdem die Identität mithilfe einer Zero-Trust-Validierung genehmigt wurde.

Standort zu Standort

Wenn sich Zugriff und Kontrollen in einem Unternehmen weiterentwickeln, sollte Zero Trust für die Intersite-Konnektivität in Betracht gezogen werden. Man muss bestimmte Services auf ein Netzwerk, einen Standort oder eine VPC einschränken. Die Verbindung zwischen dem Standort und dem bekannten Ort sollte nicht über ein gemeinsames Netzwerk erfolgen. Mithilfe von Zero Trust kann eine Verbindung zwischen einem gültigem Standort und gültigen Workloads an einem anderen Ort hergestellt werden. Bei Zero Trust wird nicht über Link-Layer auf ein Netzwerk zugegriffen. Stattdessen werden Verbindungen zwischen Anwendungen hergestellt – einheitlich an jedem Standort, in jeder VPC und in jedem VLAN.

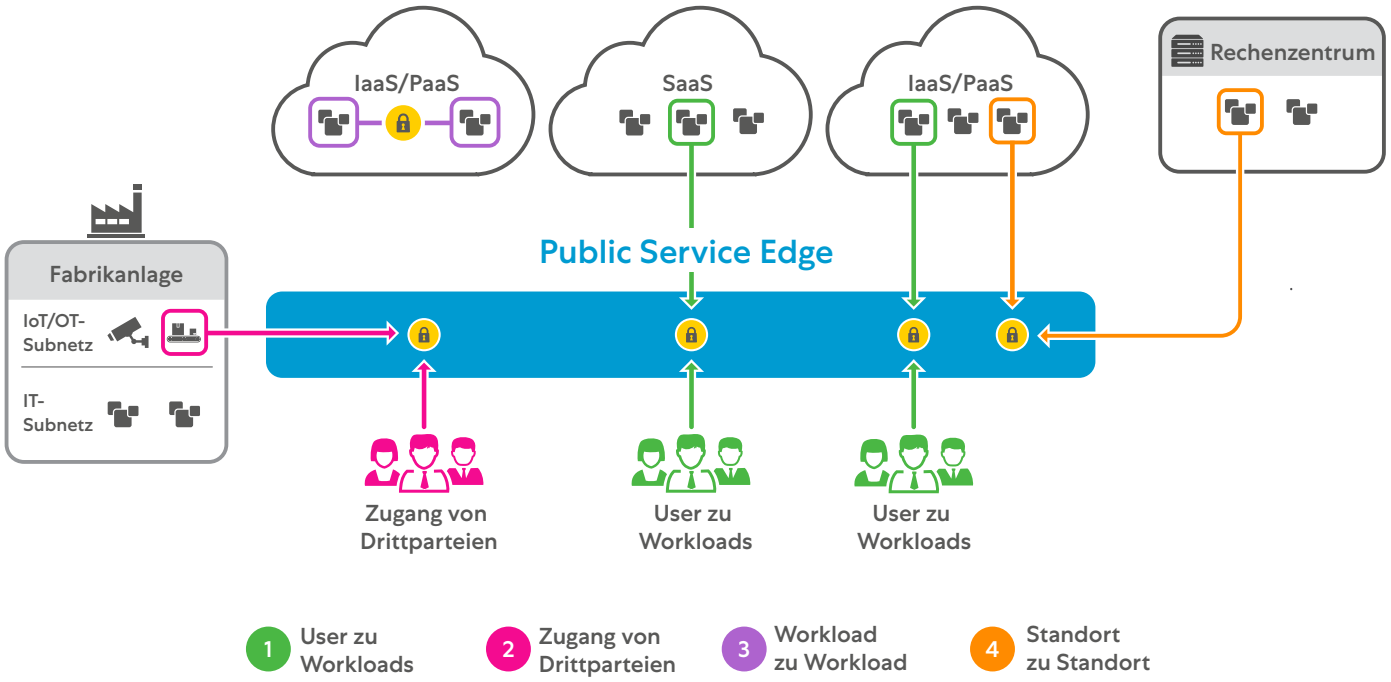

Abbildung 7: Ein empfohlener Ansatz zur Segmentierung in Unternehmen. Ein Ansatz in Phasen für Kontrolle, Lernen, weitere Segmentierung und Isolierung – als Teil einer Zero-Trust-Implementierung

Als Sicherheitsforscher vor kurzem die Zero-Day-Schwachstelle in Log4j entdeckten, bestand für jeden Kunden, der das anfällige, auf Apache Java basierende Protokollierungsprogramm verwendete, das Risiko einer vollständigen Remote-Code-Ausführung. Interne Anwendungen in einer Zero-Trust-Architektur sind für das Internet jedoch völlig unsichtbar. Das bedeutet, dass die Angreifer sie nicht finden und ausnutzen könnten, sodass selbst Unternehmen, die anfällige Versionen von Apache Log4j verwenden, vor diesem und zukünftigen Sicherheitsrisiken geschützt sind. Dies wäre mit herkömmlichen, angreifbaren Methoden wie VPNs und Firewalls nicht möglich. **Zero Trust stellt sicher, dass nur autorisierte User auf Anwendungen zugreifen können. Dank User-to-App- und App-to-App-Mikrosegmentierung können sich Bedrohungen nicht lateral ausbreiten. Zudem werden sowohl eingehender als auch ausgehender Traffic überprüft**.

Ähnliches gilt für den Angriff auf Colonial Pipeline, bei dem Hacker mithilfe von gestohlenen VPN-Zugangsdaten (ohne aktivierte MFA) Zugriff auf das Netzwerk erhielten und sich dann lateral bewegen und auf sensible Daten zugreifen konnten. Eine Zero-Trust-Architektur, die nur autorisierte User mit Anwendungen und nicht mit dem Netzwerk verbindet, verhindert laterale Bewegungen, indem sie die Kommunikation zwischen Usern und Anwendungen sowie zwischen einzelnen Anwendungen segmentiert.

Worauf sollte man achten?

- Vermeidung von SSE-Services, die nicht den Prinzipien einer Zero-Trust-Architektur entsprechen (z. B. nach NIST Special Publication 800-207).
- Der SSE-Service sollte Zero-Trust-Kontrollen für alle Unternehmensressourcen bieten, nicht nur für User.
- Zero Trust ist keine Funktion von Firewalls oder SD-WANs. Zero Trust ist netzwerkunabhängig. Wenn man die SSE-Lösung eines netzwerkabhängigen Anbieters auswählt, erhält man möglicherweise eine mangelhafte Zero-Trust-Architektur.
- Zero-Trust-Kontrollen sollten mit Zero-Trust-Zugriff beginnen. Erst nach der Validierung sollte man auf Unternehmensressourcen zugreifen können.
- Man sollte alle Aspekte eines Unternehmens einbeziehen. Zero-Trust-Kontrollen sollten nicht auf nur einen Teil des Unternehmens beschränkt sein.

Ergebnisse:

Unternehmen und User können am effizientesten geschützt werden, wenn Zugriffe nur nach Erforderlichkeitsprinzip mit minimaler Rechtevergabe erfolgen. **Aus folgenden Gründen muss Zero Trust bei der Auswahl einer SSE-Lösung das entscheidende Kriterium sein:**

- Der SSE-Anbieter schützt alle Unternehmensservices und validiert die Identität der Entitäten, bevor Zugriff gewährt wird. Alle anderen Zugriffsversuche müssen blockiert werden.
- Lösungen, für die eine Verbindung mit dem Netzwerk erforderlich ist, sollten vermieden werden. Der Zugriff sollte netzwerkunabhängig erfolgen – überall.
- Der SSE-Service bietet hinsichtlich privater Unternehmensservices keine Angriffsfläche.

#3 Fehler

Auswahl einer SSE-Lösung, die vermeintlich Advanced Threat Protection und erweiterte DLP bereitstellt, ohne verschlüsselten Traffic bei hohem Datenvolumen überprüfen zu können

Stattdessen sollte man bei der Auswahl einer SSE-Lösung folgende Kriterien beachten:

- Die SSE-Lösung gewährleistet eine SSL/TLS-Überprüfung des gesamten Traffics in der Produktivumgebung. Dabei wird die Performance nur minimal beeinträchtigt. Voraussetzung dafür ist eine skalierbare Proxy-Architektur.
- Die aus der Überprüfung gewonnenen Erkenntnisse werden zur Erstellung von ATP-Richtlinien für verschlüsselten Traffic sowie DLP-Richtlinien auf der Grundlage erweiterter Datenklassifizierung verwertet.
- Der gesamte Traffic (verschlüsselt, User, Objekte, Workloads usw.) wird überprüft.

Umsetzung durch kompetente SSE-Anbieter

SSE-Anbieter können nicht behaupten, die beste Advanced Threat Protection und Data Loss Prevention zu bieten, wenn sie nicht in der Lage sind, den gesamten Traffic in der Produktivumgebung zu überprüfen (einschließlich verschlüsseltem Traffic).

Man sollte sich solche Behauptungen genau ansehen, da vieles von der zugrundeliegenden Architektur der Lösung abhängt. SSE-Anbieter, die einen von Grund auf Cloud-nativen Cloud-Proxy entwickelt haben, haben in diesem Bereich einen entscheidenden Vorteil.

Da die überwiegende Mehrheit (schätzungsweise etwa 85 %) des Internet-Traffics verschlüsselt ist, müssen SSE-Anbieter diesen Traffic umfassend und detailliert überprüfen, um einen angemessenen Schutz vor Bedrohungen und Datenverlusten zu gewährleisten. Angesichts der exponentiell zunehmenden Sicherheitsrisiken durch verschlüsselte Kanäle sind solche Schutzmaßnahmen dringend erforderlich. Warum ist eine umfassende SSL/TLS-Entschlüsselung so wichtig (siehe Abbildung 8)?

- SSL/TLS-Verschlüsselung wird verwendet, um gefährliche Inhalte wie Viren, Spyware und andere Malware zu verbergen.
- Angreifer erstellen Websites mit TLS- und SSL-Verschlüsselung oder schleusen ihre schädlichen Inhalte in bekannte und vertrauenswürdige Websites mit SSL- und TLS-Verschlüsselung ein.
- SSL/TLS kann verwendet werden, um Datenlecks zu verbergen, z. B. die Übertragung vertraulicher Finanzdokumente einer Organisation.
- Mit SSL/TLS kann das Browsen auf rechtlich fragwürdigen Websites verborgen werden.
- Die Möglichkeit, den von Onlineservices eingehenden und ausgehenden Traffic mit HTTPS zu steuern und zu überprüfen, ist zu einem wichtigen Bestandteil des Sicherheitsstatus von Unternehmen geworden.

Abbildung 8: Mit der von manchen Anbietern eingesetzten Passthrough-Architektur kann verschlüsselter Traffic nicht umfassend überprüft werden. Dieses Sicherheitsproblem ähnelt einer einfachen Verkehrskontrolle, bei der ein Auto passieren darf, ohne dass im Kofferraum nach illegalen Gegenständen gesucht wurde.

Angesichts dieser Risiken muss die Architektur eines SSE-Anbieters so skaliert werden können, dass sie als SSL/TLS-Proxy nach dem Man-in-the-Middle-Prinzip fungiert. So können eingehende und ausgehende Inhalte vollständig analysiert und alle in der Cloud entdeckten Bedrohungen sofort blockiert werden.

Bedrohungsakteure entwickeln ihre Tools, Techniken und Methoden für Angriffe auf Unternehmen ständig weiter. Dazu gehört auch der Missbrauch von legitimen Anbietern von Speicherservices wie Dropbox, Box, OneDrive und GDrive zum Hosten schädlicher Payloads. Bei solchen Verbindungen werden SSL/TLS-Zertifikate dieser renommierten Anbieter als Platzhalter für die schädlichen Payloads verwendet. Wenn diese also nicht überprüft werden, kann es zu einem erfolgreichen Angriff kommen. Die schädlichen Payloads (ausführbare Dateien, Office-Dokumente usw.) sind zudem polymorph, da grundlegende Fingerprint-Erkennung umgangen werden soll. Mithilfe der Architektur der SSE-Anbieter müssen Payloads vollständig aus diesen SSL/TLS-verschlüsselten Verbindungen extrahiert und die Dateien entpackt sowie entschlüsselt werden, um sie genau zu überprüfen (siehe Abbildung 9).

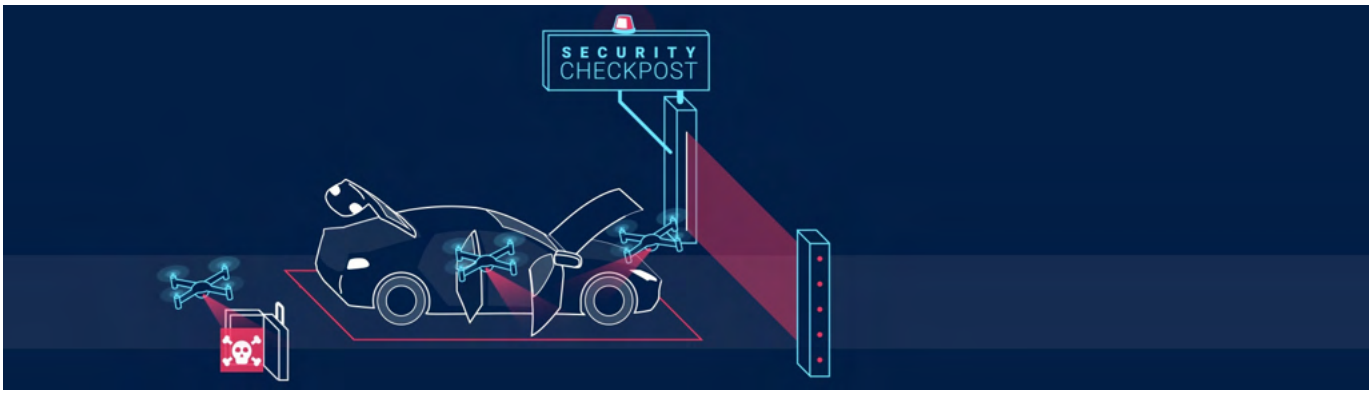

Abbildung 9: Der richtige SSE-Anbieter bietet eine vollständige SSL/TLS-Überprüfung des gesamten Traffics mithilfe einer Proxy-Architektur. Der Prozess ähnelt einer Verkehrskontrolle, bei der ein Fahrzeug angehalten und vollständig durchsucht wird, bevor es weiterfahren darf.

Bei diesen Schutzmaßnahmen sollten diverse branchenspezifische Bedrohungsdaten aus Open-Source-, kommerziellen und privaten Quellen genutzt werden. Zudem sollten regelmäßige Sicherheitsupdates durchgeführt werden.

Durch eine umfassende Überprüfung können nicht nur Bedrohungen blockiert, sondern auch erweiterte DLP-Funktionen realisiert werden. **Bei der Auswahl eines SSE-Anbieters sollten auch die Funktionen zur Datenklassifizierung** berücksichtigt werden. Diese sollten reguläre Ausdrücke (Regex) als grundlegenden Mechanismus beinhalten. Schnelles Erkennen und Klassifizieren sensibler Daten in allen Cloud-Datenkanälen ist jedoch entscheidend, um persönliche, gesundheitsbezogene und vertrauliche Daten vor Verlust zu schützen. Dazu ist eine SSL/TLS-Überprüfung erforderlich. Durch die Klassifizierung können weitere Funktionen genutzt werden, darunter:

- **Exact Data Match**: Die SSE-Lösung verwendet Indexvorlagen, um einen Datensatz aus einer strukturierten Datenquelle zu identifizieren, der mit vordefinierten Kriterien übereinstimmt.
- **Fingerprinting für Dokumente**: Die SSE-Lösung verwendet ein Dokumenten-Repository, um bei der Überprüfung des ausgehenden Traffics vollständig oder teilweise übereinstimmende Dokumente zu identifizieren.
- **OCR (Optical Character Recognition)**: Die SSE-Lösung erkennt sensible Daten in Bilddateien, eingebetteten Bildern, Screenshots sowie handschriftlichen Texten und schließt alle Cloud-basierten Kanäle zur Datenexfiltration.
- **Maschinelles Lernen:** Mithilfe zuvor trainierter Algorithmen wird bestimmt, wie sensibel die Daten sind.

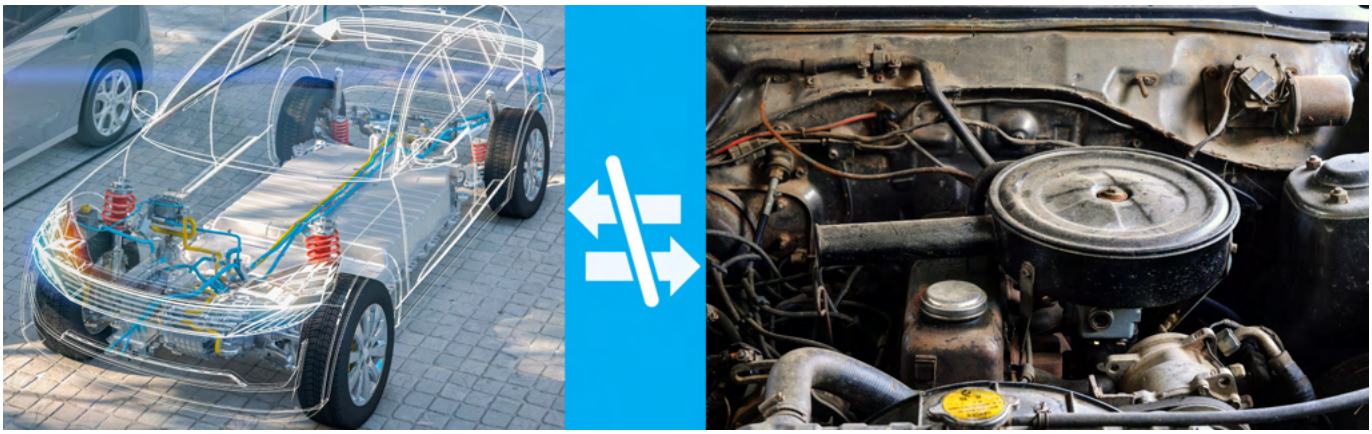

Abbildung 10: Ein Verbrennungsmotor kann nicht einfach zu einem Elektromotor umgebaut werden. Entsprechend sollte man Anbieter kritisch betrachten, die Funktionen wie SSL/TLS-Überprüfung in Legacy-Architekturen integrieren.

SSE umfasst die Funktionen eines Cloud Access Security Broker (CASB) zum Monitoring und Durchsetzen von Richtlinien zwischen Usern von Cloud-Services und Anwendungen. Den verschlüsselten Traffic inline überprüfen zu können, bietet in diesem Zusammenhang eine Reihe von Vorteilen. Die Überprüfung kann „Out-of-band" erfolgen, d. h. die APIs von SaaS-Anbietern werden gescannt, um ruhende Daten zu schützen, oder „inline", d. h. Daten werden bei der Übertragung gescannt. Die Inline-Überprüfung ist besonders relevant, da sie verhindert, dass Daten in inoffiziell genutzte Anwendungen hochgeladen, auf inoffiziell genutzte Geräte heruntergeladen und schädliche Inhalte herunter- oder hochgeladen werden. Der SSE-Anbieter sollte zudem granulare Zugriffskontrollen auf Grundlage unterschiedlicher Definitionen Cloud-basierter Anwendungen, Dateitypkontrollen und Risikoattribute bereitstellen.

Durch die Einführung von unzähligen Cloud-basierten Anwendungen sind die sensiblen Daten von Unternehmen heute sehr verteilt. In zwei Kanälen kommt es hauptsächlich zur Datenexfiltration: Cloud-basierte Desktop-Anwendungen und persönliche E-Mail-Anwendungen. Ein guter SSE-Anbieter sollte vollständige kontextbezogene Transparenz und Richtliniendurchsetzung bereitstellen, wenn User sensible Daten auf ihre persönlichen Box-, Dropbox- und andere Cloud-Desktops hochladen. Sie sollten auch Datenexfiltration über persönliche und inoffiziell genutzte Webmail-Services wie Gmail und Hotmail unterbinden.

Besonders deutlich werden die Unterschiede zwischen verschiedenen SSE-Anbietern, wenn man folgende Faktoren berücksichtigt: Wie gut können sie SSL/TLS-Traffic entschlüsseln und überprüfen? Können Funktionen zur Entschlüsselung und Überprüfung elastisch den Anforderungen entsprechend skaliert werden? Werden diese umfassenden Funktionen ohne Beeinträchtigung der Leistung bereitgestellt? All diese Anforderungen können nur mit einer Proxy-basierten SSE-Lösung erfüllt werden, die von Anfang an auf Skalierbarkeit ausgelegt ist (siehe Abbildung 10).

Man sollte sich unbedingt informieren, inwiefern der SSE-Anbieter diesen Anforderungen entspricht. Um die Latenz bei jeder Paketüberprüfung so gering wie möglich zu halten, sollte der Anbieter eine Single-Pass-Architektur verwenden, bei der das Paket einmal im Speicher abgelegt wird. Die Services zur Überprüfung haben jeweils eigene CPU-Ressourcen und können Scans zeitgleich durchführen. Bei Anbietern, die diese Überprüfungen mit serialisierten physischen und virtuellen Anwendungen durchführen, verzögert sich die Verarbeitung bei jedem Hop – sie laufen Gefahr, dass es bei jedem Paket zu übermäßiger Latenz kommt.

Diese architektonischen Vorteile müssen auf neuere Standards wie TLS 1.3 angewendet werden, bei denen eine echte Proxy-Architektur mit zwei getrennten Verbindungen zu Client und Server vorliegt. Da auf diese Weise das gesamte Objekt wieder zusammengesetzt und gescannt werden kann, können Advanced Threat Protection, DLP und Sandboxing angewendet werden. Upgrades der TLS-Versionen und Verschlüsselung sollten nahtlos vom Anbieter innerhalb der Cloud durchgeführt werden. Bestimmte hardwarebasierte Anbieter erzwingen möglicherweise Appliance-Aktualisierungen, um die für die Unterstützung neuer Verschlüsselungen benötigte Kapazität auszugleichen.

Auch das Zertifikatmanagement sollte angesichts der Komplexität, die damit einhergehen kann, berücksichtigt werden. SSE-Anbieter sollten es Kunden freistellen, ob sie Zertifikate des Anbieters oder eigene verwenden. Auch ein Wechsel zwischen den Zertifikaten sollte über API möglich sein. Zertifikate sollten automatisch an den verschiedenen Service Edges repliziert werden.

SSE-Anbietern, die Funktionen zur SSL/TLS-Überprüfung zu vorhandenen NGFWs hinzufügen, die inhärente Skalierungsprobleme haben, sollte man kritisch gegenüberstehen. Dies betrifft auch Anbieter, die NGFWs mit Überprüfungsfunktionen in virtuelle Instanzen in CSP-Computing-Nodes übertragen.

⚠ Worauf sollte man achten?

Wenn man die Funktionen eines SSE-Anbieters zur SSI-/TLS-Überprüfung bewertet, sollte man auch darauf achten, dass die auftretende Latenz akzeptabel ist. Leider können nicht Cloud-native Architekturen erhebliche Leistungseinbußen verursachen, insbesondere unter Verwendung von TLS 1.2 oder älteren Versionen. **Auch Datenschutz kann ein Problem sein, daher sollte man sich mit regulatorischen Einschränkungen befassen und herausfinden, wie der Anbieter damit umgeht**. SSE-Anbieter sollten den einfachen Ausschluss bestimmter Datentypen ermöglichen, um den Datenschutzbestimmungen zu entsprechen. SSE-Anbieter sollten User-Daten niemals in der Cloud speichern.

SSE-Anbietern, die Funktionen zur SSL/TLS-Überprüfung zu vorhandenen NGFWs hinzufügen, die inhärente Skalierungsprobleme haben, sollte man kritisch gegenüberstehen. Dies betrifft auch Anbieter, die NGFWs mit Überprüfungsfunktionen in virtuelle Instanzen in CSP-Computing-Nodes übertragen. Auch Anbieter, die Out-of-Band-CASB-Funktionen mit einer begrenzten Inline-Traffic-Überprüfung kombinieren, sind mit Vorsicht zu genießen. Ruhende Daten und Daten bei der Übertragung zu schützen, ist entscheidend.

Man sollte sich informieren, wie der SSE-Anbieter Zertifikate verwaltet, und sich darüber im Klaren sein, dass Certificate Pinning ein Problem darstellen könnte.

Die Implementierung einer SSL/TLS-Überprüfung ist seit jeher aus verschiedenen Gründen eine Herausforderung für Unternehmen. **Der SSE-Anbieter sollte diesbezüglich ein vertrauenswürdiger Experte sein und bei der Einführung solche Funktionen anleiten und unterstützen. Die SSL/TLS-Überprüfung** ist in einer SSE-Umgebung unerlässlich, da sowohl Geschwindigkeit als auch Sicherheit dringend erforderlich sind.

Ergebnisse:

Mithilfe einer umfassenden SSL/TLS-Überprüfung mit minimaler Latenz können Bedrohungen deutlich effizienter blockiert werden, indem die Leistungsfähigkeit der Cloud genutzt wird, um sensible Daten zu identifizieren und zu schützen. Nur SSE-Anbieter mit der richtigen Cloud-nativen Architektur können Kunden Folgendes bieten:

- Eine SSL/TLS-Überprüfung des gesamten Traffics in der Produktivumgebung mit minimalen Auswirkungen auf die Performance, um einen umfassenden Schutz vor Bedrohungen sowie umfassenden Datenschutz zu erzielen
- Eine Single-Pass-Architektur, bei der Pakete einmal im Speicher abgelegt und gescannt werden – so lassen sich Skalierbarkeit und Entschlüsselung in großem Maßstab realisieren
- Die erforderliche Erfahrung, um Kunden bei der Implementierung der SSL/TLS-Überprüfung und möglichen Herausforderungen zu unterstützen

#4 Fehler

Die ausgewählte SSE-Lösung ist eine Allzwecklösung ohne flexible, skalierbare und vielseitige Bereitstellungs- und Verwaltungsoptionen

Stattdessen empfiehlt sich die Auswahl einer Lösung, die folgende Voraussetzungen erfüllt:

- Die SSE-Lösung unterstützt flexible Bereitstellungsmodelle zum Schutz von Usern und Anwendungen, die in unterschiedlichen Umgebungen gehostet werden, einschließlich Rechenzentrum, öffentliche Cloud, private Cloud, Edge-Computing-Node und On-Premise.
- Sie schützt User, die sowohl über verwaltete als auch nicht verwaltete Endgeräte auf Anwendungen oder Objekte zugreifen.
- Die Lösung bietet Schutz vor Cyberbedrohungen und Datenschutz für jegliche Kommunikation zwischen Workloads – egal, ob sie sich in derselben oder mehreren Clouds befinden.

Umsetzung durch kompetente SSE-Anbieter

Wenn man nach der richtigen SSE-Lösung sucht, muss man auch beurteilen, wie ausgereift die eigene Umgebung ist. Nur so kann man herausfinden, wie SSE-Schutzmaßnahmen am besten integriert werden können. Aufgrund unterschiedlichster Bereitstellungsszenarien müssen SSE-Anbieter sowohl Public Service Edges als auch Private Service Edges unterstützen.

Umsetzung durch kompetente SSE-Anbieter

Wenn man nach der richtigen SSE-Lösung sucht, muss man auch beurteilen, wie ausgereift die eigene Umgebung ist. Nur so kann man herausfinden, wie SSE-Schutzmaßnahmen am besten integriert werden können. Aufgrund unterschiedlichster Bereitstellungsszenarien müssen SSE-Anbieter sowohl Public Service Edges als auch Private Service Edges unterstützen.

Die meisten User verbinden sich über die Public Service Edge eines Anbieters mit der SSE. Dabei handelt es sich um sichere Internet-Gateways mit vollem Funktionsumfang und private Anwendungsbroker, die integrierte Sicherheit bieten. Sie untersuchen den gesamten Traffic bidirektional auf Malware und setzen Sicherheits-, Compliance- und Firewall-Richtlinien durch. Dabei müssen sie Hunderttausende von Usern mit Millionen von simultan stattfindenden Sitzungen verarbeiten. Daher ist der User-Zugriff an jedem Standort geräteunabhängig möglich. Dieser Ansatz bietet folgende Vorteile:

- Internet mit Public Service Edges zum Schutz des Traffics und zur Durchsetzung von Unternehmensrichtlinien
- Durchsetzung von Zugriffs- und Re-Authentifizierungsrichtlinien für interne Anwendungen, wobei die Richtlinien auf den Best Practices des Unternehmens basieren

Abbildung 11: Ein SSE-Anbieter muss Public Service Edges und Private Service Edges als Option bieten, die zudem mit zentralem Management kombinierbar sein müssen.

Es ist wichtig, dass diese Public Service Edges sehr fehlertolerant sind und im Aktiv/Aktiv-Modus bereitgestellt werden, um Verfügbarkeit und Redundanz zu gewährleisten. Der Anbieter sollte seine Public Service Edges warten und überwachen, um kontinuierliche Verfügbarkeit sicherzustellen. Um Datenschutz zu gewährleisten, darf Kunden-Traffic nicht an andere Komponenten innerhalb der Infrastruktur weitergegeben werden. Daten sollten nicht auf der Festplatte gespeichert werden.

Es kann jedoch vorkommen, dass die Public Service Edge nicht den Anforderungen entspricht und der SSE-Anbieter daher Private-Service-Edge-Optionen anbieten muss (siehe Abbildung 11). Mithilfe solcher Optionen werden die Architektur und die Funktionen der Public Service Edge auf On-Premise- oder private Umgebungen eines Unternehmens ausgeweitet. Dabei werden dieselben zentral gesteuerten Richtlinien wie bei der Public Service Edge verwendet.

Um sicheren Zugriff auf das Internet zu ermöglichen, können Private Service Edges im Unternehmensrechenzentrum installiert werden. Sie sind für den Traffic bestimmt und werden vom SSE-Anbieter verwaltet und gewartet, sodass das Unternehmen kaum tätig werden muss. Von diesem Bereitstellungsmodell profitieren in der Regel Organisationen, die bestimmte geopolitische Anforderungen haben oder Anwendungen nutzen, deren Quell-IP-Adresse die IP-Adresse der Organisation sein muss.

Für den Zugriff auf interne Anwendungen bietet die Private Service Edge ähnliche Optionen, um Verbindungen zwischen User und Anwendung zu verwalten. Zudem werden dieselben Richtlinien angewendet wie bei der Public Service Edge, wobei der Service entweder vor Ort oder in der öffentlichen Cloud gehostet, aber auch vom SSE-Anbieter verwaltet wird. Bei diesem Bereitstellungsmodell wird Zero Trust intern angewendet, denn es ist sinnvoll, die Anwendungslatenz zu verringern, wenn sich Anwendung und User am selben Ort befinden. Der Umweg zur Public Service Edge würde nur zusätzliche Latenz verursachen. Diese Option bietet auch eine Ausfallsicherheit, wenn die Internetverbindung unterbrochen wird. Der SSE-Anbieter sollte Images für den Einsatz in Unternehmensrechenzentren und lokalen privaten Cloud-Umgebungen bereitstellen.

Um Zero-Trust-Schutz für interne Anwendungen bereitzustellen, müssen SSE-Anbieter eine sichere, authentifizierte Schnittstelle zwischen Anwendungsservern und Public sowie Private Service Edges einrichten. **Dies sollte in verschiedenen Formen möglich sein**: ein Standard-Image einer virtuellen Maschine (VM) oder eine Container-Bereitstellung in Unternehmensrechenzentren, lokalen privaten Cloud-Umgebungen wie VMware oder öffentlichen Cloud-Umgebungen wie Amazon Web Services (AWS) EC2 sowie Pakete, die auf unterstützten Linux-Distributionen installiert werden können.

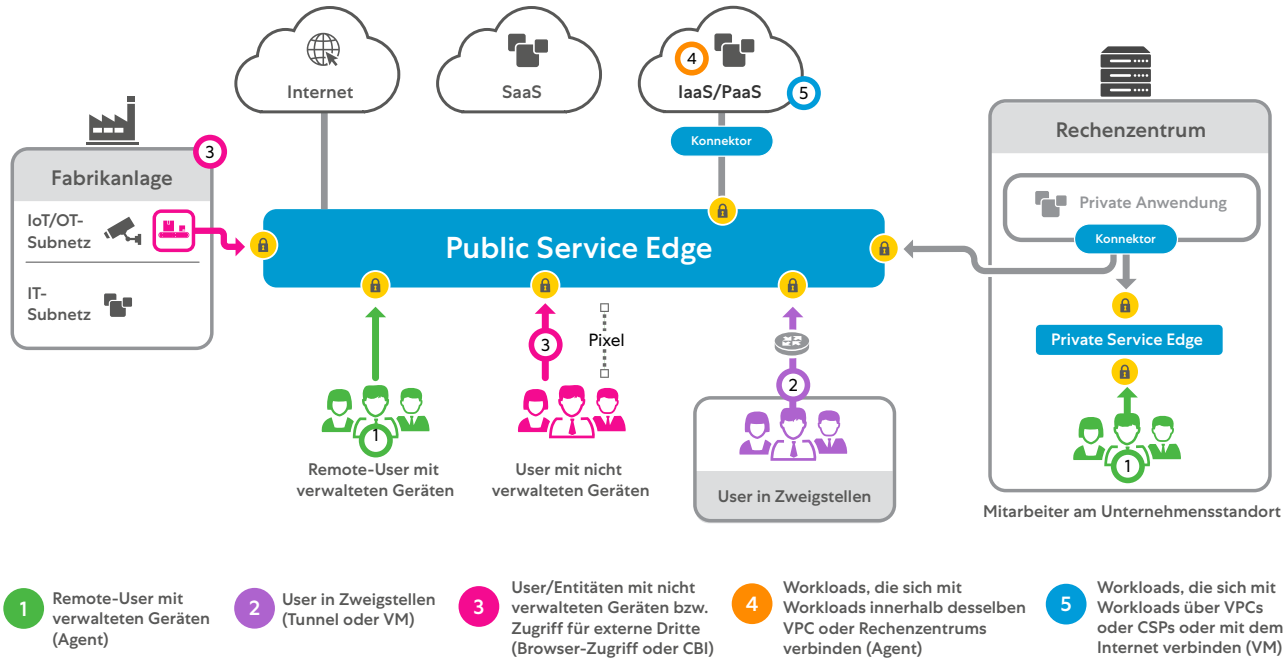

Abbildung 12: Der SSE-Anbieter sollte eine Reihe von Bereitstellungs- und Verwaltungsoptionen unterstützen, bei denen unter anderem Remote-User, User in Zweigstellen, User in der Unternehmenszentrale und Kommunikation zwischen Workloads über Agenten und VMs berücksichtigt werden.

Sobald feststeht, von welchem Ort aus die SSE-Richtlinien verwaltet und durchgesetzt werden sollen, muss man festlegen, wie User und Workloads geschützt werden. Es ist wichtig, verschiedene Szenarien einzubeziehen (siehe Abbildung 12):

Remote-User mit verwalteten Geräten: Bei diesem Szenario muss der SSE-Anbieter einen einzigen, einheitlichen Agenten bereitstellen, der den Traffic an die Service Edge weiterleitet, damit User sicher auf das Internet zugreifen können. Der Agent sollte auch granularen, richtlinienbasierten Zugriff auf interne Ressourcen ermöglichen. Diese Prozesse sollten aufgrund integrierter KI-Funktionen automatisiert erfolgen. Auch der mobile Traffic der User über WLAN oder Mobilfunknetze sollte geschützt werden. Der Agent leitet den User-Traffic an den SSE-Service weiter, der die Sicherheits- und Zugriffsrichtlinien der Organisation überall durchsetzt, wo User auf das Internet zugreifen, und sicheren Zugriff auf Unternehmensanwendungen und -services bereitstellt. Der Agent muss erkennen, wenn sich ein User mit einem vertrauenswürdigen Netzwerk verbindet. Je nach Richtlinie muss er zudem seinen Service deaktivieren, wenn ein vertrauenswürdiges Netzwerk erkannt wird. Außerdem müssen solche Agents verschiedene Betriebssysteme unterstützen, darunter Windows, MacOS, Linux, iOS und Android.

User in Zweigstellen: Eine gängige Methode zur Weiterleitung des Traffics zur Service Edge ist bei diesem Szenario ein GRE- oder IPSec-Tunnel. Der SSE-Anbieter sollte jedoch auch eine Alternative bieten. Eine virtuelle Maschine, die in der Zweigstelle installiert wird, kann die Komplexität reduzieren, die Verwaltung dieser Tunnel vereinfachen und die laterale Ausbreitung von Bedrohungen verhindern, indem das vom Kunden verwaltete routingfähige Netzwerk entfernt wird. Die Bereitstellung sollte automatisiert sein und flexible Richtlinien zur Weiterleitung des Traffics zum Service Edge mit integriertem SLA-Monitoring und Failover umfassen. Diese Option eignet sich bestens für mittlere und große Zweigstellen und solche, die lokale Services anbieten.

Besonders kleinere Zweigstellen, die keine lokalen Services anbieten, sollten in Betracht ziehen, jeden User entsprechend der vorherigen Option als Remote-User zu behandeln. In Anbetracht der jüngsten Ereignisse, die die Bedeutung von Zweigstellen verändert haben, ist diese Option äußerst praktisch, da niemand ins Unternehmensnetzwerk gelangt und laterale Bewegungen verhindert werden.

User/Objekte mit nicht verwalteten Geräten oder Zugriff von externen Usern auf interne Webanwendungen: Hierbei sollten SSE-Anbieter einen ähnlichen SSE-Schutz bieten, ohne dass ein Agent installiert werden muss. Solche User sollten einen Webbrowser für die Authentifizierung nutzen. Dadurch wird ein anwendungsspezifischer CNAME-Eintrag in der DNS-Zone angelegt, sodass der Webbrowser diese Anfragen automatisch umleiten kann, wodurch umfassender Zero-Trust-Schutz erzielt wird. Alternativ muss der SSE-Anbieter integrierte Cloud Browser Isolation (CBI) bereitstellen, um nicht verwaltete Geräte überall ohne Agent zu schützen. Dies hat den Vorteil, dass ein anfälliger Reverseproxy nicht mehr erforderlich ist.

Über CBI können Administratoren die SSO-Einstellungen genehmigter Cloud-Ressourcen konfigurieren, damit eine Weiterleitung an den SSE-Anbieter erfolgt. Wenn User dann versuchen, über persönliche oder externe Endgeräte auf diese Cloud-Ressource zuzugreifen, wird der Traffic automatisch und ohne Softwareinstallationen an die CBI gesendet. Sie rendert Inhalte in Pixel, die daraufhin an die Endgeräte gesendet werden, damit User Inhalte nicht herunterladen, kopieren, einfügen oder drucken können. Auf diese Weise können User ihre Aufgaben über nicht verwaltete Endgeräte erledigen, ohne dass das Risiko von Datenverlusten und Malware-Uploads besteht, während gleichzeitig die Compliance-Anforderungen eingehalten werden.

Verbindung von Workloads innerhalb derselben VPC oder desselben Rechenzentrums: Hier war bisher herkömmliche Netzwerksegmentierung die Lösung. Während dies in der Theorie Sinn ergab, stellte die praktische Umsetzung eine Herausforderung dar. Daher müssen SSE-Anbieter ihre Schutzmaßnahmen zwischen User und Anwendung auf die Kommunikation zwischen Workloads ausweiten. Wenn der SSE-Anbieter einen Agent auf der Workload installiert, sollte er Risiken erkennen und identitätsbasierten Schutz auf die Workloads anwenden können, ohne dass Änderungen am Netzwerk erforderlich sind. Zudem sollten Richtlinien vorhanden sein, die sich automatisch an Änderungen an der Umgebung anpassen.

Verbindung von Workloads zwischen VPCs oder CSPs oder mit dem Internet: Auch in diesem Szenario müssen SSE-Anbieter SSE-Schutzmaßnahmen, die üblicherweise für User bereitgestellt werden, auf diese Workloads ausweiten. Daher sollten SSE-Anbieter eine Methode bieten – in der Regel über eine virtuelle Maschine (verfügbar in Public Clouds oder On-Premise-Hypervisoren) –, mit der sich die Traffic-Weiterleitung zur Service Edge vereinfachen lässt. Das Ergebnis: Schutz vor Cyberbedrohungen und Datenschutz für Workloads, die ins Internet gelangen, sowie Zero-Trust-Schutz für Workloads in einer Cloud, die auf Workloads in einer anderen Cloud zugreifen. Mit diesem Ansatz können SSE-Anbieter mehrere Produkte (z. B. Web-Proxys, Firewalls, NAT-Gateways, URL-Filterung) in einer einzigen Lösung konsolidieren.

Ruhende Daten in IaaS- und SaaS-Umgebungen: Um diese Daten zu schützen, muss der SSE-Anbieter auch Lösungen in den Bereichen CASB, Cloud Infrastructure Entitlements Management (CIEM) und Cloud Security Posture Management (CSPM) anbieten, damit gängige SaaS- und IaaS-Anwendungen API-basiert gescannt werden können. Auf diese Weise können Fehlkonfigurationen und unnötige Berechtigungen in Cloud-Umgebungen identifiziert und behoben werden. Außerdem können SaaS- und IaaS-Plattformen überprüft und gescannt werden, um Schutz vor Bedrohungen und Datenschutz zu gewährleisten.
Ein SSE-Anbieter sollte diese Out-of-Band-Funktionen in enger Abstimmung mit seinen Inline-Funktionen bereitstellen, um konsistente Richtlinien auf ruhende Daten und Daten bei der Übertragung anzuwenden.

Der Vorteil eines einzigen SSE-Anbieters, der diese umfassenden Schutzmaßnahmen bereitstellt, besteht darin, dass die Verwaltung über eine zentrale Steuerungsebene erfolgt, wobei Unternehmensrichtlinien einheitlich und dynamisch auf jegliche Kommunikation zwischen User/Objekt und Anwendung sowie zwischen einzelnen Workloads angewendet werden.

⚠ Worauf sollte man achten?

Die Bereitstellung von SSE-Technologie hängt vor allem von der Komplexität der Unternehmensumgebung ab. **Daher ist es unerlässlich, Standort, Verhalten und Zugriffsanforderungen der User sowie die Anwendungsanforderungen einschätzen zu können**. Außerdem gibt es in bestimmten Ländern wie China aufgrund von Internetkontrollen besondere Schwierigkeiten hinsichtlich der Performance, die auch durch flexible Bereitstellungsmodelle nicht gelöst werden können. Der SSE-Anbieter sollte innovative Lösungen zur Bewältigung dieser Herausforderungen bereitstellen.

Ergebnisse:

Richtig eingesetzt bieten diese flexiblen, vielfältigen und skalierbaren Optionen einem Unternehmen alle Vorteile der Security Service Edge, unabhängig davon, wo sich User oder Objekte befinden oder wo Anwendungen gehostet werden, und erhöhen den Schutz sogar innerhalb der Anwendung:

- Der Vorteil eines einzigen SSE-Anbieters, der diese umfassenden Schutzmaßnahmen bereitstellt, besteht darin, dass die Verwaltung über eine zentrale Steuerungsebene erfolgt, wobei Unternehmensrichtlinien einheitlich und dynamisch auf jegliche Kommunikation zwischen User/Objekt und Anwendung sowie zwischen einzelnen Workloads angewendet werden
- Auftragnehmer und Mitarbeiter können flexibler arbeiten, da die Schutzmaßnahmen für verwaltete Geräte auf nicht verwaltete Privatgeräte (BYOD) und den Zugriff von externen Usern ausgeweitet werden
- Workload-to-Workload-Sicherheit bietet DevOps- und CloudOps-Ingenieuren denselben Zero-Trust-Schutz für Anwendungen, die auf andere Workloads, andere Clouds oder das Internet zugreifen

#5 Fehler

Auswahl einer SSE-Lösung, die eine mittelmäßige User Experience bietet, da die Anwendungskonnektivität nicht optimiert wird oder Beeinträchtigungen der User Experience nicht diagnostiziert werden

Stattdessen empfiehlt sich die Auswahl einer Lösung, die folgende Voraussetzungen erfüllt:

- Eine SSE-Lösung, die transparenten Einblick sowie unkomplizierte Authentifizierungsoptionen bietet und ständig aktiv ist. Nur so lässt sich eine objektiv messbare positive User Experience für Enduser der SSE-Plattform gewährleisten.
- Eine negative Anwendererfahrung wird den zugrundeliegenden Ursachen zugeordnet, sei es das Endgerät, das Netzwerk, die Anwendung oder der Security-Stack.
- Es gibt Partnerschaften mit Anbietern gängiger SaaS wie Microsoft 365, um die Latenz zwischen der Public Service Edge und dem Netzwerk des Anwendungsanbieters zu minimieren.

Umsetzung durch kompetente SSE-Anbieter

Mithilfe von weltweiten Points of Presence und Peering-Partnerschaften mit verschiedenen Anwendungsanbietern können SEE-Anbieter eine leistungsstarke Alternative zu Backhauling und Hairpinning, die bei herkömmlichen Security-Stacks erforderlich sind, bieten.

Neben diesen architektonischen Vorteilen sind SSE-Anbieter bestens positioniert, um die Anwendererfahrung zu messen und Probleme zu diagnostizieren, da sie auf den Endgeräten der User und im Anwendungsdatenpfad präsent sind. So können SSE-Anbieter die Anwendererfahrung direkt über das Endgerät erfassen und durch die Nutzung der Public-Service-Edge-Infrastruktur detailliertere Diagnose- und Skalierungsoptionen bereitstellen.

Man sollte sich mit SSE-Anbietern auseinandersetzen, die eine Monitoring-Lösung (**Digital Experience Monitoring** oder DEM) in bestehende Agents und Cloud-Infrastruktur integriert haben. Anbieter von Lösungen, für die zusätzliche Agenten erforderlich oder die nur lose integriert sind, stellen nicht im selben Maße Transparenz und Diagnosefunktionen bereit.

Ein SSE-Anbieter muss eine DEM-Lösung mit vielfältigen Funktionen zur Verfügung stellen. Sie sollte umfassende Transparenz und Fehlerbehebung bei Performance-Problemen für alle User und Anwendungen unabhängig von deren Standort bieten. Darüber hinaus sollten Netzwerk-, Sicherheits-, Desktop- und Helpdesk-Teams von kontinuierlichem Monitoring mit Einblick in Probleme hinsichtlich der Performance von Endgeräten, Netzwerken und Anwendungen profitieren. Zudem sollte die Lösung sowohl reaktive Workflows zum Lösen von Support-Tickets als auch proaktive Workflows zur Identifizierung von Makroproblemen (wie z. B. regionale ISP-Ausfälle oder globale Anwendungsausfallzeiten) umfassen. **Diese Funktionen lassen sich mithilfe von Algorithmen realisieren, die auf maschinellem Lernen basieren. Dabei werden normale und ungewöhnliche Anwendererfahrungen nach User, Anwendung, Büro oder Standort erfasst**.

Das Monitoring sollte auf mehreren Ebenen erfolgen, einschließlich Layer 7, um Einblicke in die Antwortzeiten von Webanwendungen zu erhalten, und Layer 3, um das Netzwerkverhalten inklusive Hop-by-Hop-Informationen zu Pfad, Latenz und Paketverlust nachvollziehen zu können. Diese Analyse sollte auch eine Selbstdiagnose der Cloud des SSE-Anbieters beinhalten, um festzustellen, ob und wann der SSE-Hop eine anomale Verzögerung verursacht. Schließlich sollte die Lösung Einblicke in den Zustand des Endgeräts geben und Geräteereignisse identifizieren, die zu einer sinkenden Bewertung führen **(siehe Abbildung 13)**.

SSE-Anbieter sind bestens positioniert, um die Anwendererfahrung zu messen und Probleme zu diagnostizieren, da sie auf den Endgeräten der User und im Anwendungsdatenpfad präsent sind.

Performance-Monitoring und Fehlerbehebung für Microsoft Teams und Zoom

Angesichts der Tatsache, dass Teams und Zoom für viele Unternehmen zur wichtigsten Plattform für Zusammenarbeit und Kommunikation geworden sind, hat auch die Erfassung und Diagnose von Problemen mit der Audio-/Videoqualität noch mehr an Bedeutung gewonnen. DEM-Lösungen sollten mit gängigen UCaaS-Anwendungen wie Zoom und Microsoft Teams kompatibel sein, um Metriken zu Audio- und Videoqualität zu erfassen und detaillierte Hop-by-Hop-Netzwerk- und Endgeräte-Analysen durchzuführen. Durch die Kombination dieser Datensätze sollte die DEM-Lösung Bereiche identifizieren, in denen Qualitätsprobleme auftreten, und deren Ursache ermitteln.

Darüber hinaus sollte die DEM-Lösung mithilfe der Cloud des SSE-Anbieters Telemetrietests über Proxy-Caching durchführen, sodass alle paar Minuten granulare Daten von jedem Enduser erfasst werden können. Dieser Prozess wirkt sich nur minimal auf Anwendungen aus.

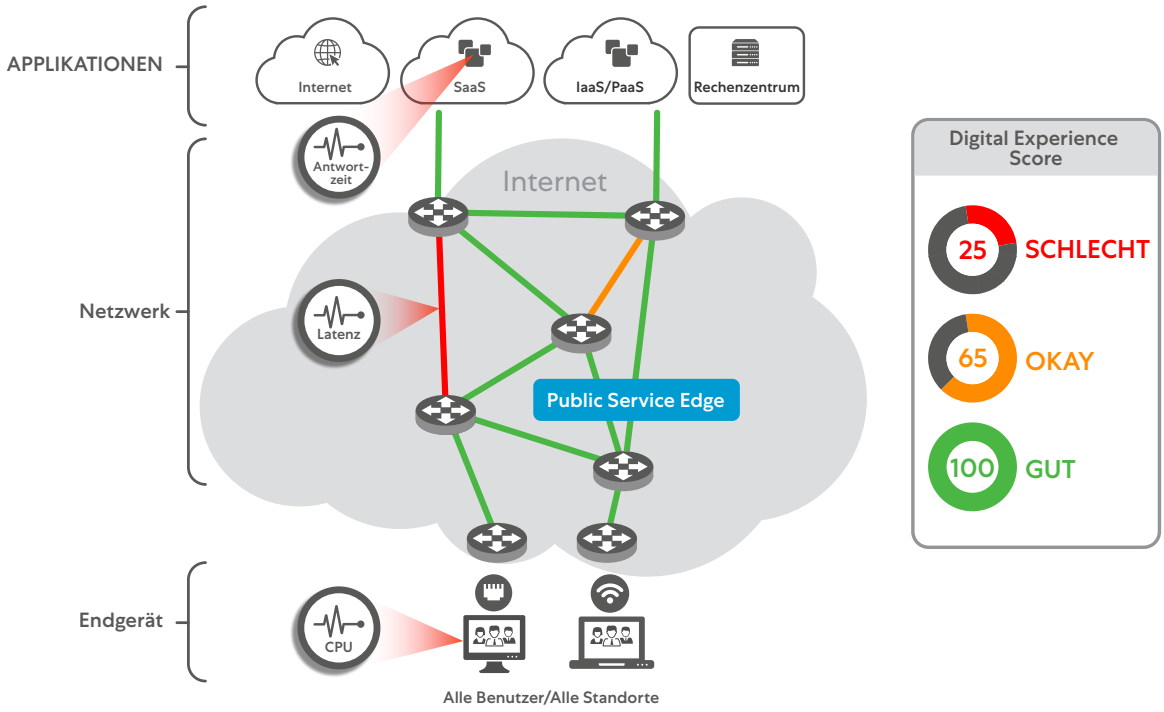

Abbildung 13: Eine in die SSE-Plattform integrierte DEM-Lösung sollte vollständige Transparenz über die Qualität der Anwendererfahrung aus der Perspektive des Endusers bieten und Probleme mit Endgerät, Netzwerk und Anwendung aufzeigen.

Bei älteren rechenzentrumszentrierten Monitoring-Tools, die Metriken von festen Standorten und nicht direkt vom Endgerät erfassen, ist Vorsicht geboten. Dieser Ansatz stellt keinen einheitlichen Überblick über die Performance von Endgerät, Netzwerkpfad oder Anwendung bereit und bietet wenig Transparenz, wenn sich User und Anwendungen nicht im Rechenzentrum oder im Unternehmensnetzwerk befinden. Diese Tools schaffen Informationssilos und teilen keinen Kontext, was zu einem fragmentierten Einblick in die Anwendererfahrung führt und die Fehlerbehebung verzögert. Einzellösungen, die für das Monitoring von Rechenzentren konzipiert wurden, führen zu lückenhafter Transparenz, die sich auf die Erkennung, Behebung und Diagnose von Leistungsproblemen bei Endusern im Internet auswirkt. Im Gegensatz dazu können moderne, in die SSE-Plattform integrierte DEM-Lösungen unzählige Daten erfassen, um Ursachenanalysen durchzuführen (siehe Abbildung 14).

Die DEM-Lösung sollte Bereiche identifizieren, in denen Qualitätsprobleme auftreten, und deren Ursache ermitteln.

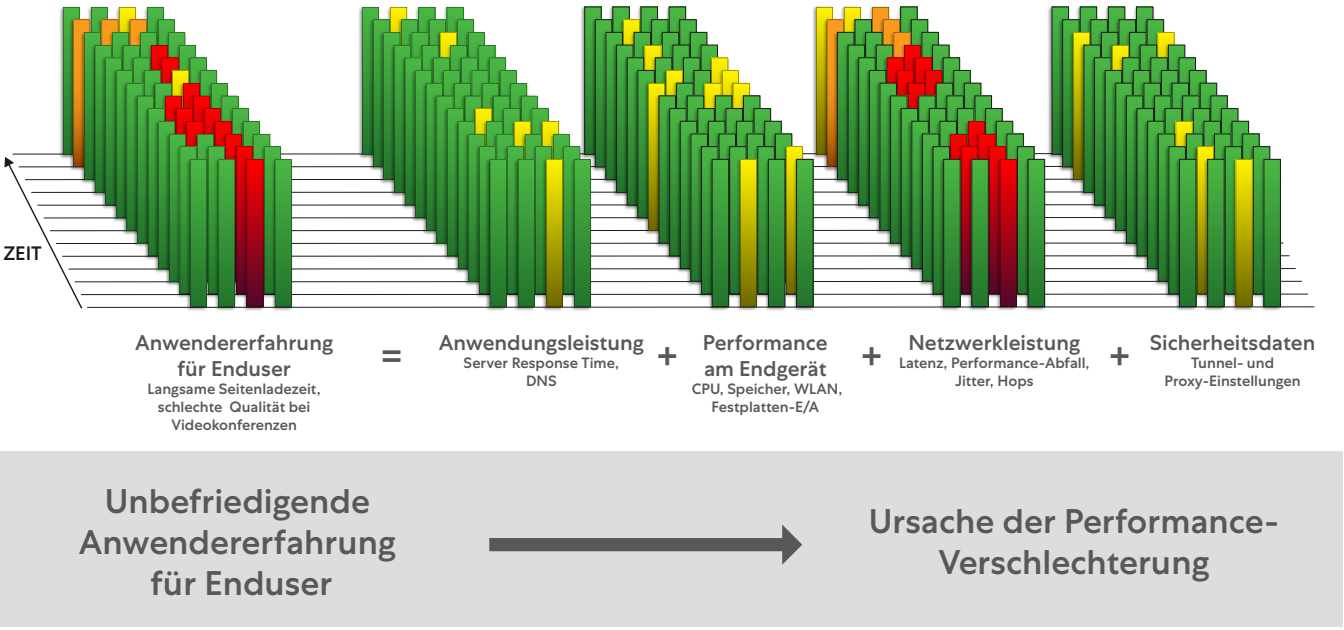

Abbildung 14: Eine in die SSE-Plattform integrierte DEM-Lösung sollte vollständige Transparenz über die Qualität der Anwendererfahrung aus Perspektive des Endusers bieten und Probleme mit Endgerät, Netzwerk und Anwendung aufzeigen.

Optimierte M365-Anwendererfahrung

Eine umfangreiche SSE-Lösung kann mehr als nur die Anwendererfahrung erfassen und Probleme diagnostizieren, um die Leistung gängiger SaaS-Anwendungen wie Microsoft 365 zu optimieren. In den meisten Unternehmen wird der Traffic jedoch zentral durch Hub-and-Spoke-Netzwerke und ExpressRoute geleitet. Darüber hinaus erhöht der User-Traffic von M365 die Netzwerkauslastung um 40 %. Die Infrastrukturen des Internet-Übergangs der meisten Unternehmen sind dieser Aufgabe jedoch einfach nicht gewachsen, sodass die Anwendererfahrung darunter leidet. Microsoft empfiehlt direkte Internetverbindungen und eine Architektur, über die SSE-Anbieter lokale Internet-Breakouts bereitstellen können, um die Performance zu optimieren und Kosten zu senken.

Abbildung 15: Microsoft empfiehlt entsprechend den Grundsätzen von SSE eine direkte Internetverbindung, um Performance und Kosten zu optimieren (Quelle: microsoft.com).

Architektur ist ein wichtiger Aspekt. Die weltweiten Points of Presence des SSE-Anbieters und die Peering-Partnerschaften mit Anwendungsanbietern müssen die Edge näher an die User bringen, um die Verbindungsgeschwindigkeit zu erhöhen und die Latenz bei Zugriffen zu reduzieren. Ein SSE-Anbieter sollte an den meisten großen Knotenpunkten direkte Glasfaserverbindungen zu Microsoft 365 haben, um die Latenzzeit auf ca. 1–2 ms zu reduzieren, die hohe Anzahl langer Verbindungen zu bewältigen und schnelle Dateidownloads sowie eine schnelle DNS-Auflösung mit weniger Hops zu ermöglichen (siehe Abbildung 15).

Besonders M365-Transaktionen sollten mithilfe von SSE-Lösungen geschützt werden, da der Verlust sensibler Daten verhindert werden kann, wenn Anwendungen wie OneDrive und SharePoint überprüft werden. Dadurch wird auch ein vollständiger Audit-Pfad jeglicher Kommunikation zu und von M365-Anwendungen erstellt. Bestimmte M365-Anwendungen wie Teams müssen jedoch möglicherweise nicht überprüft werden, da es sich bei einem Großteil des Traffics um Sprach-/Videodaten über UDP handelt.

⚠ Worauf sollte man achten?

In unserer „Work-from-Anywhere"-Welt gibt es bei der Bereitstellung einer guten Anwendungs-Performance in kabelgebundenen und drahtlosen Netzwerken einige potenzielle Schwachstellen. Selbst mit einer hervorragenden Architektur und speziellen Tools zur Erfassung und Diagnose von Problemen mit der Anwendererfahrung ist es schwierig, diese zu optimieren. Es ist unerlässlich, dafür zu sorgen, dass die Erwartungen der Enduser in Hinblick auf eine angemessene Anwendererfahrung mit kritischen Anwendungen realistisch bleiben. Anhand dieser Erwartungen sollten dann Standards für Monitoring und Management entwickelt werden.

Die Diagnose von Problemen mit der Anwendererfahrung ist eher eine Kunst als eine Wissenschaft. Man benötigt erstklassige Tools und Architekturen, aber auch die richtigen Fähigkeiten, um die Daten interpretieren und auf die Ergebnisse reagieren zu können. Während die von SSE-Anbietern bereitgestellten DEM-Tools die Ursachen der meisten Probleme (zum Beispiel mit WLAN, ISP, Backbone, Endgerät oder DNS) identifizieren, sind bei manchen Problemen weitere Aktionen oder zusätzliche Datensätze erforderlich. So können beispielsweise Protokolle und Paketerfassung nötig sein, um der Ursache auf den Grund zu gehen. Und manche Probleme können überhaupt nicht gelöst werden – was völlig normal ist.

Von der Auswahl eines Anbieters, der den Traffic zur Überprüfung weiterleitet („Hairpinning"), ist abzuraten. Alle Rechenzentren des SSE-Anbieters müssen über Rechen- und Überprüfungskapazitäten verfügen, damit eine möglichst reibungslose User Experience gewährleistet werden kann. In einer Cloud-nativen Architektur darf der Traffic zur Überprüfung nicht an eine Handvoll zentraler Standorte weitergeleitet werden: Angenommen, der User befindet sich in Melbourne, dann sollte die Überprüfung durch entsprechende Services zur Bedrohungsabwehr und Gewährleistung des Datenschutzes lokal erfolgen, statt den Traffic per Backhauling nach Sydney oder Singapur umzuleiten. SSE-Anbieter, die ihre Cloud bei einem Hyperscaler betreiben, müssen sich häufig mit Hairpinning behelfen. Denn wenn der Hyperscaler über 120 Edge-Punkte verfügt, handelt es sich bei 80 Prozent davon wahrscheinlich um Onramp-Services, die lediglich zur Weiterleitung des Traffics an ein Rechenzentrum dienen, wo die SSE-Richtlinien durchgesetzt werden können. Vor der Entscheidung für einen SSE-Anbieter sollte man sich also darüber informieren, wie viele seiner Rechenzentren tatsächlich über die Kapazität zur Durchsetzung von Richtlinien verfügen.

Ergebnisse:

Der Erfolg jeder Transformation – ob Digitalisierung, Netzwerk- oder Sicherheitstransformation – steht und fällt letztlich damit, wie sie sich auf die Anwendererfahrung des Endusers auswirkt. Das eigentliche Ziel besteht bei jedem SSE-Projekt darin, die Anwendererfahrung für Enduser zu verbessern. Zugleich soll das Bedrohungsrisiko reduziert und zuverlässiger Schutz für sensible Daten gewährleistet werden. Im Idealfall sollte die Fähigkeit des Anbieters zur Verbesserung der User Experience mit der DEM-Funktion konkret messbar sein. Wenn durch die Umstellung auf SSE die Notwendigkeit zum Hairpinning an ein Rechenzentrum bzw. zum Einsatz von VPNs entfällt, müssten sich entsprechende Verbesserungen problemlos nachweisen lassen.

- Die SSE-Lösung sollte durch proaktive Überwachung der User Experience auch die Effizienz des Helpdesks optimieren. Im Idealfall können Probleme frühzeitig behoben werden, bevor die User sie überhaupt bemerken und sich beschweren.
- Die SSE-Lösung sollte für Kooperationsplattformen wie Teams und Zoom Echtzeitdaten zur Audio- und Video-Performance liefern.
- Die SSE-Lösung sollte Metriken aus der Anwendungs-, der Endgerät- und der Netzwerkschicht erfassen, um Anomalien zu erkennen und die jeweiligen Ursachen zu ermitteln.
- Der SSE-Anbieter muss die Verbindung zwischen seiner Cloud und gängigen Zugriffszielen wie Microsoft 365 mit möglichst wenigen Hops gewährleisten.

#6 Fehler

Die ausgewählte SSE-Lösung lässt sich nur eingeschränkt mit Drittanbieterlösungen integrieren und orchestrieren

Stattdessen empfiehlt sich die Auswahl einer Lösung, die folgende Voraussetzungen erfüllt:

- Sie kann über robuste APIs mit Produkten anderer führender Anbieter innerhalb des Ökosystems (CSP, SD-WAN, IAM, SOAR/SIEM, EDR usw.) integriert werden, um ein optimales Schutzniveau und eine hervorragende User Experience zu gewährleisten.
- Diese Integrationen werden zur Unterstützung der Automatisierung und Orchestrierung sowie zur Reduzierung der operativen Komplexität und der Betriebskosten genutzt.
- Bei der Lösung darf es sich nicht um ein Portfolio aus Einzelprodukten handeln. Durch die begrenzte Integration zwischen den Einzelprodukten sowie mit Drittanbieter-Lösungen würden zusätzliche technische Schulden verursacht.

Umsetzung durch kompetente SSE-Anbieter

Unternehmen, die sich mit technischen Schulden konfrontiert sehen, wissen, dass diese Problematik überwiegend auf die jahrelange Beschaffung von Technologien unterschiedlicher Anbieter zurückzuführen ist, die nicht miteinander kompatibel sind.

Noch schlimmer ist die vorgebliche „Plattform“ eines einzelnen Anbieters, die nicht wirklich integriert ist, sondern aus einem Sammelsurium von Einzelprodukten besteht, wobei lediglich ein Dashboard für minimale Integration sorgt. Zum Betreiben dieser Plattform sind oft Spezialkenntnisse erforderlich, um ein fragiles Zusammenwirken mit den umgebenden Begleittechnologien zu gewährleisten. Dank einer einheitlichen Cloud-basierten Sicherheitsplattform, die durch einen einzigen Anbieter bereitgestellt wird, kann SSE diese technischen Schulden auf ein Minimum reduzieren. Indes ist auch SSE von einem Ökosystem aus Begleittechnologien (primär anderen Sicherheits-, Netzwerk- und Cloud-Lösungen) umgeben – entsprechend muss die Interoperabilität mit diesen Begleittechnologien für Anbieter hohe Priorität haben **(siehe Abb. 16)**.

Abb. 16: SSE-Anbieter, die keine Integrationen mit einem vielfältigen Ökosystem aus Drittanbietern gewährleisten, lassen ihre Kunden im Regen stehen. Das Ergebnis sind technische Schulden, begrenzte Interoperabilität und ein Security-Stack, der nicht agil, sondern fragil ist.

Zur Gewährleistung einer schnellen, einfachen und sicheren Bereitstellung und Integration muss der SSE-Anbieter Integrationen mit Marktführern in folgenden Bereichen bereitstellen:

- Cloud Service Provider (CSP), sowohl IaaS/PaaS als auch SaaS
- Endpoint Detection and Response (EDR)
- SD-WAN
- Identitäts- und Access-Management (IAM)
- Security Information and Event Management (SIEM)/Security Orchestration, Automation and Response (SOAR)
- Orchestrierungstools

Zur Reduzierung der Komplexität und Betriebskosten und Verbesserung des Sicherheitsstatus müssen diese Integrationen eine Orchestrierung zwischen der SSE-Lösung und Begleittechnologien innerhalb des Ökosystems ermöglichen (siehe Abb. 17).

Cloud Service Providers (IaaS/PaaS und SaaS)

Um die Verlagerung interner Anwendungen in die Cloud bzw. ihre Cloud-native Entwicklung zu unterstützen, muss die SSE-Lösung die Integration mit führenden IaaS/PaaS-Anbietern wie AWS, GCP und Azure ermöglichen, um den Remotezugriff auf diese Anwendungen über Zero Trust zu unterstützen. Dadurch lässt sich gewährleisten, dass diese Anwendungen niemals im Internet exponiert werden und für unbefugte User komplett unsichtbar sind. Statt Remote-Usern Zugang zum Netzwerk zu gewähren, erfolgt der Zugriff auf interne Anwendungen ausschließlich richtlinienbasiert über ausgehende Verbindungen.

Dieser Ansatz gewährleistet Direktverbindungen zur Cloud ohne ein Remote-Access-VPN. Das Unternehmen profitiert von den Skaleneffekten des Cloud-Anbieters sowie von den Vorteilen des Zero-Trust-Modells zur Minimierung der Angriffsfläche, ohne die zusätzliche Komplexität einer Netzwerksegmentierung in Kauf nehmen zu müssen. Ein weiterer Vorteil liegt darin, dass weder virtuelle noch physische Appliances erforderlich sind.

SSE-Anbieter sollten Ein-Klick-Integrationen für gängige SaaS-Anwendungen bereitstellen. Insbesondere sollte die Integration des SSE-Anbieters alle Microsoft-IP-Bereiche und -Domains für gelistete M365-Anwendungen visualisieren und so eine transparente Weiterleitung des Enduser-Traffics an die M365-Cloud ermöglichen. Durch Peering mit Microsoft 365 lässt sich zudem die Roundtrip-Dauer verkürzen, die Skalierbarkeit verbessern und schnellere Dateidownloads und DNS-Auflösung ermöglichen.

Durch Integration von SSE mit anderen SaaS-Anbietern wie ServiceNow lässt sich ein höheres Datenschutzniveau erzielen. Durch Überprüfung von neuen und Bestandsdaten in ServiceNow sollte der SSE-Anbieter die Erkennung sensibler Daten anhand von DLP-Richtlinien unterstützen und ausgehende Uploads von Dateien blockieren, die sensible Daten enthalten. Die Integration ermöglicht die Orchestrierung von Gegenmaßnahmen zur Behebung von Sicherheitsvorfällen in ServiceNow, u. a. durch Aktualisieren mandantenspezifischer Custom Block Lists. Verdächtige IPs, Domains und URLs können ohne manuelle Eingriffe blockiert und Cloud-Fehlkonfigurationen korrigiert werden, um das Risiko von Sicherheitsverletzungen zu verringern.

Endpoint Detection and Response

Der SSE-Anbieter sollte Integrationen mit verschiedenen Partnern für Endgerätesicherheit unterstützen, um Telemetriedaten auszutauschen, die gegenseitige Transparenz zu verbessern und Reaktionen zu orchestrieren. Dadurch wird eine Defense-in-Depth-Strategie zur effektiven und effizienten Implementierung von Zero Trust ermöglicht.

Diese Integration sollte die Möglichkeit bieten, Identität, Standort und Gerätestatus des Users zu bewerten, um die entsprechenden bedingten Zugriffsrichtlinien automatisch zu implementieren. Durch plattformübergreifende Korrelation und Workflows lassen sich Probleme schneller untersuchen und beheben. Das umfasst folgende Kapazitäten:

- Bewertung des Gerätezustands und die automatische Implementierung geeigneter Zugriffsrichtlinien
- Erkennen von Zero-Day-Bedrohungen und Korrelieren mit den Telemetriedaten der Endgeräte, um betroffene Geräte zu identifizieren und einen plattformübergreifenden Quarantäne-Workflow einzuleiten
- Untersuchung von Bedrohungen anhand von Kontextdaten zu Endgeräten und Netzwerk zur Unterstützung einer effektiven Erkennung und Entscheidungsfindung

SD-WAN

Um das Routing von Zweigstellen-Traffic und die Einrichtung lokaler Internet-Breakouts zu vereinfachen, sollte die SSE-Lösung mit SD-WAN-Anbietern integrierbar sein.

Die gemeinsame SSE-/SD-WAN-Lösung ermöglicht schnellen, sicheren, auf Richtlinien basierenden Zugriff auf das Internet und geschäftskritische Anwendungen und gewährleistet jederzeit identischen Schutz für alle User bei sämtlichen Verbindungen zu Cloud-Applikationen und zum offenen Internet. SD-WAN-Lösungen lassen sich über eine API-Integration mit SSE integrieren. Mit dieser kombinierten Lösung können Zweigstellen jeden Anstieg von Cloud- und Internet-Traffic ohne Backhauling zur zentralen DMZ im Rechenzentrum bewältigen, indem sie eine hybride WAN-Architektur zur Netzwerktransformation in Kombination mit robuster Sicherheit einsetzen.

Dabei ist zu beachten, dass SSE-Lösungen netzwerkunabhängig sein müssen und nicht exklusiv an eine bestimmte Underlay-Lösung gebunden sein dürfen. Tatsächlich liegen die Vorteile von SD-WAN eher in den softwaredefinierten Komponenten und weniger im Wide Area Network selbst. Letzteres erweitert das Unternehmensnetzwerk und erhöht das Risiko einer lateralen Ausbreitung von Bedrohungen. Bei der Auswahl des SSE-Anbieters sollten die Gründe für die Erweiterung des Unternehmensnetzwerks zur Zweigstelle sorgfältig gegenüber den inhärenten Risiken abgewogen werden. Es empfiehlt sich, Alternativen (z. B. reine Internet-Zweigstellen) in Betracht zu ziehen, die mehr Sicherheit gewährleisten.

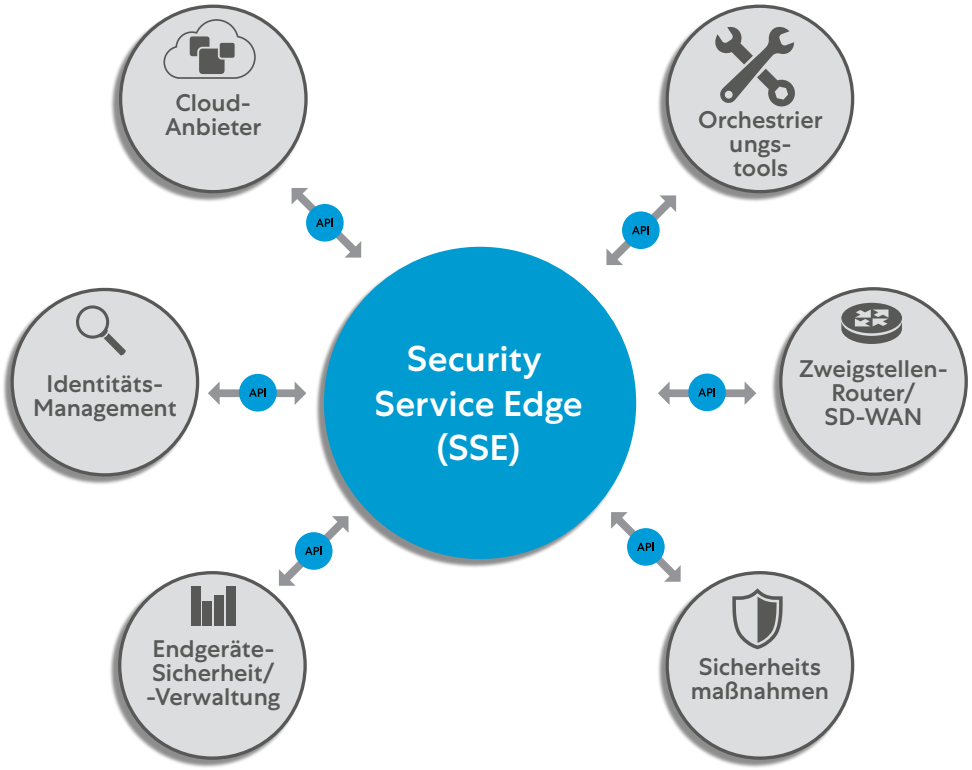

Abb. 17: SSE-Lösungen sollten mit marktführenden Anbietern in verschiedenen Bereichen integrierbar sein.

Identitäts- und Access-Management

SSE-Lösungen sollten Integrationen mit IAMs ermöglichen, um Zero-Trust-Zugriff basierend auf dem Sicherheitsstatus des jeweiligen Endgeräts durchzusetzen und unternehmensweit zuverlässigeren Schutz vor Bedrohungen zu gewährleisten.

Mithilfe von Standards wie Security Assertion Markup Language (SAML) sollte sich die Integration unkompliziert bereitstellen lassen. Dadurch wird sowohl die Authentifizierung von Usern als auch die Absicherung von Verbindungen zum Internet und der Zugriff auf interne Anwendungen unterstützt. Das IAM verwaltet den User-Zugriff auf Anwendungen durch eine Kombination aus SSO und MFA, während die SSE-Lösung die Verbindung absichert. Durch die Unterstützung des SCIM-Protokolls (System for Cross-Domain Identity Management) ist gewährleistet, dass User-Daten zwischen beiden Systemen synchronisiert werden. Dies betrifft insbesondere Änderungen an User-Gruppen oder Job-Rollen sowie die Löschung von User-Konten bei Verlassen des Unternehmens.

SIEM und SOAR

Zur Unterstützung eines effizienten und effektiven Risiko- und Compliance-Managements mit erweiterten Informationen und Automatisierung sollte die SSE-Lösung Integrationen mit SIEM- und SOAR-Anbietern ermöglichen.

SSE-Lösungen müssen zudem die Option bieten, Log-Daten nahezu in Echtzeit sowohl an lokal installierte als auch Cloud-basierte SIEM/SOAR-Lösungen zu senden. Dadurch wird die Korrelation von Protokollen aus mehreren Quellen erleichtert und die netzwerkübergreifende Analyse von Traffic-Mustern unterstützt. Darüber hinaus müssen Unternehmen die Möglichkeit haben, die Weblog-Daten im SIEM für erweiterte historische Analysen zu verwenden (> 6 Monate). Mittels lokaler Log-Archivierung lässt sich zudem die Einhaltung gesetzlicher Vorgaben sicherstellen.

Orchestrierungstools

Neue Ansätze wie Infrastructure as Code (IaC) und DevSecOps machen zunehmend eine „Shift Left"-Strategie erforderlich, d. h. Sicherheitsprozesse werden in eine frühere Phase des Entwicklungszyklus vorgezogen. Diesem Trend müssen SSE-Anbieter Rechnung tragen und entsprechende APIs für die Orchestrierung bereitstellen. Dies gilt insbesondere für interne Anwendungen, bei denen die durch Orchestrierungsskripte wie Ansible oder Terraform ermöglichte Instanziierung des Zero-Trust-Zugriffs in den Zyklus der Anwendungsbereitstellung integriert ist, und zwar vor allem für Segmentierungen zwischen User und Anwendung bzw. zwischen zwei Workloads. Durch diese Orchestrierung lassen sich Zero-Trust-Funktionen mit den von Softwareentwicklern verwendeten agilen Methoden in Einklang bringen.

Neue Ansätze wie Infrastructure as Code (IaC) und DevSecOps machen zunehmend eine „Shift Left"-Strategie erforderlich, d. h. Sicherheitsprozesse werden in eine frühere Phase des Entwicklungszyklus vorgezogen. Diesem Trend müssen SSE-Anbieter Rechnung tragen und entsprechende APIs für die Orchestrierung bereitstellen.

⚠ Worauf sollte man achten?

Bei der Auswahl einer SSE-Lösung sind verschiedene Faktoren zu berücksichtigen: Wie tief sind die API-Integrationen? Wie häufig werden Updates verfügbar gemacht? Zudem müssen die zuständigen Entscheidungsträger die Marktlage im Auge behalten: Zeichnen sich Trends ab, die zukünftigen Integrationen im Wege stehen könnten (z. B. die Übernahme eines Anbieters durch einen Mitbewerber)? Auch ein etwaiger Fachkräftemangel im eigenen Unternehmen könnte hier ins Gewicht fallen, da die Implementierung dieser Integrationen – erst recht mit Legacy-Tools – spezielle Kenntnisse erfordert.

Ergebnisse:

SSE-Anbieter, die umfassende API-basierte Drittanbieter-Integrationen bereitstellen, unterstützen Effizienzgewinne, die sich aus der Möglichkeit ergeben, führende Lösungen zu orchestrieren und das Risiko einer Anbieterbindung zu reduzieren:

- SSE-Anbieter, die Integrationen mit führenden Akteuren innerhalb des Ökosystems anbieten (wie CSPs, SD-WAN, IAM, SOAR/SIEM, EDR usw.), machen ihre Technologie zukunftssicher und bauen technische Schulden ab.
- Ein orchestriertes Ökosystem aus integrierten Anbietern reduziert betriebliche Komplexität und Kosten und kann zur Vermeidung von Bedienfehlern beitragen.
- SSE-Anbieter, die ein Lösungsportfolio aus Einzelprodukten quasi „zusammenkaufen", hinken oft bei der Produktinnovation hinterher und bieten nur unzureichende Interoperabilität mit Drittanbietern.

#7 Fehler

Der Geschäftsnutzen der ausgewählten SSE-Lösung lässt sich in einer Testumgebung schwer nachweisen

Stattdessen empfiehlt sich die Auswahl einer Lösung, die folgende Voraussetzungen erfüllt:

- Sie muss sich reibungslos mit einem einheitlichen Agent steuern lassen und über eine zentrale, benutzerfreundliche Grafikoberfläche Zugriff auf einen global verfügbaren Satz von Service Edges (in User-Nähe) bieten.
- Die zahlreichen Komponenten der SSE-Plattform müssen sich im Pilotlauf mit minimalem Zusatzaufwand bereitstellen lassen.
- Der SSE-Anbieter kann überzeugend nachweisen, dass seine Lösung nach der vollständigen Bereitstellung mit minimalem Nachbearbeitungsaufwand wie vorgesehen funktionieren wird.

Abb. 18: Bei der Probefahrt darf kein Spielzeugmodell zum Einsatz kommen. Der tatsächliche Geschäftsnutzen einer SSE-Lösung lässt sich nur durch einen Pilotlauf in einer Produktivumgebung nachweisen.

Umsetzung durch kompetente SSE-Anbieter

Die Umstellung auf eine SSE-Plattform erfordert, dass das Unternehmen seine gesamte Sicherheitsarchitektur umstrukturiert. Die Entscheidung für den richtigen SSE-Anbieter muss daher gründlich durchdacht werden. Ein ausschlaggebender Faktor ist dabei die Gewissheit, dass die ausgewählte SSE-Lösung in der Produktivumgebung des Unternehmens einwandfrei funktioniert. Ob bzw. inwieweit der Anbieter dies überzeugend nachweisen kann, sagt einiges über die Architektur der Plattform aus.

Als weiteres Auswahlkriterium sollte auch berücksichtigt werden, welche Schritte konkret zur Ausführung des Pilotlaufs erforderlich sind. Ein geeigneter SSE-Anbieter würde zunächst den optimalen Weg zur Weiterleitung des Traffics zur SSE Service Edge ermitteln. Von dort aus übernimmt dann die eigene Cloud des SSE-Anbieters die weitere Verbindung. Der damit verbundene Aufwand sollte sich für den SSE-Administrator in Grenzen halten und neben Authentifizierung und Reporting im Wesentlichen darauf beschränkt sein, den Weiterleitungsmechanismus einzurichten und grundlegende Richtlinien zu konfigurieren. Die Konfiguration erweiterter Richtlinien nimmt selbstverständlich mehr Zeit in Anspruch.

Der Pilotlauf sollte den Nutzen der Lösung anhand einer Reihe von Geschäftsergebnissen nachweisen und Mitarbeiter aus mehreren Teams einbeziehen (insbesondere aus den Bereichen IT-Sicherheit und Netzwerkarchitektur sowie Desktop-Experten, die z. B. für die Installation der Endgeräte-Agents zuständig sind). Die aktive Mitwirkung dieser Mitarbeiter sollte jedoch auf ein Minimum reduziert sein – schließlich handelt es sich um die Evaluierung im Vorfeld der Anschaffung einer SaaS-Lösung. Von SSE-Lösungen, die eine intensive Mitwirkung insbesondere von Netzwerkteams erfordern, um komplexe Routing-Szenarien in einem Pilotlauf zu bewältigen, ist abzuraten.

Bei der Planung eines aussagekräftigen Pilotlaufs für eine SSE-Lösung empfiehlt sich ein sequenzieller Ansatz, der den Geschäftszielen des Unternehmens entspricht:

Alle aufgeführten Schritte sollten für den SSE-Anbieter problemlos innerhalb kurzer Zeit (nach Möglichkeit innerhalb einiger Tage) und ohne größere Routing- oder Konfigurationsänderungen zu bewältigen sein. Der SSE-Anbieter sollte in der Lage sein, im Rahmen eines unkomplizierten, aber souverän ausgeführten Pilotlaufs den Geschäftsnutzen der Plattform nachzuweisen. Für die eigentliche Bereitstellung werden dann weitere Schritte erforderlich: die Konfiguration erweiterter Richtlinien, Optionen für verschiedene Anwendungen und Endgeräte, Integrationen und Zusammenwirken mit anderen Agents/Technologien usw.

Entsprechend den bereits dargelegten Handlungsempfehlungen muss der SSE-Anbieter im Zuge des Pilotlaufs folgende Nachweise erbringen:

- **Globale Cloud-Infrastruktur mit minimaler Latenz für den Enduser mit hoher Verfügbarkeit und Performance.** Der Anbieter sollte seine Fähigkeit nachweisen, diese Cloud auch bei hohem Datenvolumen zu betreiben, sowie die Wirksamkeit seiner Failover-Maßnahmen.
- **Zero-Trust-Schutz für alle User-Sitzungen**, sowohl für Verbindungen zu privaten als auch zu öffentlichen Anwendungen sowie Kommunikationen zwischen Workloads (sofern im Rahmen des Pilotlaufs erforderlich).
- **Schutz vor komplexen Bedrohungen und erweiterte DLP durch Überprüfung des verschlüsselten Traffics**. Möglicherweise sind in der Pilotphase weitere Schritte zur Verwaltung von Zertifikaten erforderlich. Die Fähigkeit eines SSE-Anbieters, SSL/TLS-Überprüfung mit minimaler zusätzlicher Latenz durchzuführen, stellt jedoch ein aussagekräftiges Differenzierungsmerkmal dar.
- **Flexible Bereitstellungsoptionen**. Möglicherweise kann dieser Nachweis im Pilotlauf nicht erbracht werden. In jedem Fall sollte der SSE-Anbieter einen Plan für die Absicherung sämtlicher User – unabhängig vom Standort oder Gerät – vorlegen. Dies kann auch die Bereitstellung von Private Service Edges bzw. Cloud Browser Isolation für Auftragnehmer beinhalten. Ausschlaggebend ist der überzeugende Nachweis des SSE-Anbieters, dass seine Bereitstellungsmodelle den Anforderungen geografisch distribuierter User und Anwendungen gerecht werden.

- **Optimale Anwendererfahrung**. Hier wird sowohl die Benutzerfreundlichkeit der Plattform selbst bewertet (z. B. die User Interface des Agents) als auch im weiteren Sinne die Anwendererfahrungen beim Zugriff auf öffentliche und private Anwendungen über die Plattform. Der Anbieter sollte die Fähigkeit zur Messung und Diagnose verschiedener Performance-Probleme aus der Perspektive des Endusers (WLAN, ISP, CPU usw.) nachweisen. Die entsprechenden Funktionen sollten direkt in die SSE-Plattform integriert sein, ohne dass zusätzliche Agents bereitgestellt werden müssen.
- **Integration mit Drittanbietern**. Auch dieser Nachweis kann unter Umständen während des Pilotlaufs nicht erbracht werden. Der SSE-Anbieter sollte jedoch Methoden zur Integration von Protokolldaten in ein externes SIEM-Tool bzw. eine Integration mit einem vorhandenen EDR-Tool bereitstellen. Basierend auf einer Analyse des vorhandenen Tool-Ökosystems sollte der Anbieter Empfehlungen für zukünftige Integration in der eigentlichen Bereitstellungsphase geben.

Angesichts des akuten Fachkräftemangels in der Branche empfiehlt sich die Auswahl einer SSE-Lösung, deren Bereitstellung und Verwaltung mit möglichst geringem Aufwand verbunden ist.

Eine SaaS-Sicherheitslösung hat den Vorteil, dass der SSE-Anbieter Aufgaben übernimmt, die sonst in die Zuständigkeit interner Mitarbeiter fallen. Der Pilotlauf sollte Auskunft darüber geben, wie hoch der Aufwand für die Bereitstellung, Verwaltung und regelmäßige Aktualisierung der SSE-Lösung ist.

⚠ Worauf sollte man achten?

- In der Pilotphase ist es nicht möglich, sämtliche Eventualitäten zu testen, daher können bei der eigentlichen Bereitstellung unvorhergesehene Probleme auftreten.
- Entsprechend empfiehlt sich die Auswahl eines kundenorientierten SSE-Anbieters, der die Bereitschaft zeigt, etwaige Probleme bei der Bereitstellung zu bewältigen.
- Im Pilotlauf lässt sich in der Regel weder die Skalierbarkeit der betreffenden Lösung prüfen, noch erhält der Kunde einen realistischen Eindruck davon, wie der Anbieter auf Pannen reagiert. SSE-Anbieter können während des Pilotlaufs schwerwiegende Netzwerk- oder Routing-Probleme vermeiden, die sich womöglich erst während der Bereitstellung zeigen. Daher empfiehlt sich die Entscheidung für einen Anbieter, dessen Lösung nicht auf Netzwerkrouten angewiesen ist.
- Als weiterer Faktor ist der jeweils erforderliche Verwaltungsaufwand zu berücksichtigen – welche Aufgaben fallen in die Zuständigkeit des Unternehmens, welche in die des Anbieters? In die Berechnung muss sowohl der Aufwand für die Bereitstellung in der Produktivumgebung als auch für die laufende Verwaltung der Lösung einbezogen werden.
- Nicht alle SSE-Anbieter stellen ihre Lösung tatsächlich als SaaS bereit. Bei der Entscheidung für eine SSE-Lösung ist unbedingt darauf zu achten, dass die Gesamtbetriebskosten möglichst niedrig sind – dies gilt erst recht angesichts des eklatanten Mangels an IT-Fachkräften, mit dem viele Unternehmen zu kämpfen haben.

Ergebnisse:

Ein aussagekräftiger Pilotlauf erbringt den Nachweis, dass sich die SSE-Lösung einfach bereitstellen lässt, in der Produktivumgebung einwandfrei funktioniert und die jeweiligen Zielvorgaben des Unternehmens erfüllt

- Ein reibungsloser Pilotlauf der Lösung ist ein guter Indikator für eine erfolgreiche Bereitstellung. Im Hinblick auf das Ziel möglichst geringer Gesamtkosten sind mehrere Faktoren zu berücksichtigen, die den laufenden Wartungsaufwand reduzieren. Insbesondere zählt dazu ein einheitlicher Agent, Zugriff auf global distribuierte Service Edges und eine zentrale, einfach zu bedienende Benutzeroberfläche. Jede groß angelegte Implementierung ist mit Zeit- und Arbeitsaufwand verbunden. Jedoch lässt sich dieser Aufwand durch die Auswahl des richtigen Partners für die Zusammenarbeit beträchtlich reduzieren.
- Hinsichtlich Architektur und Design sollte eine SSE-Lösung so ausgelegt sein, dass sich ihr Funktionsumfang mit minimalem Implementierungsaufwand (z. B. zusätzliche Agents oder VMs) problemlos erweitern lässt. Dadurch wird dem Kunden eine phasenweise Umstellung auf SSE ermöglicht, wobei der Wechsel von einer Phase zur nächsten mit überschaubarem Aufwand verbunden ist.
- Letztlich kommt es darauf an, inwieweit der SSE-Anbieter überzeugend nachweisen kann, dass sich seine Lösung in der Produktivumgebung reibungslos bereitstellen lässt – und dass das Unternehmen sich auf seine Unterstützung verlassen kann, wenn doch einmal eine unvermeidliche Panne auftritt. Um zu gewährleisten, dass sich die Investitionen in die Transformation der Sicherheits- und Netzwerkarchitektur lohnen, sollte man sich für einen kundenorientierten Anbieter entscheiden, dessen Architektur sich bereits in der Praxis bewährt hat.

Kundenstimmen und Fallbeispiele

Abrupte Paradigmenwechsel, die massive Investitionen aufgrund einer Neuorientierung sinnvoll machen, sind sehr selten. Insofern will auch das Vorgehen zur Bereitstellung von SSE gut durchdacht sein. Der Anwendungsbereich für unternehmensfähiges SSE (öffentlich zugänglich über https://trust.zscaler.com) unter Einbeziehung sämtlicher denkbarer User, Server, Geräte usw. wird im Abschnitt zum 2. Fehler abgesteckt. Im Folgenden wird anhand mehrerer Kundenbeispiele veranschaulicht, wie eine erfolgreiche Umstellung auf SSE aussehen kann:

Kundenbeispiel A:

Die SSE-Plattform von Zscaler wurde zur Bereitstellung von Zero-Trust-Kontrollen für folgende Bereiche eingesetzt:

- Granularer Enduser-Zugriff auf private Services
- Internet-Sicherheit für Enduser, einschließlich Inline-Überprüfung und Datenschutz
- Netzwerktransformation mit kompletter Entfernung der User aus dem Netzwerk
- Schutz von Workloads, Internet und Private Access
- Einschränkung des Zugriffs für externe Dritte

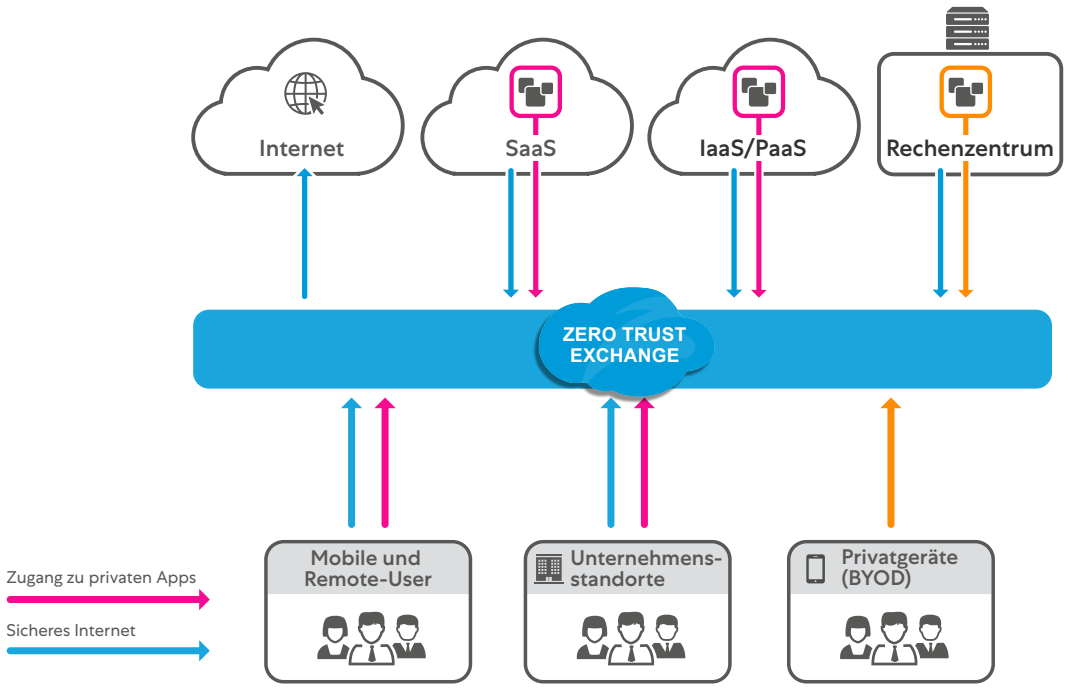

Abb. 19: Absicherung von Verbindungen zu Unternehmensressourcen mit Zscaler (Überblicksdarstellung)

„In nicht einmal fünf Tagen haben wir 20.000 Mitarbeiter reibungslos, sicher und kostengünstig auf WFA umgestellt, indem wir VPNs durch die Zero-Trust-Netzwerkzugriffslösung von Zscaler ersetzten."

Michael Alvmarken, Service Manager for Cybersecurity and Technology, Sandvik Group

„Durch die Nutzung der Cloud-Infrastruktur von Zscaler und der nativen Integration mit ZIA und ZPA erhalten wir optimale datengestützte Erkenntnisse zur Performance aus Sicht der Enduser."

John Dawes, Director Enterprise Architecture, Reckitt Benckiser

„Indem wir auf das Backhauling unseres Traffic verzichten und stattdessen das Internet direkt nutzen, können wir unsere Kosten voraussichtlich um 70 % senken."

Frederik Janssen, VP Global IT Infrastructure Portfolio, SIEMENS

Kundenbeispiel B:

- Die SSE-Plattform von Zscaler wurde zu folgenden Anwendungszwecken eingesetzt:
- Vollständige Transparenz für den Zugriff auf alle Internet-Services (in und außerhalb der Cloud)
- Vollständige Inline-Kontrolle zur Reduzierung der Verluste von geistigem Eigentum des Unternehmens
- Digital Experience Monitoring des User-Zugriffs für Mitarbeiter im Homeoffice

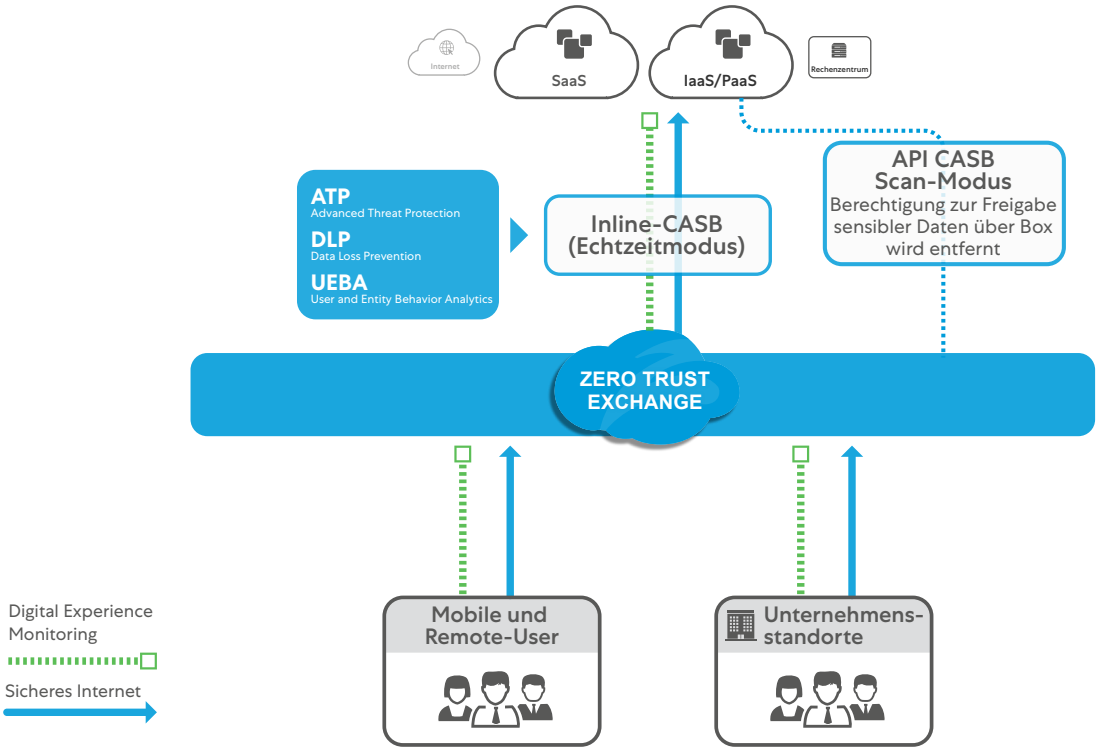

Abb. 20: Inline-Überprüfung und Digital Experience Monitoring mit Zscaler (Beispiel)

ciena

„Wir betrachten Zscaler Digital Experience als unverzichtbare Voraussetzung für die Produktivität unserer Remote-Mitarbeiter. Früher waren wir schon froh, wenn wir 25 % der User-Probleme lösen konnten. Heute nutzen wir ZDX als Ausgangspunkt zur Behebung aller Probleme mit der User Experience und schaffen es in 95 % der Fälle, die Ursache zu identifizieren."

Ed DeGrange, Principal Security Architect, Ciena

SIEMENS

„Sicherheitsverletzungen auf der Website haben ebenso finanzielle Konsequenzen wie beispielsweise Wirtschaftsbetrug oder Handelsprobleme. Deswegen ist IT-Sicherheit ein betriebswirtschaftlich relevantes Thema."

Frederik Janssen, VP Global IT Infrastructure Portfolio, SIEMENS

BOMBARDIER

„Mit der Advanced Cloud Sandbox von Zscaler ist der Arbeitsaufwand für die IT sehr gering. Angesichts der angespannten Lage auf dem Fachkräftemarkt ist das ein entscheidendes Kriterium."

Mark Ferguson, CISO, Bombardier

Kundenbeispiel C:

Die SSE-Plattform von Zscaler wurde zur Bereitstellung granularer Schutzmechanismen für Nicht-IT-Services eingesetzt:

- Zero-Trust-Zugriff auf Betriebstechnologie für Mitarbeiter und externe Dritte
- OT zu Workload
- Cloud zu Workload

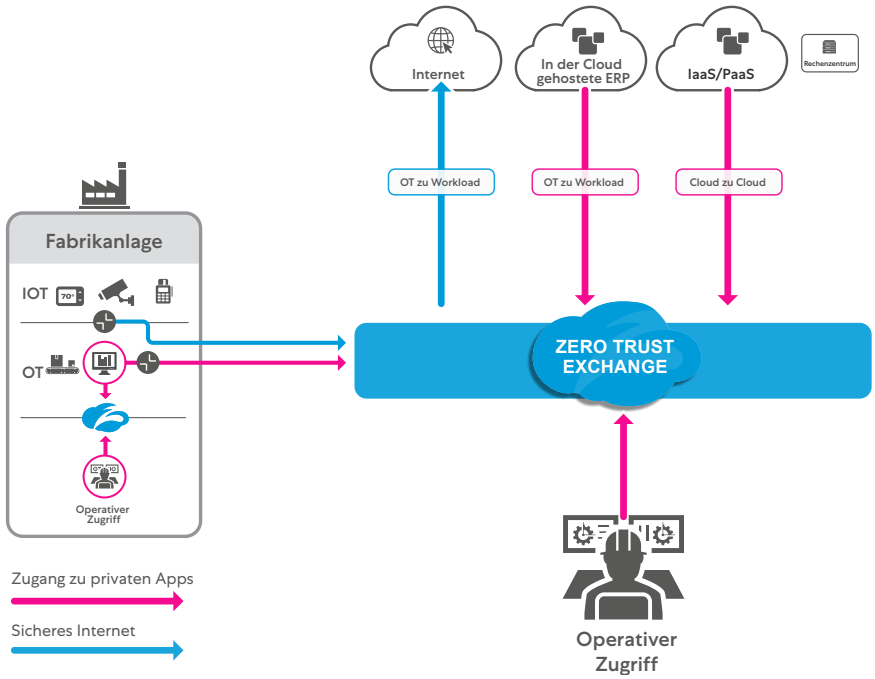

Abb. 20: Inline-Überprüfung und Digital Experience Monitoring mit Zscaler (Beispiel)

Wichtige Schlussfolgerungen

Der Anbieter muss ein schriftliches SLA vorlegen, das bei Verlust oder Verschlechterung der Servicequalität greift.

Die SSE-Lösung muss die Durchsetzung von Richtlinien an allen Standorten ermöglichen – inline, weltweit und in Carrier-neutralen Rechenzentren von Peering-Partnern –, um zu gewährleisten, dass Kunden immer über den effektivsten Pfad verbunden werden.

Der SSE-Anbieter muss Zero-Trust-Kontrollen für alle befugten User, Workloads und Geräte über sämtliche Protokolle bereitstellen.

Die SSE-Lösung muss Services netzwerkunabhängig bereitstellen.

Der SSE-Anbieter muss seine Inline-Überprüfung über eine Proxy-Cloud-Architektur bereitstellen, die minimale Latenzzeiten gewährleistet und eine vollständige Transparenz des gesamten Web-Traffics (bis einschließlich TLS 1.3) ermöglicht.

Die SSE-Lösung muss mehrere Sicherheitskontrollen über eine Single-Pass-Architektur bereitstellen, bei der Pakete einmal im Speicher abgelegt und gescannt werden – so lassen sich Skalierbarkeit und Entschlüsselung auch bei hohem Datenvolumen realisieren.

Der SSE-Anbieter muss seine Lösung zentral verwalten und verschiedene Bereitstellungsoptionen anbieten, um unterschiedlichen Kundenstandorten in verschiedenen Regionen gerecht zu werden sowie kundenspezifische Funktionsanpassungen zu ermöglichen.

Die SSE-Lösung muss sich so erweitern lassen, dass sie für den Zugriff über nicht verwaltete Enduser-Geräte (BYOD, externe Dritte und Geschäftspartner) ein identisches Niveau an granularer Kontrolle gewährleistet wie für interne Mitarbeiter.

Der SSE-Anbieter muss die Anwendererfahrung durch Digital Experience Monitoring und Diagnose von Performance-Problemen bei Teams, Zoom und anderen geschäftskritischen Services optimieren.

Die SSE-Lösung sollte Metriken aus der Anwendungs-, der Endgerät- und der Netzwerkschicht erfassen, um Anomalien zu erkennen und den Support-Teams aussagekräftige Erkenntnisse bereitzustellen.

Der SSE-Anbieter muss durch Integrationen mit führenden Akteuren innerhalb des Ökosystems (wie CSPs, SD-WAN, IAM, SOAR/SIEM, EDR usw.) eine umfassende Kontrolle und Sicherheit für sämtliche Unternehmensbereiche gewährleisten.

Die SSE-Lösung muss mit diesen Anbietern integriert werden, um eine Orchestrierung zur Minimierung des Betriebsaufwands zu ermöglichen.

Der SSE-Anbieter muss bei einem Pilotlauf nachweisen können, dass die Bereitstellung aller für den laufenden Betrieb erforderlicher Funktionen und Standorte problemlos möglich ist.

Die SSE-Lösung muss sich unkompliziert und ohne Installation zusätzlicher Hardware oder Agents erweitern lassen, damit Unternehmen ihre SSE-Deployments phasenweise ausbauen können.

Weitere Informationen zu SSE unter Zscaler SSE 2022

Zu den Verfassern:

Sanjit Ganguli (VP, Transformation Strategy/Field CTO) und Nathan Howe (VP, Emerging Technology und 5G) haben sich als führende Experten im Bereich Cloud-Sicherheit, Transformation und neue Technologien etabliert. Aus langjähriger globaler Berufserfahrung u. a. bei Gartner, Nestle, Riverbed und Verizon zeigen sie innovative Perspektiven zu hochakuten Themen auf.