

WHITE PAPER

Rethinking Enterprise SD-WAN with Zero Trust

SPONSORED BY





TRADITIONAL ENTERPRISE NETWORKS HAVE REACHED A BREAKING POINT. Fast-growth technologies, such as AI, big data and IoT, stress both the hub-and-spoke architecture of traditional networks and the castle-and-moat cybersecurity approach used to protect critical resources.

At the same time, the enterprise edge is sprawling to encompass everything from work-from-home (WFH) employees to autonomous robots to remote sensor networks in extreme locations such as on oil rigs or in mines. As the edge expands, the attack surface for new waves of malware and zero-day attacks expands right along with it.

To cope with these challenges, many enterprises have deployed cloud-based WAN technologies, typically SD-WANs, along with some managed security services. These approaches have proven to be insufficient.

What modern, digital-dependent enterprises don't need is another quick-fix, temporary solution built on top of obsolete paradigms. What's needed is a new way of handling networking and security that prioritizes the protection of sensitive data without hurting application performance, impeding the productivity of workers or expanding the enterprise attack surface.

This paper will investigate a new platform approach to enterprise networking and security, one that extends zero-trust security to all aspects of your network. In this white paper, you will learn:

- **Why traditional networking and security paradigms fail to meet the demands of AI, IoT, hybrid work and more.**
- **How hackers exploit traditional networking and security architectures to move laterally throughout organizations.**
- **What solutions enterprises need to deliver real-time insights to use cases such as AI, IoT and big data.**
- **Why a platform approach to networking and zero-trust security is the right way to counter evolving threats.**


INTRODUCTION:

The traditional enterprise perimeter is under siege

IT'S NO SECRET THAT TRADITIONAL PERIMETER CYBERSECURITY ARCHITECTURES ARE NOT KEEPING PACE WITH THE MODERN THREAT ENVIRONMENT. Hybrid and WFH employment models, digital transformation and ongoing cloud migrations have upended the perimeter-based security paradigm, with many mission-critical applications and core workloads residing in a combination of public and private clouds. Users typically access these applications over the public internet (which IT has no control over) on personal devices (which IT has no control over) from any location (which may or may not be safe).

In the past, sensitive resources were accessed only on enterprise LANs, where physical security eliminated many threats. Implicit trust was built into the concept of the LAN, and once you were inside the perimeter you were considered vetted and were free to move about the internal network at will. Under the traditional network and security paradigm, branch offices were connected via expensive and difficult-to-maintain private WANs, such as MPLS. When workers were remote, they relied on site-to-site VPN connections, which added protection but undermined productivity and raised costs.

Now, both the edge and the people who access mission-critical enterprise resources are, more often than not, located outside of perimeter protections. As recent high-profile breaches have shown, implicit trust leads to explicit risks.



A ransomware attack will hit every 2 seconds, costing victims \$265B annually.

At the same time, attackers now have a variety of new weapons at their disposal. AI, automation, rental botnets and cheap malware that's available on the dark web both increase the number of attacks and make those attacks more damaging.

In 2023, for instance, ransomware attacks alone increased by over 37%, according to the [Zscaler 2023 ThreatLabz State of Ransomware](#) report. On average, attackers demanded \$5.3 million to unlock an organization's assets, while they typically ended up settling for much less — on average settling for just over \$100,000. According to [Cybersecurity Ventures](#), a ransomware attack will hit every 2 seconds by 2031, and, in total, will cost victims \$265 billion each year.

When security vendors adjust and figure out how to block certain types of ransomware, AI helps attackers respond with new varieties that evade perimeter and signature-based protections. While the AI-enhanced malware threat is still emerging, generative AI tools such as ChatGPT have already enabled a sharp increase in malicious phishing emails. The number of malicious emails increased by 1,265% in 2023, with the [biggest spike being a 967% rise in credential phishing](#).

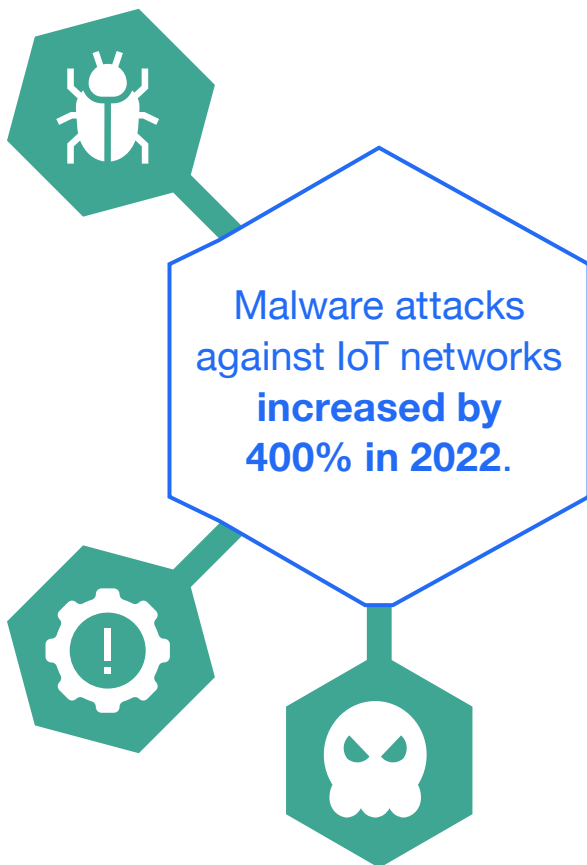
Zero-day attacks on critical infrastructure are also on the rise. For instance, [tens of thousands of Cisco devices were hacked](#) in late 2023. Also in 2023, a zero-day attack [compromised Citrix NetScaler ADC appliances](#), which allowed attackers to steal data from the infrastructure provider's Active Directory. At the time of these attacks, all of the impacted devices were patched and included the latest software updates.

The enterprise edge sprawls beyond perimeter protections

AS ATTACKERS GET MORE SOPHISTICATED, THE EVER-SPRAWLING ENTERPRISE EDGE EXPANDS THE ATTACK SURFACE THAT ENTERPRISES MUST PROTECT. IoT, WFH and cloud migrations all make perimeter security designs obsolete. In this hyperconnected world, anyone with an internet connection can easily find your exposed IP addresses, giving bad actors a bunch of juicy targets.

According to research firm IDC, IoT networks will grow to include [55.7 billion devices](#) by 2025, with IoT devices generating 80 billion zettabytes (ZB) of data. A [recent report by MarketsandMarkets](#) puts the IoT surge in dollar terms, forecasting that the global edge computing market size will grow at a compound annual growth rate (CAGR) of 15.7% from 2023 to 2028, increasing from \$53.6 billion in 2023 to \$111.3 billion by 2028.

Predictably, along with the surge in IoT devices, comes a surge in IoT attacks. According to the [Zscaler ThreatLabz 2023 Enterprise IoT and OT Threat Report](#), there was a 400% surge in malware attacks against IoT networks and devices in 2022. Botnet activity was the most common type of malware targeting IoT networks, with the Mirai and Gafgyt malware families accounting for 66% of attack payloads.



WFH, mobile and hybrid workforces also place the weakest security link (people) outside of traditional protections. [According to Pew Research](#), 41% of those who could work remotely or hybrid in 2023 did so, with 35% WFH full time.

Research indicates that this trend should continue indefinitely. A [survey by Mercer of 800 HR leaders](#) found that they estimated 94% of the staff at their companies were more or equally productive working remotely. In a survey [by Cisco of 28,000 full-time employees](#), 78% of employees said that remote and hybrid work improved their overall well-being. This cut across generational lines, including 83% of millennials, 82% of Gen Z, 76% of Gen X and 66.3% of baby boomers.

Unfortunately for enterprise security, the WFH trend positions knowledge workers farther and farther outside of traditional security perimeters, making them easy prey for motivated attackers.

Traditional WANs reach a breaking point

THE NETWORKS CONNECTING FAR-FLUNG REACHES OF THE ENTERPRISE, CORPORATE WANs, HAVEN'T KEPT PACE WITH THE THREATS DISCUSSED ABOVE. Hybrid work, cloud computing and IoT all stress traditional WAN technologies.

Traditional WANs also were not designed to meet the needs of new types of traffic, such as machine-to-machine communications, AI traffic and the need to grant partners and customers access to corporate resources.

Traditional approaches that depend on legacy WANs, such as MPLS, mesh VPNs and firewalls to manage application access, have become ineffective in a world that prioritizes cloud and mobile technologies. MPLS- and VPN-based network architectures expand your attack surface and allow for lateral movement of threats. Moreover, legacy architectures don't account for remote users or cloud workloads, leading to inconsistent user experiences and needless network complexity.

Drawbacks of legacy WANs

- **Hub-and-spoke perimeter security design exposes enterprises to a high risk of lateral threats and internet-based attacks.**
- **Increased complexity due to complicated routing, multiple network hops and a patchwork of appliances.**
- **Fragmented policy management due to the need to manage policy through multiple tools.**
- **Lack of visibility across the branch, data center and cloud connectivity paths, which creates both network and security blind spots.**
- **Poor performance and scalability due to the increasing number of network and security services within branch and data-center environments; the high number of services and appliances forces traffic through hairpin turns and chokepoints to attain any sort of centralized security inspection and control.**
- **Sky-high costs due to the need to overprovision legacy network and security appliances, such as routers, firewalls, IPS and other point products.**

Technologies such as SD-WAN have emerged to help accelerate high-priority traffic, but SD-WAN technologies fail to eliminate the ability of attackers to move freely throughout corporate networks. In fact, by extending the enterprise's trusted network to branches and clouds, many SD-WAN solutions make the risks associated with lateral movement even higher.

Siloed networking and security from a patchwork of vendors increases costs and complexity, and legacy networking designs funnel traffic through numerous bottlenecks. This still leaves numerous security gaps, such as allowing attackers to move freely through networks.

Add it all up, and legacy hub-and-spoke networks with perimeter protections undermine the goals of digital transformation initiatives while draining worker productivity and failing to protect against modern threats.



Why the modern enterprise needs a zero-trust networking foundation

THE MODERN ENTERPRISE NEEDS A NEW NETWORKING AND SECURITY PARADIGM TO DELIVER RELIABLE, SECURE, SPEEDY CONNECTIVITY TO WORKERS, PARTNERS AND CUSTOMERS, NO MATTER WHERE IN THE WORLD THEY ARE LOCATED AND NO MATTER WHAT DEVICES THEY ARE USING. In addition, the modern enterprise must also support IoT and operational technology (OT) networks that are mission-critical in factories, data centers, retail locations and more.

These shifts in the digital world mean that core computing resources of the enterprise will continue to migrate to the cloud (with many software tools now delivered only as cloud services), with more mission-critical resources moving away from centralized protections.

Thus, what the enterprise needs is a security-first networking foundation that protects against ransomware, phishing, zero-day attacks and other emerging threats, while also limiting movement within the network when a bad actor gains access or an employee or partner goes rogue and tries to damage or steal important assets.

The only way to protect assets in a cloud-centric, hyperconnected, highly mobile world is through a zero-trust foundation to networking and security.

What is zero-trust security?

TRADITIONALLY, ENTERPRISE NETWORKS WERE BUILT ON THE CONCEPT OF IMPLICIT TRUST. If someone had the credentials to get on your wired LAN, the assumption was that they were supposed to be there. Legacy networks were designed for a pre-WFH, pre-mobile, pre-IoT time when LANs were purely internal, with physical security, such as a security desk when you enter the building, mitigating risks.

Today, implicit trust exposes the enterprise to massive security risks.

[According to Gartner](#), zero-trust security is a paradigm in which no person or device is trusted, even if they are already within the network. In a zero-trust architecture, all users, devices and applications are suspect. Connectivity is brokered as needed based on business policies, identity, behaviors and context, and communications can then be revoked if context or behaviors change.

Practically, this means that all communications are backstopped by strong identity protections, such as multifactor authentication (MFA), while the connections to various assets are wrapped in policies that determine who can access what, as well as where they can access those resources from (i.e., not over public networks) and when.

Some vendors have already started layering zero-trust solutions on top of services like SD-WANs, but these retrofits haven't been terribly successful. The problem is that retrofitted zero-trust solutions require enterprises to consume separate networking and security products from multiple vendors. While this is an improvement over legacy perimeter security, this approach is complex and costly.

Moreover, bolting on zero trust often leaves major security gaps, and the patchwork of security tends to slow down application performance, undermining the real-time decision-making that many AI and IoT use cases exist to facilitate in the first place. Even worse, this patchwork approach to zero trust is labor-intensive, complicated to deploy and exponentially more difficult to manage as time goes on.

How to make zero trust the foundation of your WAN

TO ENABLE ZERO-TRUST CONNECTIVITY IN BRANCHES, CLOUD DATA CENTERS, IOT NETWORKS, WFH SETTINGS AND MORE, ENTERPRISES NEED A FOUNDATION THAT STARTS WITH TRUST.

Building a zero-trust network for the modern enterprise requires platforms, rather than point products. Plug-and-play services are needed that discover, classify and control all assets connecting to the network. Enterprises need strong authentication for all users and devices (even legacy unpatched ones), and they need tools that enforce policies.



The future of the WAN: Zscaler Zero Trust SD-WAN

ZSCALER ZERO TRUST SD-WAN DELIVERS A PLATFORM APPROACH TO NETWORKING AND SECURITY THAT IS DESIGNED TO MEET THE CHALLENGES OF THE CURRENT THREAT LANDSCAPE, WHILE ALSO DELIVERING THE SPEEDY, RELIABLE CONNECTIVITY THAT MODERN APPLICATIONS DEMAND. Zero Trust SD-WAN provides branches, smart factories and other remote sites with fast and reliable access to the internet, security-as-a-service (SaaS) and private applications with a direct-to-cloud architecture that provides high security and operational simplicity.

Zscaler Zero Trust SD-WAN dramatically simplifies branch, cloud and IoT/OT communications by eliminating complex routing, VPNs and firewalls, while allowing for flexible forwarding and simple policy management by using Zscaler's proven Secure Internet and SaaS Access ([ZIA](#)) and Secure Private Access ([ZPA](#)) policy frameworks.

With Zero Trust SD-WAN, branch traffic is forwarded securely and directly to Zscaler's Zero Trust Exchange, a comprehensive networking, security and analytics platform. When traffic is routed through Zero Trust Exchange, enterprises can apply ZIA or ZPA policies for full security inspection, as well as access identity-based control communications. Trusted application traffic can also be sent directly across the internet with direct internet breakout.


This unique approach provides four key advantages:

- **Elimination of network-based, site-to-site VPN connectivity** in favor of identity- and application-based control over communications for true, zero-trust security.
- **Phasing out of legacy castle-and-moat architecture** without throwing open the castle doors, thereby compromising security.
- **Removal of the patchwork problem**, as there is now no need for legacy products, such as Squid proxies, NAT gateways, IPSs and so on.
- **Prioritization of security as the foundation** for distributed, scalable connectivity delivered wherever it's needed via centralized, automated policy management that simplifies branch, cloud, data center and IoT/OT communications.

With Zscaler Zero Trust SD-WAN, enterprises connect to branches directly without extending the WAN or relying on VPNs, both of which increase a network's attack surface. Applications are hidden from discovery behind the branches, and access is restricted via the Zero Trust Exchange to a set of named entities. Identity, context and policy adherence of the specified participants are all verified before access is allowed, prohibiting lateral movement elsewhere in the network.

Already, Zscaler customers are using Zero Trust SD-WAN to:

- **Replace site-to-site VPNs** with simple plug-and-play connectivity that delivers operational simplicity with better security.
- **Secure access to IoT/OT resources** without the need for VPNs and without exposing ports.
- **Deliver remote desktops** that are fully isolated and clientless to provide access to internal remote desktop and Secure Shell protocol target systems for vendors/contractors.
- **Accelerate M&A integration**, becoming operational on day 1 by avoiding the need to merge routing domains or translate overlapping IP addresses.
- **Connect new users** to critical resources like Active Directory by simply adding plug-and-play appliances to new sites.
- **Discover and classify IoT devices**, finding and classifying unsanctioned and unknown IoT devices to give IT teams deeper visibility into behavior for better access-control policies.



Learn more about how you can modernize your WAN, super-charge app performance and reduce your organization's attack surface with the [Zscaler Zero Trust SD-WAN](#) today!

CONCLUSION:

Platform-based zero-trust security is the best foundation for digital transformation

AS TRADITIONAL NETWORKING AND CYBERSECURITY ARCHITECTURES CONTINUE TO BREAK DOWN UNDER THE STRESS OF AI, IOT, WFH, ZERO-DAY ATTACKS, AUTOMATED MALWARE, TARGETED RANSOMWARE, AND MUCH MORE, enterprises need not just new band-aid tools to protect and enable knowledge workers, but an entirely new way of connecting and securing employees, partners and customers.

To stop reacting to threats, to stop falling behind attackers and to fix the foundational networking and security problems that undermine digital transformation initiatives, enterprises need a new paradigm for modern communications that prioritizes trust above all else.

A platform approach to networking and zero-trust security is that foundation. Under zero trust, no person or device is implicitly trusted, even if they (or it) are already within the network. In a zero-trust network, all users, devices and applications are suspect and, thus, are prevented from freely communicating with one another. Connectivity is brokered as needed based on business policies, identity, behaviors and context, and communication privileges can then be automatically revoked if context or behaviors change. Some vendors have already started layering zero-trust solutions on top of services like SD-WANs, but these retrofits haven't been terribly successful, leaving major security gaps, among other issues.

Zscaler Zero Trust SD-WAN delivers a platform approach to networking and security that is designed to meet the challenges of the current threat landscape. Zero Trust SD-WAN provides branches, smart factories and other remote sites with fast and stable access to the internet, SaaS and private applications with a direct-to-cloud architecture that delivers high security and operational simplicity. Stop struggling with outdated networking and security architectures. Learn more about the [Zscaler Zero Trust SD-WAN](#) solution today.



About SDxCentral

SDxCentral is the leading resource for IT infrastructure knowledge.

IT infrastructure is under more demand and more scrutiny than ever. The way we build networks has fundamentally changed, with new technologies constantly popping up to solve new challenges. At the same time, the role of IT departments and of individuals within the department is changing. While vendors and executives strategize around new technologies, those in the trenches scramble to keep up.

These guides are independent content designed to share knowledge and help technology professionals stay ahead of the curve.

www.sdxcentral.com