The Data Fabric for Security

Enabling Continuous Risk Management

Solution Brief

Security teams currently leverage a myriad of technologies and solutions to protect their businesses from an expanding attack surface. Each of these tools produces massive amounts of valuable data. However, this data is often siloed and duplicative across tools. As a result, security teams struggle with information overload, opaque workflows, and increasing difficulty in defending their cybersecurity posture.

In particular, security practitioners tasked with designing Risk-Based Vulnerability Management practices struggle to remediate risk with speed and scale, according to business priorities. Without an integrated and complete view of their attack surface, they cannot assess vulnerabilities in the context of their organizational impact. This makes identifying and executing informed remediations time-intensive and inefficient.

At the heart of these pains are foundational data challenges

- **Siloed, disjointed, and high volumes of data**
- **Manual, error-prone processes**
- **Lack of business context**
- **Information and alert overload**
- **Misalignment across teams**

While data is at the root of the problem, it is also part of the solution. The Zscaler Data Fabric for Security automates data ingestion, normalization, enrichment, and cross-contextualization, providing security organizations a complete and real-time view of their cybersecurity posture.

Key Data Fabric for Security Benefits

Bring total flexibility to security operations Make your security data work for your team. Slice and dice data in any way and power cross-team workflows with accurate, contextualized insights.

Optimize security resources with automation
Automate data management, reduce technical debt, minimize data latency, and reallocate valuable time and resources to critical security programs (e.g. vulnerability remediation, threat hunting).

Improve security efficiency and effectiveness
Measure the performance of security investments, tools/technology, and programs. Infuse security workflows with data, share cross-team insights, and drive more effective collaboration with IT and developers.

Ensure data quality and control
Eliminate manual error-prone data processes. Build trust with data governance best practices and a unified foundation of security and business data.

64% of teams complain about pivoting among too many disparate security tools and management consoles, with little (if any) integration, inhibiting comprehensive and timely investigations and response.

Why the Data Fabric approach?

Data fabrics are a technological approach to data management focused on extracting value out of the underlying data in the form of actionable cross-platform insights, analytics, and operational use cases.

Forrester defines data fabrics as delivering "a unified, integrated, and intelligent end-to-end data platform to support new and emerging use cases. It automates all data management functions – including ingestion, transformation, orchestration, governance, security, preparation, quality, and curation – enabling insights and analytics to accelerate use cases quickly."[2]

The Zscaler Approach

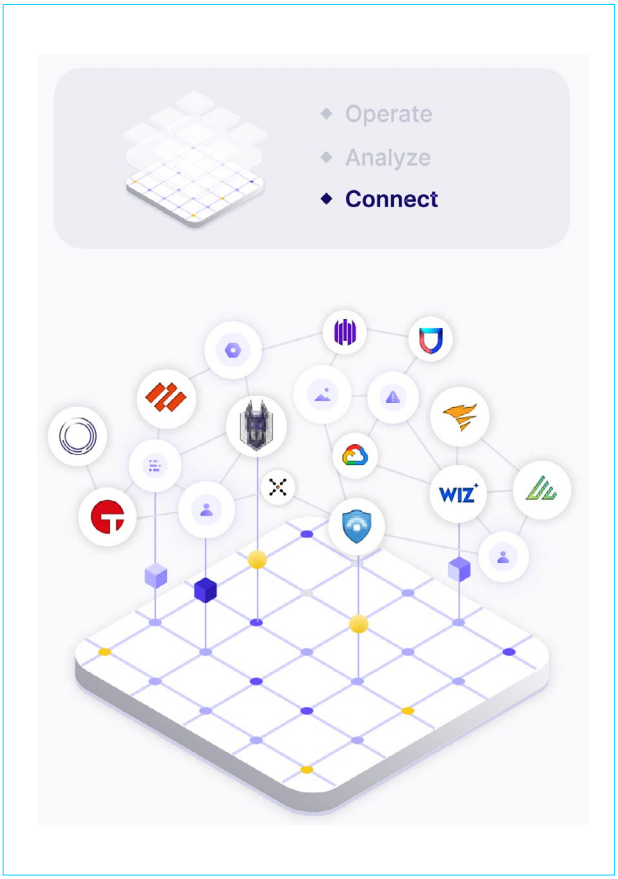
Zscaler's data fabric technology is unique in its focus entirely on security. Each data management function is built with security use cases in mind, providing practitioners with data integration, mapping, and enrichment capabilities infused with out-ofthe-box vertical-specific logic.

Zscaler's flexible Data Fabric for Security empowers teams with the architecture to connect any data across their entire security stack, enhance their workflows with critical business context, and expand into any use case to support and optimize security operations.

Overview: Zscaler Data Fabric for Security

Create a system of record for your entire security stack

- Seamlessly integrate data from security tools, IT systems, tech environments, and business applications in one accurate, cross-contextualized foundation.
- Connect any data, across any source, in any format, at any granularity. Free your teams from manual, timeconsuming processes with automated, flexible data integration.
- Leverage 150+ pre-built and continuously maintained connectors for security, IT, and business.
- No API? No problem. Zscaler's proprietary AnySource™ connector can intelligently ingest, detect, and map any file to your security data model.



Ensure data integrity and scalability with best practices

- Efficiently process and normalize data sets at any complexity while minimizing data redundancies and anomalies.
- Automatically structure data according to use case, making it easier for teams to maintain and update data based on business outcomes.

Maintain full data lineage and visibility into data management processes

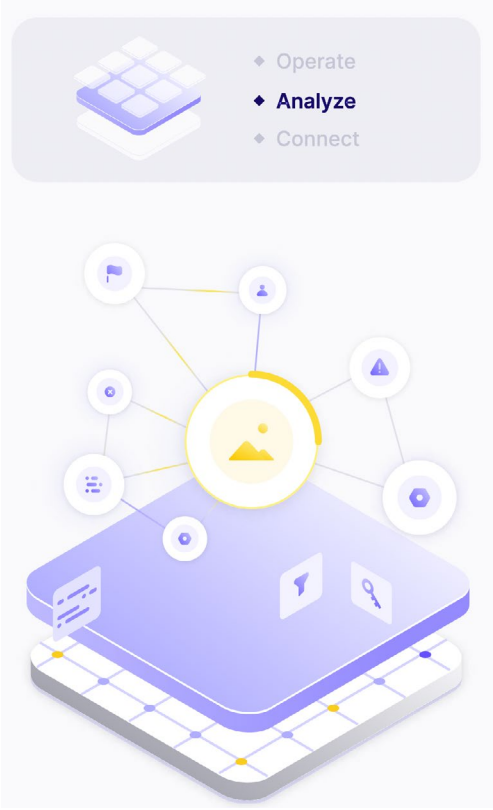
- Understand your end-to-end data flow and adhere to organizational policies.
- Facilitate organizational trust and data governance with full transparency into the data integration lifecycle.

Transform data into a universal language with a supercharged semantic layer

- Define entities, attributes, and relationships across all sources to prepare data for analytics and operational applications.
- Empower security practitioners with no-code or low-code capabilities and reduce the need for complex data engineering skill sets.

Organize and enrich data in an opinionated security data model

- Get a head start on data contextualization and correlation with a security optimized data model. Dynamically connect the dots between vulnerabilities, threats, findings, incidents, assets, software components, and users while extracting valuable metadata and telemetry across sources.
- Identify and surface gaps in your data set including asset ownership and criticality.



Enhance data sets further with the Open Security Graph

- Layer in any business context, segmentations, mitigating factors, and controls to increase organizational relevance.
- Categorize data and create custom entities and attributes at any point of the mapping and modeling process.

Answer any security question from any angle with a flexible query engine

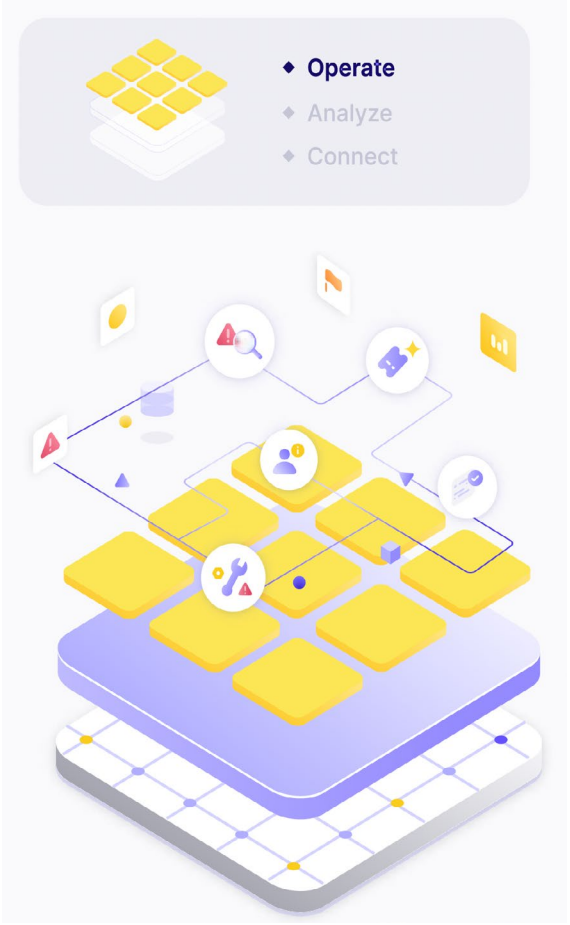
- Use preset or custom queries to retrieve information from any schema or perspective — and even layer in data outside of Zscaler through federated queries.
- Quickly pivot between data sets to find answers. Filter on any asset, finding, or any entity within the data model with no limitation.

Operationalize data with automation and insight-driven workflows

- Send real-time contextualized alerts — streamlined with the most critical information — to the appropriate teams in their system of choice.
- Reduce time spent on manual processes with no-code workflow automation tools to trigger dependencies, tasks, and actions based on any data.
- Optimize remediation workflows and filter out the noise so security, development, and IT teams can work smarter, together.
- Distill findings into logical groupings and dispatch tickets in one place with pre-built "outegrations" to ticketing and patch systems.

Report on what matters to your organization

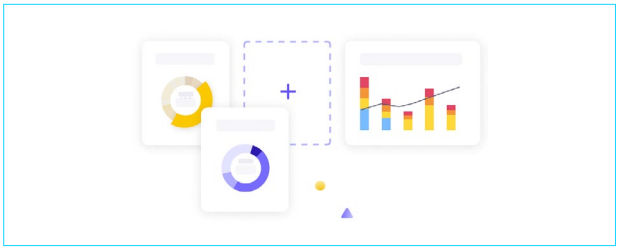
- Gain a uniquely comprehensive and dynamic understanding of risk, performance metrics, and trends.
- Tailor reports and dashboards to the exact needs of your audience, representing true residual risk by organization, from the individual analyst level all the way to the executive team and board.



- Easily share security performance with stakeholders through interactive, out-of-thebox risk dashboards and customizable reports.

Promote security awareness and cross-team collaboration

Unlock security insights and arm teams with the information needed to explain why action need to be taken — and ensure it's always delivered to the right team and business unit.

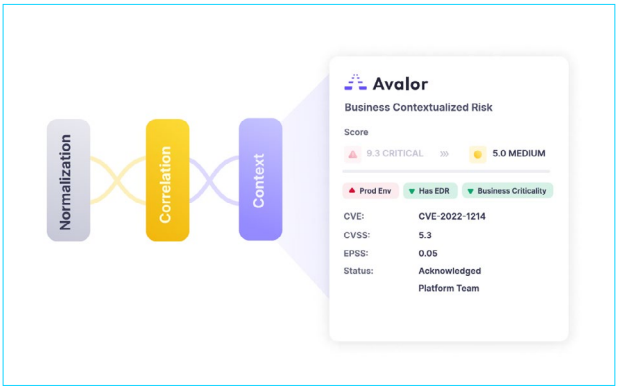


The Zscaler Unified Vulnerability Management Module

Powered by the Data Fabric for Security

Zscaler is building a series of modules to tap into the data fabric and empower security teams to reduce risk by making security data actionable and useful. Our first module delivers Unified Vulnerability Management.

The UVM module taps into the Zscaler Data Fabric for Security to provide tailored insights into a company's risk posture —- with contextual prioritization and custom workflows for remediation.



UVM provides three compelling capabilities:

- Risk prioritization based on a company's particular context — a better "to do" list for what needs fixing now
- Dynamic reports and dashboards that are automatically updated — no more Excel or BI tools needed
- Automated workflows for remediation — the right team gets the right info to meaningfully to reduce risk

The Zscaler Data Fabric for Security powers several of the Risk Management portfolio products today, and will become the foundation for them all in the near future. The 150+ connectors that enable inbound and outbound integrations already provide rich feedback loops between these products, creating layered risk insights across risk disciplines.

zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com