

Unified Risk Management Powered by the Data Fabric for Security

Siloed point products and data cannot provide the context for effective risk management

Improving your security posture requires a unified view of risk. Many modern enterprises have dozens of security tools, but the findings and data they generate live in isolation, preventing integrated insights. In addition, the sprawl of disconnected systems limits your ability to detect and mitigate breaches.

The power of a Data Fabric for Security

The Data Fabric for Security enables powerful aggregation and correlation of your security data and business context, fueling unique insights into your security posture and enabling early detection of bad actors. The fabric ingests, harmonizes, and deduplicates data from hundreds of Zscaler and third-party sources to produce consolidated findings. It then correlates and enriches those findings, offering unique insights and context that enable you to:

- Gain a holistic understanding of risk
- Know which risks to address first
- Detect compromised users early
- Contain breaches with integrated attack mitigation

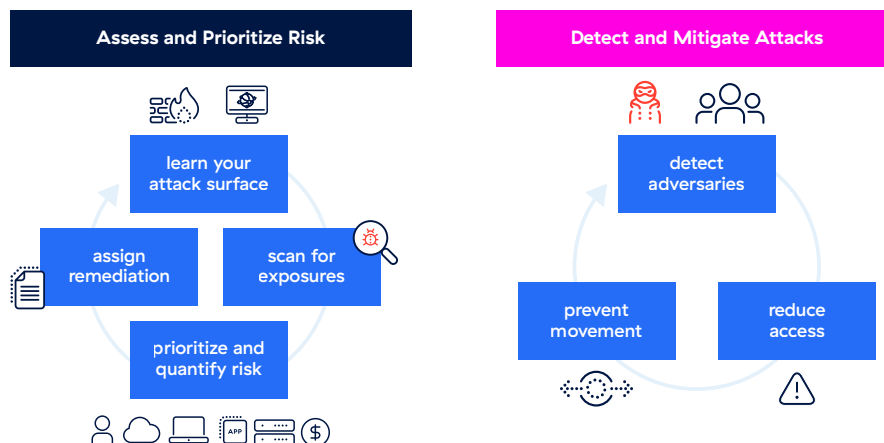
A unique platform, delivering unique security outcomes

The Data Fabric for Security, the industry's first, provides rich context and correlated findings that improve each solution in the Risk Management portfolio. No other vendor offers this approach to reducing cyber risk.



The modern risk landscape demands extensive protections

It's challenging to understand and reduce cyber risk. Even after deploying a range of preventive measures, organizations must still "assume the breach" and ensure they can quickly detect and limit attacks.



Shrink your attack surface with prevention, and reduce the blast radius with attack mitigation

The Zscaler Risk Management portfolio includes prevention and early breach detection tools. That combination is essential to maximizing risk reduction.

Prevention Solutions

Risk360

Risk quantification and visualization

- Identifies gaps in Zscaler configurations
- Provides cyber risk quantification (CRQ)
- Generates executive and board reports and presentations

Unified Vulnerability Management

Risk prioritization, remediation workflows

- Requires no Zscaler services, but uses Zscaler input when available to influence risk
- Provides customizable risk scoring using your risk factors and mitigating controls
- Automates workflows for remediation
- Supports dynamic reports and dashboards and presentations

External Attack Surface Management

Exposure identification in public assets

- Scans domains and other public-facing assets for vulnerabilities and misconfigurations
- Uncovers trends and your exposure to internet-facing threats in near-real time
- Assesses the severity of external asset vulnerabilities and continuously maps them to application assets and servers

Attack Mitigation Solutions

Deception

Honeypots to pinpoint malicious users

- Identifies malicious users, external or internal
- Provides low false positives, high-fidelity findings
- Enables containment via ZIA/ZPA policy, endpoint quarantine, or SOC alerts

Breach Predictor

Early attack detection, path analysis

- Leverages Zscaler logs to capture early signs of compromise
- Applies ML to log data to pattern match and identify a potential attack path
- Predicts the likelihood of attack based on the sequence of steps seen to date

Identity Protection

Detection of AD exposures, malicious users

- Finds Active Directory misconfigurations and exposed credentials
- Identifies malicious users running DCSync, DCShadow, kerberoasting, and similar attacks
- Leverages ZPA, EDR, and SIEMs to contain compromised users