cybereason | SOLUTIONS

zscaler™

Deploy an Integrated Zero Trust Architecture Across Your Enterprise

KEY BENEFITS

- Prevent ransomware and common initial attack vectors
- Reduce alert fatigue and increase visibility across IT/Security systems
- Identify if an attacker pivots from identity to endpoint to network

CHALLENGE

Protecting a distributed workforce that is pressed to innovate requires an efficient and effective approach. Today's defenders face attacks across workspace, identity, and endpoints. Teams must balance managing a strategy that includes prevention, modern threat detection, and guided or managed response.

SOLUTION

The combination of Cybereason and Zscaler provides a multi-layer block & detect approach against drive-by-compromise, command-and-control, unknown network connections, account takeover, and ransomware.

Telemetry and critical events from Zscaler Internet Access are streamed to Cybereason XDR, where suspicious events across your environment are correlated into MalOps (Malicious Operations), a visual timeline of any high-severity incident.

CORE USE CASES

MULTI-LAYER RANSOMWARE PROTECTION

From initial deployment, Cybereason and Zscaler block ransomware execution, drive-by-compromise, and common phishing attempts.

INVESTIGATE ATTACK STORIES, NOT ALERTS

Prioritize thousands of alerts across existing IT and security solutions, and translate them into visual timelines of detected malicious activity.

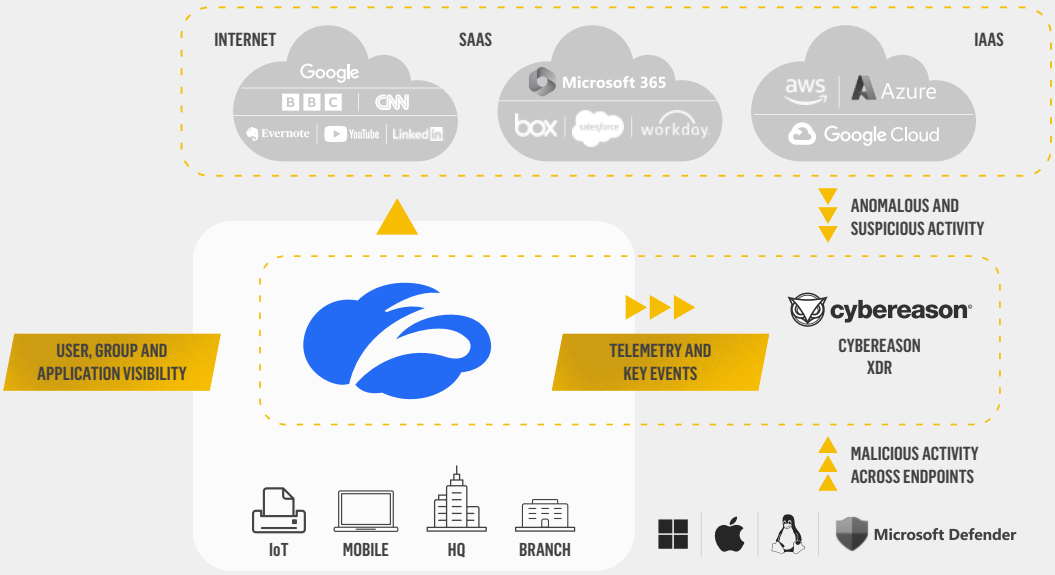
FIND AND RESPOND TO CRITICAL THREATS

A growing library of out-of-the-box detections identify key junctures in the attack chain. Take guided response actions or augment your team with Managed Detection and Response services.

HOW THE CYBEREASON & ZSCALER INTEGRATION WORKS

The standard XDR deployment includes installing the Cybereason sensor across endpoints and connecting Microsoft 365 or Google Workspace. The Zscaler Zero Trust Exchange, a leading Security Service Edge (SSE) solution, provides deep user and internet visibility, while enforcing proactive security policy across endpoint, network, and clouds. Zscaler Internet Access automatically blocks drive-by-compromise, command-and-control, and ransomware attacks. Cybereason ingests Zscaler telemetry and applies threat detections across streaming firewall, web proxy, and user activity data.

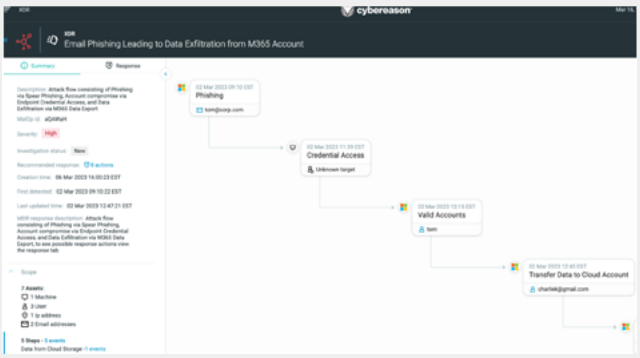
In XDR, **Suspicious Events** are correlated across workspace, identity, and endpoints. Important threats are presented in visual attack timelines known as **MalOps**.



Architecture Diagram detailing how the two platforms connect.

THE CYBEREASON MALOP

Cybereason helps you understand malicious operations (MalOps) that cross between your identity, endpoint, and workspace planes in a novel and engaging way. **MalOps** focus on identifying root cause, the correlated chain of events, affected hosts and identities, known attack tools, and most importantly, **Response Recommendations**. XDR supports Kill Process, Quarantine Host, Remote Shell, and includes Workspace and Identity responses. Cybereason's Global SOCs fully manage the XDR experience and outcomes.



INTEGRATING ZSCALER ZIA WITH CYBEREASON XDR

To forward logs from your Zscaler Internet Access (ZIA) platform to Cybereason XDR, you must set up a NSS feed that enables you to send these logs automatically.

STEP 1
In the Cybereason Connect screen, select Zscaler Internet Access (ZIA).

STEP 2
In the right side of the Connect screen, provide a Name for the integration.

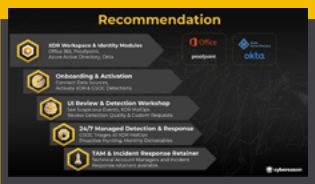
STEP 3
In the On-Site Collector details, in the Site name field, select the same site you used when you downloaded the on-site collector.

STEP 4
Below the Site name field, enter the Protocol and Port for the on-site collector. Click Connect.

LEARN MORE

READ INDUSTRY RESEARCH
Gartner Endpoint Protection Platforms Magic Quadrant

VIEW CYBEREASON-ZSCALER INTEGRATION
3-Minute Video Quadrant



EXPLORE XDR
Request a Free Trial

ABOUT ZSCALER
Zscaler (Nasdaq: ZS) accelerates digital transformation so 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 in-line cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.

ABOUT CYBEREASON
Cybereason is the XDR company, partnering with Defenders to end attacks at the endpoint, in the cloud, and across the entire enterprise ecosystem. Only the AI-driven Cybereason Defense Platform provides predictive prevention, detection, and response that is undefeated against modern ransomware and advanced attack techniques. The Cybereason MalOp™ instantly delivers context-rich attack intelligence across every affected device, user, and system with unparalleled speed and accuracy. Cybereason turns threat data into actionable decisions at the speed of business. Cybereason is a privately held international company headquartered in Boston with customers in more than 40 countries.