Unified Visibility from Endpoint to Cloud for Modern Threat Defense

SOLUTION BRIEF

The Stealthy Reality of Modern Attacks

Traditional security architectures were built on the premise of identifying malicious files. But today's adversaries no longer rely on malware that can be detected by signatures. Instead, they operate in the shadows of legitimate system processes and leverage frontier AI models to identify vulnerabilities to exploit at machine speed.

AI has lowered the bar for attack execution while increasing overall velocity: mapping an environment's infrastructure, identifying individuals to target for identity-based compromise, and building convincing spearphishing campaigns or other infiltration assets can be done now in hours or days, not weeks or months.

The bottom line: security teams need visibility into app or process execution as well as those making network connections outside the organization—this requires context to determine if the activity is legitimate or malicious.

Case Study: Volt Typhoon and "Living off the Land" Tactics
Volt Typhoon, a sophisticated Chinese state-sponsored actor, exemplifies the shift to fileless attacks. Their objective is to infiltrate critical infrastructure with long-term persistence, achieved through "Living off the Land" (LotL) techniques:

- **Initial Entry:** The attack begins by exploiting vulnerabilities in public-facing appliances, such as unpatched firewalls or VPN concentrators, to gain a foothold on the network perimeter.
- **Credential Harvesting:** Once inside, they don't deploy malware. They use native tools like ntdsutil to create snapshots of Active Directory databases or locate stored administrative credentials.
- **Discovery and Stealth:** They use standard binaries like netsh to map internal routing and systeminfo to identify high-value targets. Because these are legitimate Windows tools, they often bypass traditional EDR and antivirus alerts.
- **Lateral Movement:** Using stolen valid credentials, they move laterally via Remote Desktop Protocol (RDP) or VPNs, blending perfectly with authorized administrative activity.

In this scenario, a network alert for "unauthorized RDP" lacks the context to show that the connection was initiated by a compromised system process. Zscaler Endpoint Context changes this by providing the missing link: the identity and integrity of the application initiating the connection.

Eliminate the Visibility Gap with Zscaler Endpoint Context

Endpoint Context provides end-to-end visibility and adaptive risk-based policy enforcement by combining identity, endpoint, network, and cloud signals in a single platform. Unlike endpoint detection and response (EDR) offerings, our solution leverages inline TLS inspection at scale to empower SOC teams to detect and respond to threats faster with real-time, correlated endpoint and cloud intelligence to detect encrypted, fileless, and offline threats traditional defenses miss.

Endpoint Context extends the power of the Zscaler Zero Trust Exchange™ by integrating deep endpoint telemetry directly into your security policies, whether it be SSL/TLS inspection, DNS or IPS control. It eliminates the visibility gap between the network and the device, allowing you to see exactly which process on an endpoint is behind every packet and empowering security teams and incident responders to reduce mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR).

Key Features

Comprehensive Application Visibility
Beyond simple IP and port identification, Zscaler provides a granular view into the entire application landscape of your Windows and macOS fleet.

- **Deep Metadata:** Zscaler collects the Process Name, Parent Process, full Command Line arguments, and cryptographic hashes (SHA256).
- **Trust and Integrity:** It identifies the code-signing status and certificate vendor of every binary.
- **Example Use Case:** Instantly identify "Shadow IT" or custom scripts—like those used by Volt Typhoon—that are communicating with the internet but lack a valid corporate signature.

Dynamic Endpoint-Aware Policy Enforcement
Zscaler transforms your security from static rules to adaptive, risk-aware controls.

- **Granular Conditions:** Policies can now be based on endpoint-specific attributes. For example, you can create a policy that allows chrome.exe to access the web but blocks powershell.exe from making any outbound connections to non-corporate domains.

- **Multi-Layered Defense:** These conditions are enforced across the entire Zscaler stack, including the Advanced Threat Protection (ATP) engine, Zero Trust Firewall (ZTFW), and DNS Security.

Air-Gapped Threat Protection with Cloud Sandbox
Attackers often use "out-of-band" vectors to bypass network security. Zscaler Endpoint Context provides an industry-first defense against these entry points.

- **The Offline-to-Online Flow:** When a user introduces a new file via USB, Bluetooth, or AirDrop, the endpoint agent intercepts the file.

- **AI-Driven Analysis:** If the file is unknown, it is automatically uploaded to the Zscaler Cloud Sandbox for quarantine and inspection before it can execute. This prevents "Patient Zero" infections that traditional network-only sandboxes would miss.

Agentless Device Fingerprinting with JA4
Zero Trust must extend to devices that cannot support an agent, such as IoT, OT, and BYOD.

- **JA4 Signatures:** Zscaler uses the JA4 fingerprinting standard to identify devices based on the TLS handshake (Client Hello).

- **Anomaly Detection:** By creating a unique "digital fingerprint," Zscaler can detect if a device (e.g., a smart camera) begins communicating in a way that is inconsistent with its fingerprint, signaling a potential spoofing attempt—without requiring SSL decryption.

Vulnerability-Based Access Control
Effective cyber hygiene is the first line of defense. Zscaler correlates endpoint inventory with the global CVE database to enable proactive protection.

- **CVE-Aware Policies:** You can set a policy that automatically blocks outbound traffic from any application with a "Critical" CVE.

- **Example Scenario:** If a critical zero-day is found in an older version of a browser, Zscaler can block that specific version from accessing the internet, effectively forcing a "just-in-time" update for the user.

Accelerate SecOps with Contextually-Rich Logging
Zscaler eliminates the "manual pivot" between network logs and EDR consoles that slows down incident response.

- **Enriched Telemetry:** The Zscaler Nano Streaming Service (NSS) now includes process-level fields—such as %s{appname} and %s{apphash}—directly in the ZIA and ZPA logs.
- **SIEM Synergy:** When an analyst sees a suspicious connection in their SIEM, they don't have to search for the device in a separate console to see what caused it. The log already tells them: "This connection was initiated by cmd.exe running a base64-encoded script."

True Zero Trust Requires Endpoint Visibility

By unifying endpoint and network intelligence, Zscaler Endpoint Context allows organizations to move beyond reactive security. It provides the visibility needed to prevent stealthy "Living off the Land" attacks and detect processes—including "Shadow IT" or malicious usage of AI tools by employees or threat actors—for the controls that can help decrease the time to detect and respond to threats in real-time.

Learn more about how you can eliminate security blind spots with Zscaler Endpoint Context: Contact your Zscaler representative or visit zscaler.com

About Zscaler

Zscaler (NASDAQ: ZS) is a pioneer and global leader in zero trust security. The world's largest businesses, critical infrastructure organizations, and government agencies rely on Zscaler to secure users, branches, applications, data & devices, and to accelerate digital transformation initiatives. Distributed across 160+ data centers globally, the Zscaler Zero Trust Exchange™ platform combined with advanced AI combats billions of cyber threats and policy violations every day and unlocks productivity gains for modern enterprises by reducing costs and complexity.

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

zscaler™

Act Fast.
Stay Secure.