Zscaler Endpoint Context

Eliminate Blind Spots and Stop Attacks with Unified Visibility from Cloud to Endpoint

DATASHEET

The Challenge: Security Blind Spots in the Era of Fileless Attacks

In today's threat landscape, traditional file-based malware is no longer the primary weapon of choice for sophisticated adversaries. Instead, attackers are increasingly "Living off the Land" (LotL) using legitimate system tools like PowerShell, Windows Management Instrumentation (WMI), and Remote Desktop Protocol (RDP) to bypass legacy security controls. Because these attacks leave no malicious files behind they are virtually invisible to traditional antivirus and perimeter defenses. Incident responders also need digital "bread crumbs" to follow as they investigate an intrusion, but fileless attacks leave none for them to find.

For modern security teams, this shift creates four critical challenges:

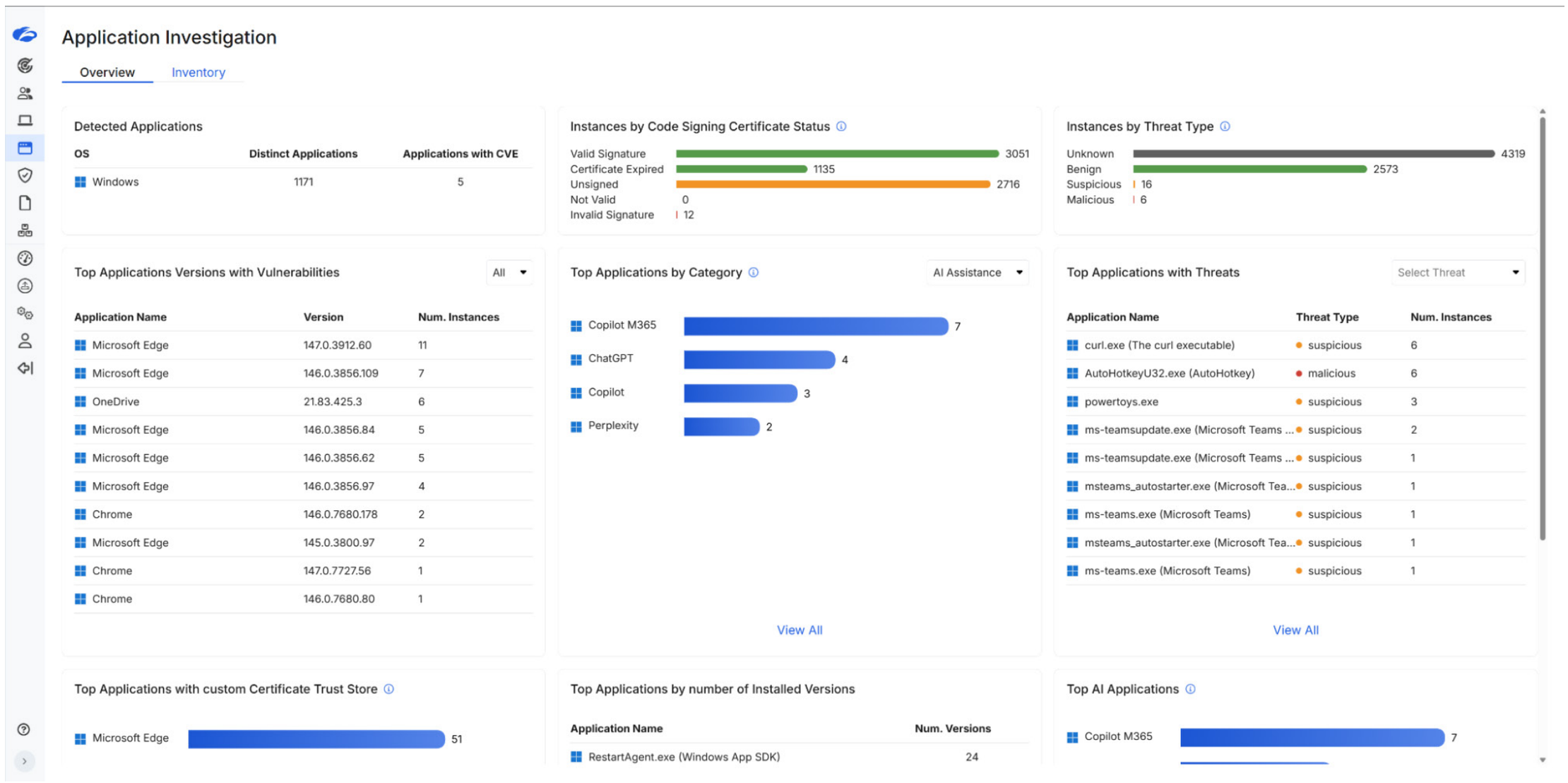
- **The Invisibility of Fileless Threats:** Detection gaps widen as attackers blend in with trusted processes, making it nearly impossible to distinguish between a routine admin task and a malicious lateral movement.
- **Fragmented Telemetry:** Analysts are overwhelmed by siloed data. Stitching together identity, network, and endpoint logs manually delays response times and leaves organizations vulnerable during the "golden hour" of an incident.
- **Invisible Risks and Shadow IT:** A lack of visibility into unmanaged, unpatched, or unsigned applications creates an unmanaged attack surface. Security teams cannot protect what they cannot see.
- **"Out-of-Band" Entry Points:** Threats introduced via USB, Bluetooth, or AirDrop often bypass network-level security entirely, allowing lateral movement to begin from within the "trusted" environment.

Zscaler Endpoint Context: Visibility from Cloud to Endpoint

Gain end-to-end visibility and adaptive risk-based policy enforcement by combining identity, endpoint, network, and cloud signals in a single solution. Unlike endpoint detection and response (EDR) offerings, Endpoint Context 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, transforming fragmented data into unified, actionable intelligence.

Instead of treating the endpoint as an isolated island, Zscaler makes the endpoint a cornerstone in your zero-trust based security posture with these key capabilities:

- **Continuous Risk Assessment:** Automatically correlate the health, posture, and risk level of a device with every access request.
- **Adaptive Policy Enforcement:** Transition from static rules to dynamic, risk-aware policies that can be adapted in real-time based on the specific application initiating the traffic.
- **Proactive Attack Surface Reduction:** Identify and block vulnerable or unsanctioned applications before they can be exploited, significantly lowering overall risk for your organization.
- **Accelerated Response:** Empower SecOps teams with rich, correlated context, reducing Mean Time to Detect (MTTD) and Respond (MTTR) by eliminating the need to pivot between multiple consoles.



The Application Investigation dashboard quickly uplevels vital information about applications running on endpoints in your environment.

Key Features

Feature	Summary
Complete Application Visibility	Gain deep insights into every process running on Windows and macOS. Identify risky, unapproved, or vulnerable software with detailed inventory data, including versions and CVE enumerations.
Endpoint Context-Aware Policy	Create granular, adaptive security policies. Block or allow traffic based on real-time metadata—such as application name, signing status, or risk level—across ATP, Firewall, and DNS policies.
Endpoint Sandbox	Extend protection to “out-of-band” threats. Unknown files introduced via USB or Bluetooth are automatically submitted to the Zscaler Cloud Sandbox for analysis before execution.
Agentless JA4 Fingerprinting	Extend Zero Trust to IoT, OT, and BYOD devices. Use unique JA4 client fingerprints to identify unmanaged devices and detect anomalies in encrypted traffic without requiring SSL decryption.
Vulnerability-Aware Protection	Correlate endpoint data with known vulnerabilities (CVEs) to proactively block traffic from high-risk software versions before they can be leveraged in an attack.
Context-Rich Log Streaming to SIEM	Augment logs with process paths, certificate status, and file hashes. Stream this rich telemetry to your SIEM via Zscaler Nano Streaming Service (NSS) for comprehensive investigations.

Ready to eliminate your security blind spots and accelerate detection and response? Visit zscaler.com to learn how Zscaler Endpoint Context can strengthen security posture from cloud to endpoint.

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.