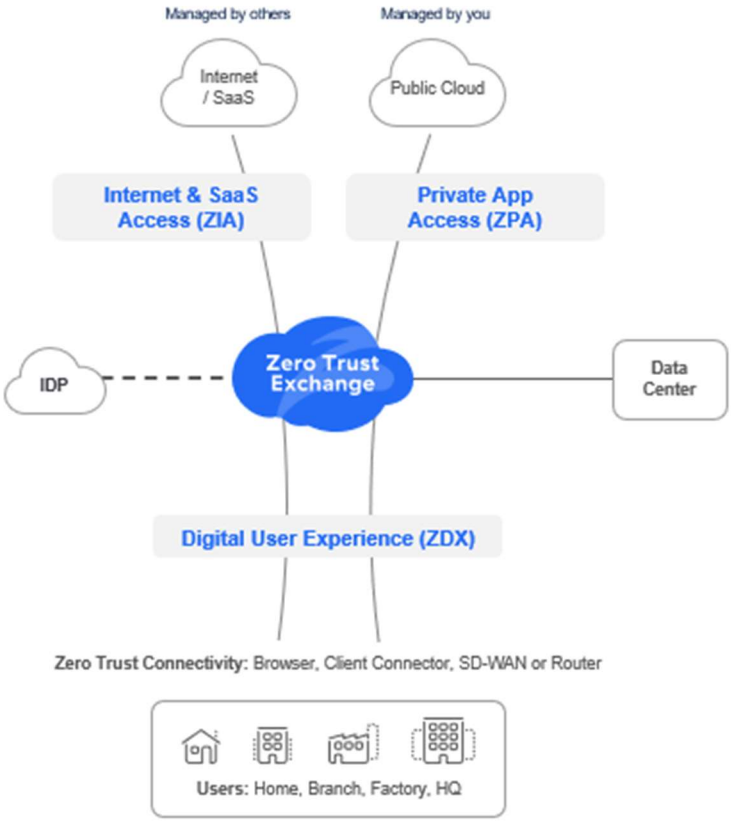
Zscaler visibility for the SOC

Enterprise-class security operations centers (SOCs) require comprehensive visibility into data flowing through the environment, wherever it resides—in a traditional data center, in the cloud, or in a hybrid architecture. NetWitness, a leader in the threat detection, investigation, and response tools that are the foundation of a high-performance SOC, is built to collect and analyze all the data an enterprise produces, eliminating blind spots that can give attackers a foothold.

The Zscaler Zero Trust Exchange™ (ZTX) is a Secure Service Edge (SSE) cloud platform that provides uniform security for entire branches, remote users, workloads and things.



With critical data flowing through the cloud SSE service, SOC visibility is essential. Using Zscaler's rich telemetry, NetWitness is able to provide unparalleled visibility into user activity when combined with the larger corpus derived from other security tools, including endpoint telemetry, applications and systems. This comprehensive visibility is what empowers security analysts and other SOC staff to detect, investigate, and respond to attacks and other threats. It leaves attackers with no place to hide and detects suspicious activity wherever it occurs, even correlating seemingly unrelated activities across an organization's environment.

The benefit to NetWitness and Zscaler customers is the ability to leverage Zscaler's zero trust architecture, active threat defense, and data protection capabilities, and provide deep visibility for an organization's SOC -- its core security team. It's the best of both worlds from a security perspective.

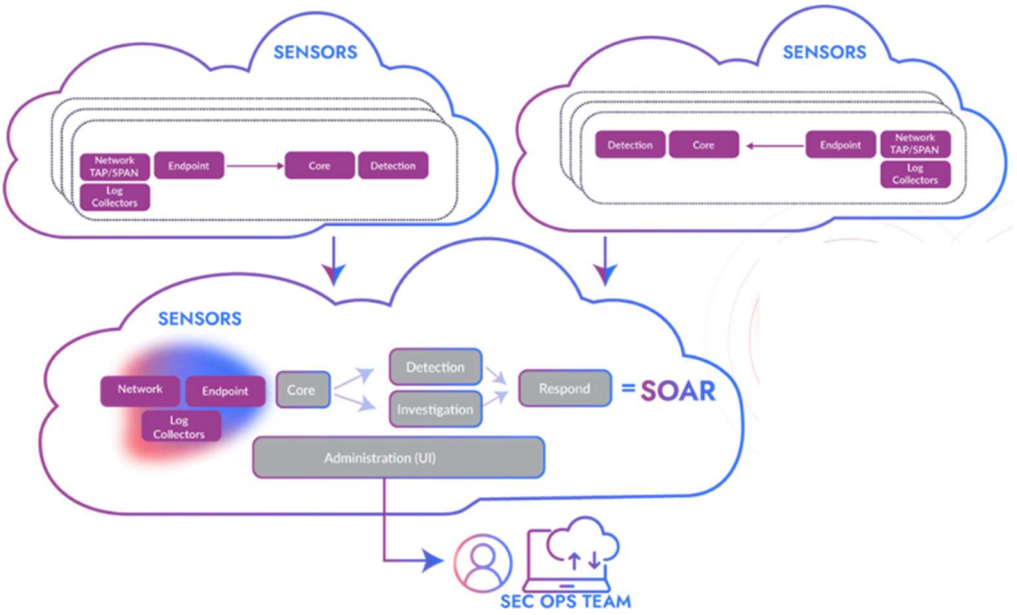
Zscaler + NetWitness

Zscaler's zero trust exchange is delivered on a custom-built zero trust architecture that securely connects users to apps, apps to apps, and machines to machines over any network, in any location. Zscaler performs for user identity, security posture and policy before allowing traffic to pass. All traffic is decrypted to check for threats and sensitive data. Applications aren't exposed to the internet, dramatically reducing the attack surface. By connecting users directly to applications rather than a network, malicious actors aren't able to move laterally, limiting the damage they are able to cause in the event of a breach.

NetWitness has a critical place in an organization's security strategy. It ingests and analyzes all of an organization's data, across diverse sources and deployed in any combination of on-premises, virtualized, and cloud locations. Important data sets like Zscaler logs, network packets, endpoint telemetry and operational technology are combined, enriched with relevant metadata, and indexed, all at ingest time for continuous protection.

Key Features

- Delivers SSE benefits like Zero Trust, Active threat Defense, and Data Protection
- Preserves full log visibility for Zscaler data in the SOC
- Easy and robust integrations using Nanolog Streaming Service (NSS)
- Supports both Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) logs
- Ongoing NetWitness-Zscaler partnership for up-to-date integrations and innovations



Once collected, data is analyzed for threats using industrial-strength threat intelligence, artificial intelligence and machine learning, behavioral analytics, and custom rules that are applied by SOC personnel. Alerts are correlated and combined into investigations, ranked by severity and risk. Security analysts are guided through the investigation process, with the ability to "drill down" on any piece of data to reveal its true intent and activity.

Once a threat has been identified, NetWitness provides orchestration and automation services to respond and mitigate harm. External systems, including Zscaler, can be instructed to block or isolate affected users and systems, and to stop processes and connections that create risk. Playbooks ensure that future attacks are quickly detected and resolved in an automated fashion, freeing security staff to defend against novel attacks.

NetWitness's rich forensics capabilities allow security analysts to see the full scope of an attack and ensure that it's not still lurking somewhere in the environment. It empowers an organization to confidently report to its board, or to external parties such as shareholders, regulators, and insurers, about what happened, how it happened, and how it was resolved.

Integration

Zscaler's Nanolog Streaming Service (NSS) provides a simple and fast way to perform log streaming to any security platform. NetWitness provides simple, robust NSS connectivity to both Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) logs. Designed to

support large throughputs, the NSS logs stream directly into the NetWitness Log Decoder or a remote Log Collector (a.k.a. "sensors"), where it is parsed, normalized, enriched, and indexed. This is all performed at ingest time, to deliver the highest fidelity analytics and most accurate detections. Other tools may perform metadata enrichment when an investigation is instantiated, likely losing context that was available at ingest time but was subsequently lost.

Summary

Zscaler integration with NetWitness enables organizations to deliver its users all the benefits of zero trust and secure connectivity, without sacrificing the visibility that is so essential to a top-tier SOC. Integrations are kept up-to-date through continuing partnership, and new opportunities to provide value are constantly being developed. For example, log data is essential to integrating Zscaler data into NetWitness, but network data can provide tools like session reconstruction, or "DVR replay" of an event to see exactly what was presented to a user and how they interacted with it. Zscaler and Netwitness will continue to explore ways to enhance security for our combined solution.

About NetWitness

NetWitness, an RSA® Business, provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats.

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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.

Ready to learn more? Visit www.netwitness.com