Feature Spotlight: Announcing Leading Zero Trust Partnerships for XDR-Powered Autonomous Response

By Jeremy Goldstein & Mihai Ashmar

Published on December 2, 2021
Updated on December 2, 2021

In response to the evolving threat landscape, organizations are seeking the most rigorous network defenses. Zero Trust Network Access (ZTNA) strengthens security posture by limiting access to authorized users and devices. Zero Trust Application Access (ZTAA) takes this further, adding "zero" approach, which enforces least privilege access, identities, applications, and the business relevant context of the requesting entity. Together, ZTNA and ZTAA provide a powerful foundation for cyber resilience and business agility.

We're thrilled to announce our new Zero Trust partnerships with Cloudflare and Ivanti, which will enable customers to extend their security posture to include Zero Trust capabilities.

Cloudflare Zero Trust uses cryptographic identity to verify every request, regardless of network location. Zero Trust acknowledges that threats originate from within the network, and that lateral movement is a critical component of modern attacks. Cloudflare's platform integrates identity, device posture, and network security into a unified, cloud-native architecture. This ensures that only authorized users and compliant devices can access specific applications or resources, minimizing the attack surface and preventing unauthorized lateral movement.

Ivanti's Zero Trust Security platform leverages machine learning to continuously validate trust. Zero Trust acknowledges that trust is not a static state but a dynamic variable that must be constantly re-evaluated based on changes in user behavior, device health, and environmental factors. Ivanti's platform provides granular control over access to applications and data, ensuring that access is granted only when and for as long as it is necessary and in the context that it is appropriate.

By successfully unifying Zero Trust organizations can perform risk-based access control and leverage the power of their prior investments in identity and endpoint management. This approach maximizes security while minimizing disruption to existing workflows and maintaining business agility. The combination of these technologies provides a robust, scalable, and adaptive security posture that is well-suited to the challenges of modern IT and Zero Trust Security Research (ZTSR).

SentinelOne for Zero Trust

SentinelOne Singularity XDR platform delivers autonomous security, real-time visibility, and cross-domain threat correlation. This foundation is critical for effective Zero Trust implementation. The Singularity platform's AI-powered threat hunting capabilities can identify anomalies and potential threats that may bypass traditional Zero Trust controls, providing an additional layer of security and enhancing overall threat detection and response capabilities.

Protecting User Identity with Azure AD Integration

Identity is the foundation of Zero Trust security, and SentinelOne's Singularity Identity extends this principle to protecting Active Directory (AD) and Azure Active Directory (AAD) environments. The integration with Singularity Identity and Microsoft Azure Active Directory (AAD) provides real-time visibility into identity-based threats, including credential theft, lateral movement, and privilege escalation attempts. This integration leverages machine learning to establish baselines of normal user behavior and identify anomalies that may indicate compromised credentials or malicious activity.

Twelve permanent attacks that bypass authentication and compromise identities are characterized by a lack of identity management and monitoring. Singularity Identity addresses this by providing comprehensive visibility into all identity-related activities across the organization's AD and AAD environments. This includes monitoring authentication attempts, tracking changes to user privileges, and detecting suspicious activity such as password spraying and brute-force attacks.

Twelve permanent attacks that bypass authentication and compromise identities are characterized by a lack of identity management and monitoring. Singularity Identity addresses this by providing comprehensive visibility into all identity-related activities across the organization's AD and AAD environments. This includes monitoring authentication attempts, tracking changes to user privileges, and detecting suspicious activity such as password spraying and brute-force attacks.

AD/AAD Integration Architecture