ShadowPlex Identity Security

Perfect Complement to CrowdStrike Falcon Identity Protection

“*Identity as the new security perimeter*” is the reality. The traditional security perimeter has become porous with the rapid adoption of cloud services, mobile solutions, internet-facing applications, and the recent hybrid work-from-home model. The new normal is that the traditional perimeters will be breached sooner or later. The focus is now on internal identity security so that the breaches do not become disasters.

- ✓ Advanced attack detection against identity repositories
- ✓ No changes required to domain controllers
- ✓ No additional logging or auditing required
- ✓ No agent installation
- ✓ Seamless and low-overhead deployment
- ✓ High-fidelity detection of identity attacks based on identity deceptions

ShadowPlex Identity Security

Attacks compromise identities from identity repositories to the multiple identity caches across the enterprise endpoints. Acalvio ShadowPlex Identity Security includes visibility and management of the identity attack surface area and an effective deception-based solution to detect and respond against identity attacks. The first step in reducing the attacker’s chance for success is discovering the identity attack surface. For the attack surface that cannot be removed due to operational reasons, ShadowPlex provides identity-specific deceptive elements to detect and respond to compromise attempts.

1. Identity Attack Surface Visibility and Management

Identity Attack Surface includes identity repositories and credential caches on endpoints. ShadowPlex provides deep visibility into the attack vectors in both kinds of identity stores and proactive management of the identity attack paths.

1.1 Identity Repositories

ShadowPlex provides valuable insights into the attack surface and attack targets in on-premises AD deployments, Azure AD, and Hybrid AD deployments. ShadowPlex also provides visibility into the M365® email attack surface. ShadowPlex conducts an automated discovery of these repositories and employs advanced AI algorithms and security domain knowledge to make visible **critical exploitable** attack surface and attack targets.

1.2 Endpoint Credential Caches

Cached data such as cached user credentials, user profiles, RDP connection objects, browser history, and access data stored in applications introduce new attack vectors in enterprise networks. Attackers move laterally within networks using native connectivity credentials and connections.

ShadowPlex offers a powerful Endpoint Attack Surface Management capability that provides in-depth **visibility** into the attack surface on endpoints.

1.3 Attack Paths

All sophisticated attacks use pre-analysis tools that can zero in on identities to compromise once they are inside the enterprise and move within the network without being detected. In any network, complex security relationships between various entities create pathways for attackers to laterally move. Adversaries assess their target network in graph models, and they know exactly how to use these pathways to avoid detection by leveraging existing trust relationships.

ShadowPlex offers a powerful **Predictive Analytics** capability that combines AI-based **Advanced Deception** with **Graph Theory** to **identify attack paths** involving **exploitable chains of relations**. ShadowPlex **leverages data from multiple sources** that include AD InSights, endpoint attack surface data, neighborhood discovery data, vulnerability data among others to compute the attack paths.

2. Active Defense against Identity Attacks

ShadowPlex identity attack detection uses a combination of decoy users, computers, and SPNs to detect sophisticated attacks against AD. Based on the attack type, ShadowPlex uses an AI module to automatically recommend the deception to deploy. By leveraging the insights gained from identity attack surface visibility, ShadowPlex can craft a set of precise deceptive elements that address the attack type and blend into the contents of the AD. ShadowPlex provides a pre-built curated palette of non-fingerprintable deceptions designed specifically to detect advanced Active Directory attacks.

ShadowPlex also provides management of endpoint attack surface area. In addition to visibility into credential caches, ShadowPlex delivers an ability to *reduce the attack surface* by removing the cached credentials, as well as a capability to replace the cache with deceptive elements.

ShadowPlex has an extensive palette of identity deceptions to deploy to endpoint credential caches, including user profiles, pathways for lateral movement, security configurations, application credentials, etc.

The deceptive elements on the endpoint redirect attacks to authentic decoys, deployed using ShadowPlex Autonomous Deception platform. Each decoy is unique and built on real network and application stacks. The decoys can engage with the attacks and collect the attack TTPs.

Comprehensive Identity Protection

Acalvio ShadowPlex analyses endpoint credential caches and credential repositories, and provides visibility into attack paths that leverage exploitable chains of relations. ShadowPlex also leverages the power of AI to deploy a layer of identity deception across the identity repositories, identity caches, and the network to detect identity attacks and generate high fidelity alerts.

Identity Security is a critical component of the enterprises' overall security strategy. Acalvio ShadowPlex Identity Security provides complementary capabilities to the CrowdStrike Identity Protection features, and both together provide a complete identity security solution.

For further details, please visit https://www.acalvio.com/shadowplex-crowdstrike/

About Acalvio:

Acalvio is the leader in Cyber Deception technology, built on over 25 issued patents in Autonomous Deception and advanced AI. The Acalvio ShadowPlex deception platform provides robust Identity Security, Active Defense, and Threat Hunting products. ShadowPlex solutions include Enterprise IT Security, OT Security, Zero Trust, Active Directory Protection and Ransomware Protection. The Silicon Valley-based company's solutions serve Fortune 500 enterprises, government agencies, and marquee MSSPs.

Acalvio Technologies| 2520 Mission College Boulevard, Suite 110, Santa Clara, CA 95054, USA | www.acalvio.com