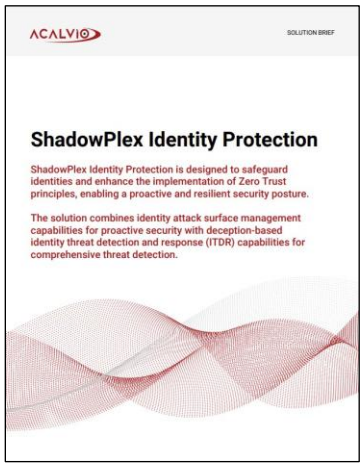


ShadowPlex Identity Protection

Thank you for downloading this Acalvio solution brief. Carahsoft is the distributor for Acalvio cybersecurity solutions available via NASA SEWP V, NASPO ValuePoint, ITES-SW2, and other contract vehicles.

To learn how to take the next step toward acquiring Acalvio's solutions, please check out the following resources and information:

For additional resources:
carah.io/acalvioresources

For upcoming events:
carah.io/acalvioevents

For additional Acalvio solutions:
carah.io/acalvio

To purchase, check out the contract vehicles available for procurement:
carah.io/acalviocontracts

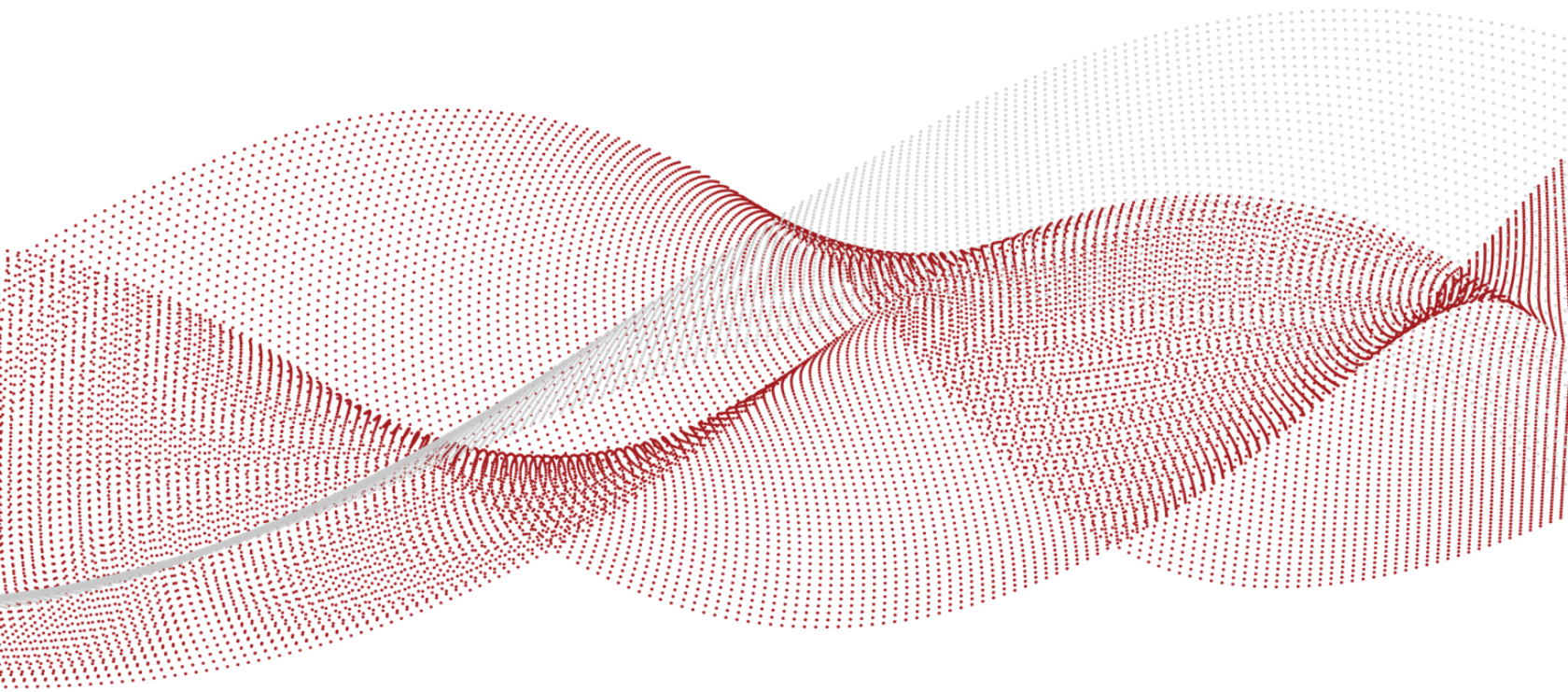
To set up a meeting:
acalvio@carahsoft.com
855-377-5865

For more information, contact Carahsoft or our reseller partners:
acalvio@carahsoft.com | 855-377-5865

ShadowPlex Identity Protection

ShadowPlex Identity Protection is designed to safeguard identities and enhance the implementation of Zero Trust principles, enabling a proactive and resilient security posture.

The solution combines identity attack surface management capabilities for proactive security with deception-based identity threat detection and response (ITDR) capabilities for comprehensive threat detection.



THE IDENTITY ATTACK SURFACE CHALLENGE

"Threat actors have shifted from gaining control of an endpoint to gaining access to a user's credentials and account… Over the next year, we will see threat actors find new ways to steal identities from users using a combination of social engineering, commodity information stealers, and information gathering from internal data sources post-compromise. They will combine stolen credentials with new techniques to bypass multifactor authentication (MFA) and abuse Identity and Access Management (IAM) systems."

— Mandiant
Cyber Security Report

The Identity Protection solution that proactively identifies and reduces the identity attack surface and detects identity-driven attacks with precision and speed

Identity-driven attacks are experiencing a significant surge. A trend that is exacerbated by the widespread adoption of cloud services and the rise of remote work. This shift has redefined the traditional enterprise perimeter, with identity emerging as the new focal point. Attackers now focus on targeting identities and the identity infrastructure that supports them, aiming to gain trusted access to critical systems and sensitive data.

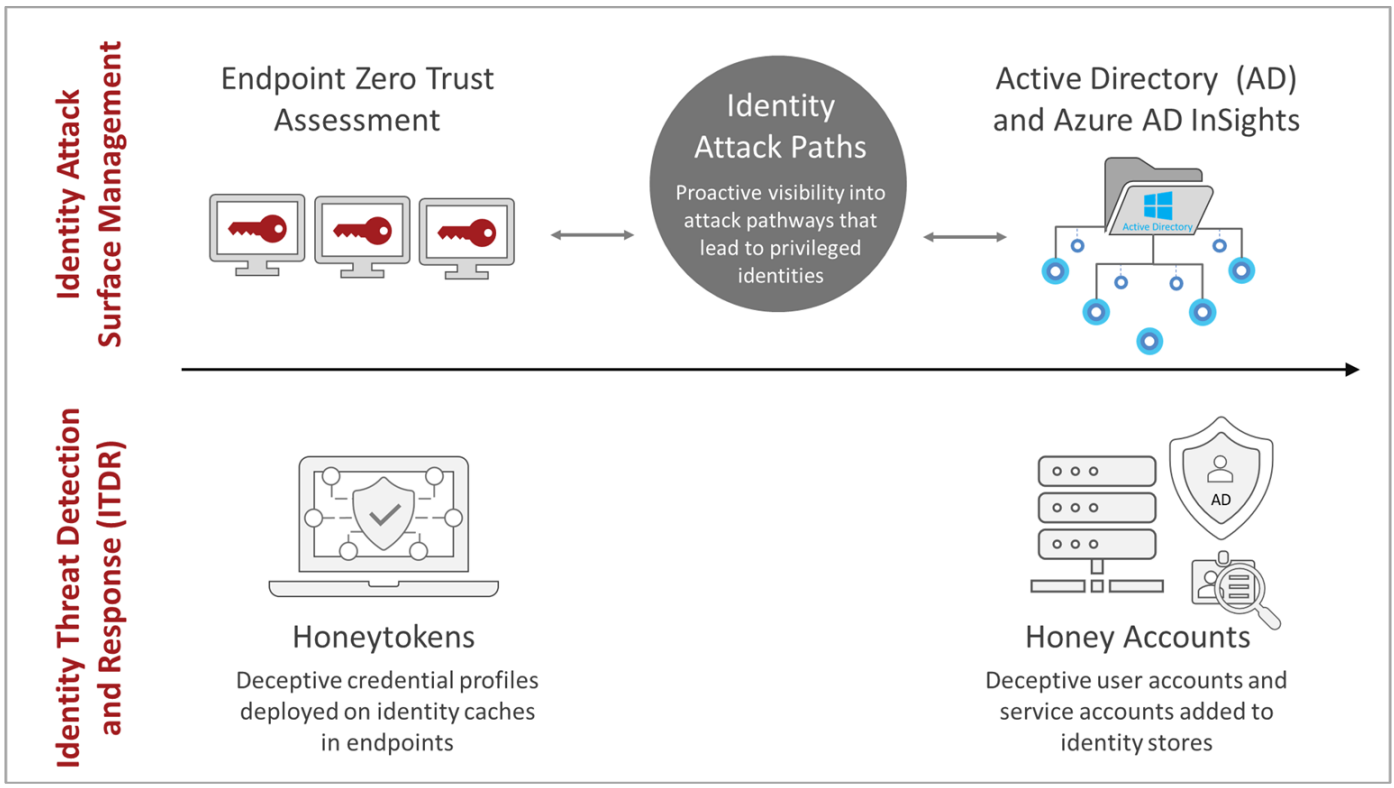
In response, organizations are turning to Zero Trust frameworks. **The foundation of Zero Trust relies on the trustworthiness of identities.** Unfortunately, attackers are adept at circumventing preventive identity security measures like Privileged Access Management (PAM), Multifactor Authentication (MFA), and Identity and Access Management (IAM). Traditional security solutions face challenges in detecting identity-driven attacks, and struggle to differentiate between legitimate and malicious identity usage. Consequently, these difficulties are causing significant concern among CISOs and security professionals.

Introducing Acalvio's solution: ShadowPlex Identity Protection, which tackles these challenges head-on. **This innovative solution combines proactive identity attack surface visibility and reduction with deception-based Identity Threat Detection and Response (ITDR) to fortify identity protection.**

ShadowPlex Identity Attack Surface Management (ASM) provides proactive visibility into the identity attack surface within identity stores and on endpoints, offering a unique "attacker view" for defense teams. This capability allows for the reduction of the identity attack surface, enhancing hygiene through advanced pre-attack stage visibility and management.

In addition, ShadowPlex **provides a novel capability in Identity Attack Paths**, a powerful feature identifying the pathways attackers use to gain access to privileged identities or critical assets. This functionality also empowers defense teams by revealing the potential "blast radius" of an attacker originating from a compromised identity or endpoint.

To bolster identity threat detection, ShadowPlex leverages Honey Accounts and Honeytokens. Honey Accounts are deceptive user and service accounts embedded within identity stores, while Honeytokens are misleading credential profiles found on endpoints. These elements work in tandem to facilitate deception-based ITDR, providing a robust mechanism for **detecting a wide array of identity threats**.



ShadowPlex Identity Protection combines Identity Attack Surface Management and Deception-Based Identity Threat Detection and Response (ITDR)

Empowering the Defense Teams: Taking Back Control

ShadowPlex Identity Protection empowers organizations to:

- Map out attack surfaces within identity repositories, including Microsoft Active Directory (AD), Azure Active Directory (Azure AD), and Active Directory Certificate Services (ADCS).
- Uncover credential caches on crucial assets enterprise-wide, spanning servers, workstations, and laptops.
- Identify credentials within repositories and on endpoints specifically belonging to privileged users such as top executives and system administrators.
- Analyze attack paths originating from endpoints with privileged credentials leading to sensitive information assets.
- Detect instances of credential harvesting on endpoints and attacks targeting AD and other identity repositories.
- Identify and respond to current and evolving identity threats, encompassing stealthy attacks like client-side attacks, offline attacks, and zero-day exploits.
- Enable early detection of identity threats using Honeytokens strategically deployed on endpoints, facilitating response actions to isolate threats and prevent their propagation.
- Leverage deceptive elements to disrupt attacks by misleading and delaying attackers, diverting them from genuine identities, and unveiling their tactics, techniques, and procedures (TTPs).

A Comprehensive Solution to the Identity Attack Surface Challenge

The potential vulnerabilities related to critical identity information and credentials are more extensive than commonly perceived. Within a typical large organization, this encompasses thousands of user and service accounts situated in central identity repositories, which may be over-permissioned or susceptible to theft due to misconfigurations and inadequate security controls. Additionally, various identities, such as local accounts and application accounts, might not be adequately managed within any identity repository. Additionally, the identity attack surface extends to passwords and other credentials that are either temporarily or permanently cached on endpoints.

Active Directory (AD) and Azure AD Assessment

The ShadowPlex AD and Azure AD Assessment offer an attacker's perspective on AD, Azure AD, and ADCS. This capability conducts an in-depth 150+ point analysis of the attack surface within the AD environment, providing visibility into potential security risks. These risks include unprotected administrator accounts, shadow administrators, and over-permissioned accounts. The assessment also identifies misconfigurations and security weaknesses, such as vulnerable service accounts and Service Principal Names (SPNs) susceptible to credential-related attacks like Kerberoasting.

By utilizing advanced AI techniques and security domain knowledge, ShadowPlex AD Assessment maps the exploitable attack surface of AD, Azure AD, and ADCS. What sets it apart is its non-intrusive nature, requiring no special permissions on the domain and having no impact on regular business operations.

Security and identity management teams can leverage the visibility and insights provided by ShadowPlex AD Assessment to address misconfigurations, remediate vulnerabilities, implement the principle of least privilege more effectively, and enhance overall identity hygiene.

Endpoint Zero Trust Assessment

Endpoints store cached credentials within the operating system and installed applications. When attackers establish an initial foothold on an endpoint, they can exploit these cached credentials, opening opportunities to laterally move and compromise other assets. These credentials often involve privileged user and service accounts, and attackers leverage readily available penetration testing tools to gain unauthorized access.

The effectiveness of Zero Trust is contingent on the reliability of secure endpoints. ShadowPlex's Endpoint Zero Trust assessment offers visibility into credential caches on endpoints, where attackers seek to gain access to trusted identities. Additionally, this assessment facilitates a proactive reduction of attack surfaces through the deletion of credential caches.

Additionally, endpoints may harbor legacy security settings that require disabling, and optional security features that remain unutilized. These settings represent an additional attack surface, providing attackers with the potential to access trusted identities on the endpoint. ShadowPlex's Endpoint Zero Trust assessment identifies and highlights the security settings that need enabling or disabling, leading to a reduced attack surface and enhanced
security posture.

Key Asset Visibility

Key assets within an organization encompass critical elements such as endpoints and identities, which include vital business applications, data repositories, infrastructure servers, workstations utilized by the executive team, and privileged identities like service and administrative accounts.

These key assets become prime targets for attackers seeking access to critical systems and sensitive data. To identify these assets, attackers employ offensive tooling. Unfortunately, many organizations lack adequate visibility into their key assets. ShadowPlex addresses this gap by providing automated visibility based on analytics and administrator-specified input.

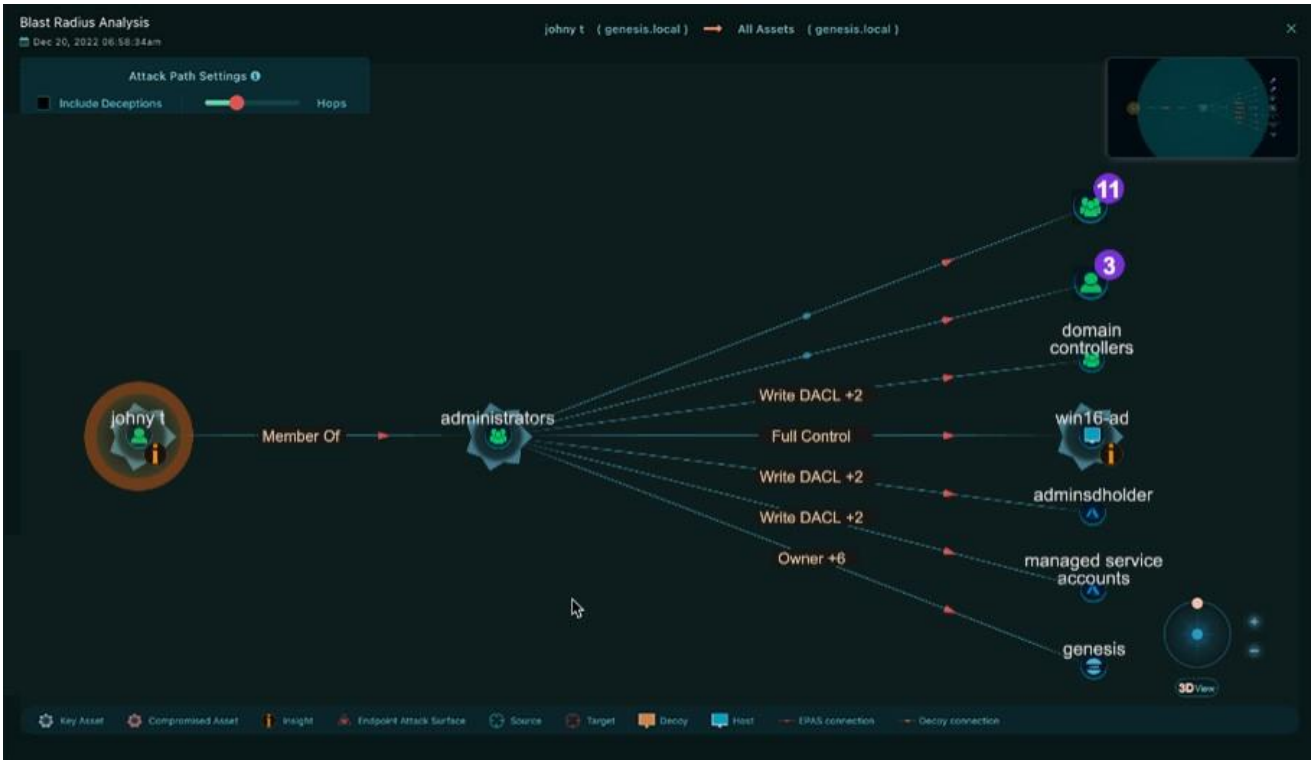
The newfound visibility of key assets offered by ShadowPlex brings significant benefits. It empowers organizations to implement prevention-based strategies for managing their attack surface and deploy effective threat detection strategies, safeguarding these crucial assets. Recognizing and understanding key assets is fundamental to the foundational principles of Zero Trust.

Identity Attack Paths

Security relationships connect assets in many ways, forming pathways that attackers may exploit to gain control over critical assets. ShadowPlex's Identity Attack Paths offer robust visibility, allowing the identification of pathways leading to critical assets or privileged identities.

Additionally, Identity Attack Paths shed light on the various attack paths accessible to an attacker with initial access to an endpoint or an identity. These paths signify the potential "blast radius" of an attack. Leveraging Identity Attack Paths enables proactive mitigation actions to reduce attack paths and enhance overall identity hygiene. This visibility is particularly potent, surpassing the capabilities of traditional security posture management tools, as it operates independently of vulnerabilities.

Organizations can enhance identity hygiene through proactive identity attack surface visibility and reduction,
a crucial prevention-based control mechanism.



Deception-Based Identity Threat Detection and Response (ITDR)

An effective strategy for identity protection involves a layered approach that combines prevention (Identity ASM) and threat detection (ITDR) strategies.

Traditional security solutions cannot differentiate between legitimate and malicious usage of trusted identities. Attackers exploit this limitation by employing stealthy exploits such as client-side attacks, offline attacks, and zero-days to evade traditional security measures.

Deception-based Identity Threat Detection and Response (ITDR) is a powerful solution that provides early and precise detection for a diverse range of identity threats. In this context, ShadowPlex offers Honey Accounts and Honeytokens for achieving deception-based ITDR capabilities.

Honey Accounts

Honey accounts are deceptive user accounts and service accounts created in identity stores.

Honey Tokens

Honeytokens are deceptive credential profiles deployed in identity and application caches on endpoints.

Collectively, Honey Accounts and Honeytokens form a robust system for identifying a wide range of current and emerging identity threats.

ShadowPlex streamlines the management process by generating automated and AI-driven recommendations for Honey Accounts and Honeytokens, making certain that they seamlessly blend into the environment and present an attractive target for potential attackers.

Additionally, ShadowPlex facilitates the automated deployment and periodic refresh of Honey Accounts and Honeytokens at scale, covering multiple domains and tens of thousands of endpoints.

Benefits of Honey Accounts and Honeytokens

Active Defense in Action

ShadowPlex Identity Protection utilizes a blend of Honeytokens and Honey Accounts to achieve the following objectives:

- Alert security and identity teams when stolen or decoy credentials are used.
- Deflect and confine attacks by diverting them toward Honey Accounts and away from legitimate accounts.
- Slow down and impede threat actors, introducing delays and causing them to distrust their tools, which changes the economics of the attack.
- Expose the TTPs of threat actors as they maneuver laterally, using Honeytokens. This information enables security teams to prioritize and enhance security controls.

Honey Accounts and Honeytokens provide notable advantages for security teams. The key advantages include:

- **Comprehensive Identity Threat Detection:** Uncovering a wide range of current and evolving identity threats that may elude traditional security solutions.
- **Early Threat Detection:** Enabling swift response actions to prevent the further spread of an attack.
- **High-Fidelity Threat Detection:** Supplying actionable intelligence for Security Operations Center (SOC) and Incident Response (IR) teams.
- **Diversion/Slow Down/Misleading of Attackers:** Safeguarding critical assets by redirecting, impeding, or misleading attackers in their activities.

Enterprise-Scale Identity Protection Made Effortless

ShadowPlex Identity Protection provides extensive protection for enterprises, **spanning multiple domains** and **tens of thousands of endpoints**. The deployment of ShadowPlex is **agentless**, eliminating the administrative and security challenges typically associated with adding extra agents.

Conclusion

Threat actors have developed highly effective techniques for capturing and exploiting identities, techniques that evade detection and neutralization by conventional directory management and passive defense security tools.

The need for IT organizations to strengthen credential protection and swiftly detect identity-based attacks has never been more pressing. This necessity arises from the need to prevent data breaches, establish robust zero-trust security models, and optimize returns on investments in existing security and IT management tools.

The Acalvio ShadowPlex Identity Protection solution provides an effective and efficient solution to tackle identity challenges:

- A comprehensive solution for identity attack surface management, which provides deep visibility into distributed endpoints and central identity repositories.
- An active defense solution with identity deceptions precisely designed to uncover credential-based attacks.
- Integrated with security and identity management tools, enhancing advanced analytics, accelerating response and remediation, and automating enterprise-scale active defense.

LEARN MORE

ACALVIO

Acalvio is the leader in autonomous cyber deception technologies, arming enterprises against sophisticated cyber threats including APTs, insider threats and ransomware. Its AI-powered Active Defense Platform, backed by 25 patents, enables advanced threat defense across IT, OT, and Cloud environments. Additionally, the Identity Threat Detection and Response (ITDR) solutions with Honeytokens enable Zero Trust security models. Based in Silicon Valley, Acalvio serves midsize to Fortune 500 companies and government agencies, offering flexible deployment from Cloud, on-premises, or through managed service providers.

For more information, please visit www.acalvio.com