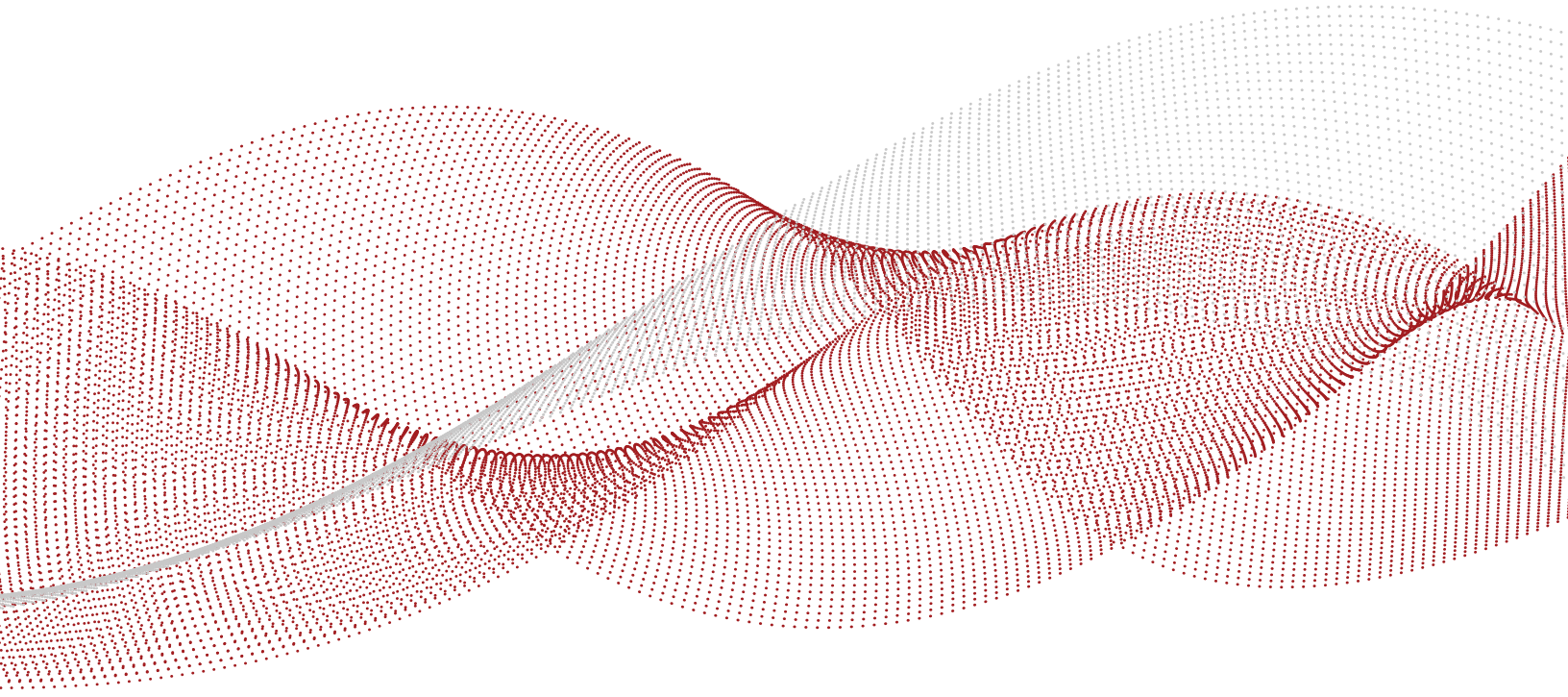
ShadowPlex Identity Protection

A comprehensive identity threat detection and response (ITDR) solution that defeats identity-based attacks with identity attack surface management and active defense



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 Forecast* 2023

The ITDR Solution That Protects Credentials Everywhere and Detects Identity-Based Attacks

Protecting employee credentials has become the #1 priority of many IT security organizations. With good reason: according to Verizon's 2022 Data Breach Investigation Report, credential-based attacks have become the top path for threat actors to reach enterprise information assets. In addition, secure credentials are a prerequisite for implementing a zero trust security model.

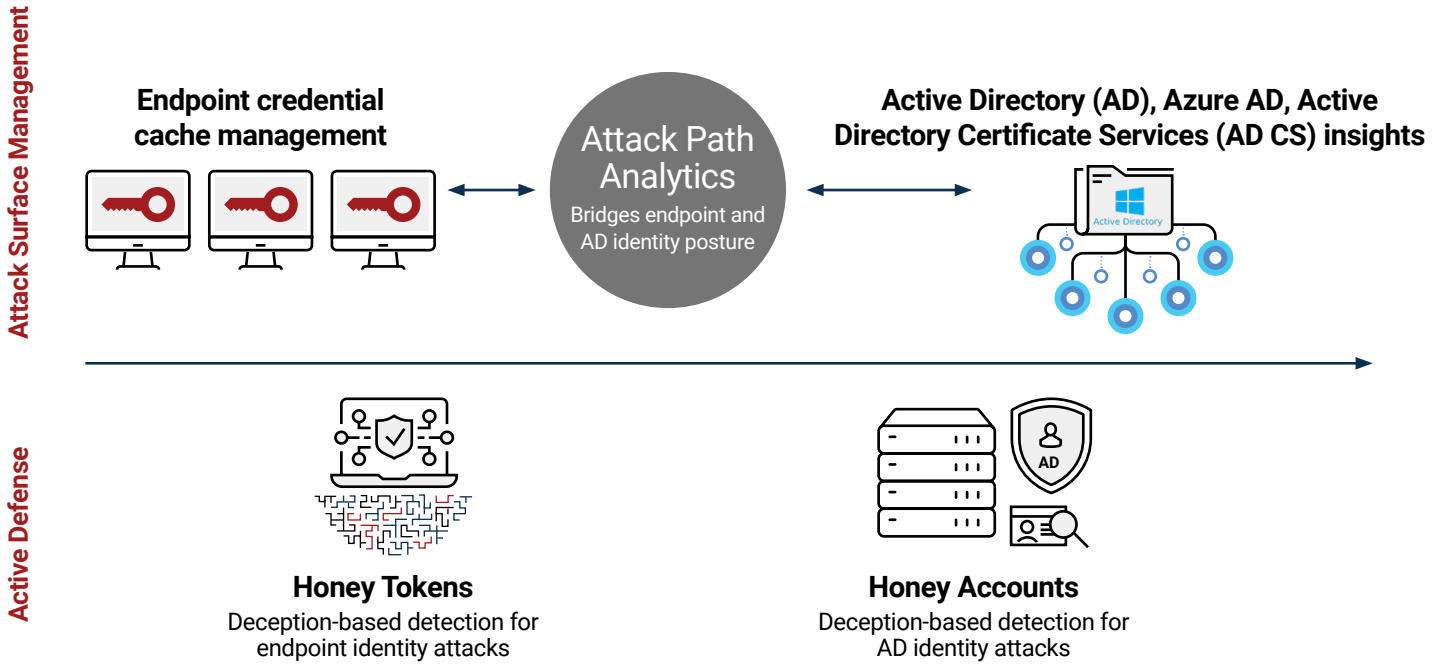
However, most organizations struggle to protect credentials and prevent their misuse by attackers. Many security and identity management teams focus on protecting central identity repositories, but find it difficult to locate and protect credentials on key endpoints across their enterprises. Compounding the problem, IT groups have few good tools to detect and neutralize attacks that exploit stolen credentials. These serious challenges cause many sleepless nights for CISOs and security professionals.

Until now. Acalvio addresses these challenges with ShadowPlex Identity Protection, an identity threat detection and response (ITDR) solution that provides visibility into organizations' identity attack surfaces and robust capabilities to detect and respond to identity-based attacks.

ShadowPlex Identity Protection delivers comprehensive identity attack surface management. It enables organizations to protect credentials in enterprise directories and on endpoints. It offers visibility into endpoint credential caches and generates insights into potential security weaknesses related to identities stored in Active Directory (AD), Azure AD, and Active Directory Certificate Services (AD CS).

In addition, ShadowPlex Identity Protection provides attack path analytics. It bridges the gap between identity repositories like AD and endpoint credential caches to show pathways that attackers can exploit to reach information assets.

Finally, ShadowPlex Identity Protection supplies deception tools to identify and thwart identity-based attacks. "Honey accounts" in Active Directory and "honey tokens" in endpoint credential caches allow security and identity management teams to detect malicious activities while attackers waste time trying to exploit decoy credentials.



ShadowPlex Identity Protection combines attack surface management and active defense

ShadowPlex Identity Protection enables organizations to:

- Map attack surfaces in identity repositories such as such as Microsoft Active Directory (AD), Azure Active Directory (Azure AD), and Active Directory Certificate Services (AD CS)
- Discover credential caches on key assets across the enterprise, including servers, workstations, and laptops
- Identify which credentials in repositories and on endpoints belong to privileged users such as top executives and system administrators
- Identify and analyze attack paths from endpoints with privileged credentials to sensitive information assets
- Detect credential harvesting on endpoints and attacks on AD and other identity repositories
- Alert security operations centers to privilege escalation attempts and access requests that use stolen credentials
- Use deceptive elements to disrupt attacks by misleading and delaying attackers, luring them away from real data and applications and exposing their tactics, techniques, and procedures (TTPs)

A Comprehensive Solution to the Identity Attack Surface Challenge

The attack surface of critical identity information and credentials is far larger than most people imagine. In a typical large organization, it includes thousands of user and service accounts in central identity repositories that are over-permissioned or exposed to theft through misconfigurations and weak security controls. Other identities such as local accounts and application accounts may not be managed in any identity repository. The identity attack surface also includes passwords and other credentials temporarily or permanently cached on endpoints.

Identity repositories

ShadowPlex Identity Protection provides visibility into potential security risks created by unprotected administrator accounts, shadow administrators, and over-permissioned accounts. It also identifies misconfigurations and security weaknesses such as service accounts and Service Principal Name (SPN) accounts that are vulnerable to password-stealing kerberoasting attacks.

ShadowPlex Identity Protection employs advanced AI techniques and security domain knowledge to map the exploitable attack surface of enterprise directory services such as AD and Azure AD, as well Microsoft 365 Email and other applications, storage systems, database servers, and virtual machines. It does not require special privileges or permissions on domains or affect the operation of the repositories.

Security and identity management teams can use visibility and insights generated ShadowPlex Identity Protection to fix misconfigurations, remediate vulnerabilities, better apply the principle of least privilege, and strengthen identity management processes.

Endpoint credential caches

Most organizations have little or no visibility into the profusion of credential caches distributed around the typical enterprise.

ShadowPlex Identity Protection discovers user, application, and operating system credentials and profiles stored in browser histories, user profiles, application modules, and other locations on laptops, workstations, servers, and other computing systems.

Security teams not only gain visibility into caches and their contents, they also have the option of automatically deleting cached credentials or replacing them with decoy credentials that can be used for deception. ShadowPlex does this by leveraging existing security infrastructure, so no additional agents need to be installed on the endpoints.

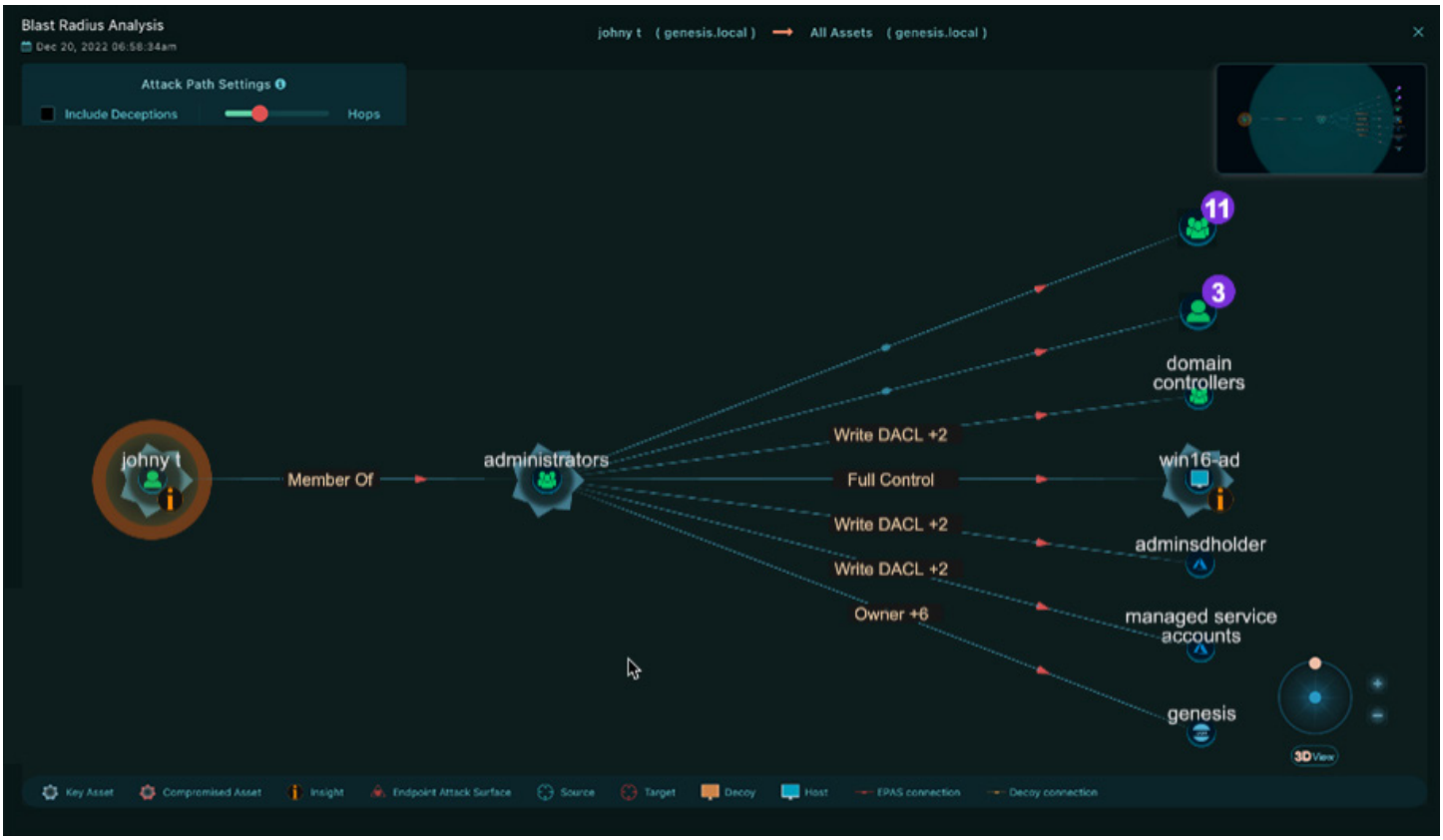
Endpoint attack surface management

ShadowPlex Identity Protection helps security teams reduce the attack surface of endpoints. It identifies potential weaknesses and recommends actions such as disabling insecure protocols and features and enabling additional security controls. It also identifies cached pathways to databases, web servers, and other assets that attackers can use for lateral movement.

Attack paths

After attackers steal credentials, they attempt to find potential attack paths to information assets such as databases and document repositories – and to enterprise directories and other sources of credentials that give them access to even more assets. These attack paths involve exploitable chains of relations between user accounts, systems, and applications that are extremely hard to detect using conventional security and network tools, especially when attackers leverage existing trust relationships.

ShadowPlex Identity Protection detects and maps these potential attack paths so security and identity management teams can take measures to break them, such as removing credential caches on endpoints, fixing misconfigurations in identity repositories, limiting overly broad permissions for privileged accounts, and tightening controls around key assets.



Example of ShadowPlex Identity Protection mapping attack paths to key assets

ShadowPlex Identity Protection leverages multiple data sources to provide far more detailed maps and actionable information than can be obtained from security tools that focus on directories alone. It also includes attack paths that do not rely on known vulnerabilities and misconfigurations, and are therefore invisible to traditional scanning technologies.

Why multiple data sources make a difference

ShadowPlex Identity Protection leverages data from multiple sources to provide security teams with visibility and actionable insights that current identity solutions can't provide. Data sets include:

Endpoint and asset discovery

AD, Azure AD, and Microsoft 365 Email discovery

Neighborhood discovery

Network sessions

Endpoint and identity attack surface analysis

Vulnerability data feeds

How does this produce more insights than a system that relies on only one or two data sources, and how do these insights enable organizations to quickly reduce their identity attack surface? Here is an example.

Suppose a large set of user credentials is found in a browser cache on an endpoint connected to the internet. Do all of them require immediate attention? Any of them? How long will it take to find out?

ShadowPlex Identity Protection might check the credentials against the associated accounts in AD and find that one of them belongs to a system administrator in one business unit, who has access to an administrative system in the corporate data center, which provides access to the password change system for the entire enterprise. Within minutes, the security team can eliminate this critical risk by deleting the browser cache, or cutting back the system admin's permissions, or tightening access to the administrative system or the password change system, or some combination of these steps.

Active Defense for Credential-Based Attacks

A typical enterprise has thousands of identities and many attack paths that cannot be rectified easily. ShadowPlex provides compensatory controls to protect such attack paths. By deploying and monitoring two types of deceptive elements, it allows enterprises to actively defend and protect privileged users, service accounts, crown jewel assets, and domain controllers.

Honey accounts

Honey accounts are deceptive accounts created in the AD and Azure AD that can be accessed by deceptive credentials cached on endpoints. ShadowPlex Identity Protection automatically recommends honey accounts by analyzing naming patterns in AD and the types of attacks the organization typically encounters. Security and identity teams can further configure recommended honey accounts as needed.

Honey tokens

Honey tokens are deceptive elements deployed in endpoint credential caches. They are associated with honey accounts in AD, Azure AD, or AD CS. They can also replace existing valid credentials in endpoint credential caches.

Active Defense in action

ShadowPlex Identity Protection leverages the combination of honey tokens and honey accounts to:

- Alert security and identity teams when stolen and decoy credentials are used
- Deflect and contain attacks by steering them away from valid accounts to honey accounts
- Slow and frustrate threat actors
- Expose the TTPs of threat actors as they move laterally and take actions with honey tokens, giving security teams information to prioritize and improve security controls

By combining identity attack surface management with active defense built on honey accounts and honey tokens, Acalvio's ShadowPlex Identity Protection enables security and identity management teams to:

- Find and track the use of stolen credentials and privilege escalation attempts
- Protect key users and accounts in AD, Azure AD, and other identity repositories
- Detect attempts to steal credentials, including Pass-the-Hash (PtH) and Pass-the-Ticket (PtT) attacks
- Detect attacks against domain controllers and identity-based services such as Active Directory Certificate Services (AD CS)

It also provides a means to reveal activities by rogue insiders that are otherwise extremely difficult to uncover. Examples include attempts by employees or contractors to use credential-stealing tools, escalate privileges, or access decoy versions of high-value assets like password lists, customer databases, and documents containing intellectual property.

Extensive Integration with the Security Ecosystem

Integrations to support advanced analytics

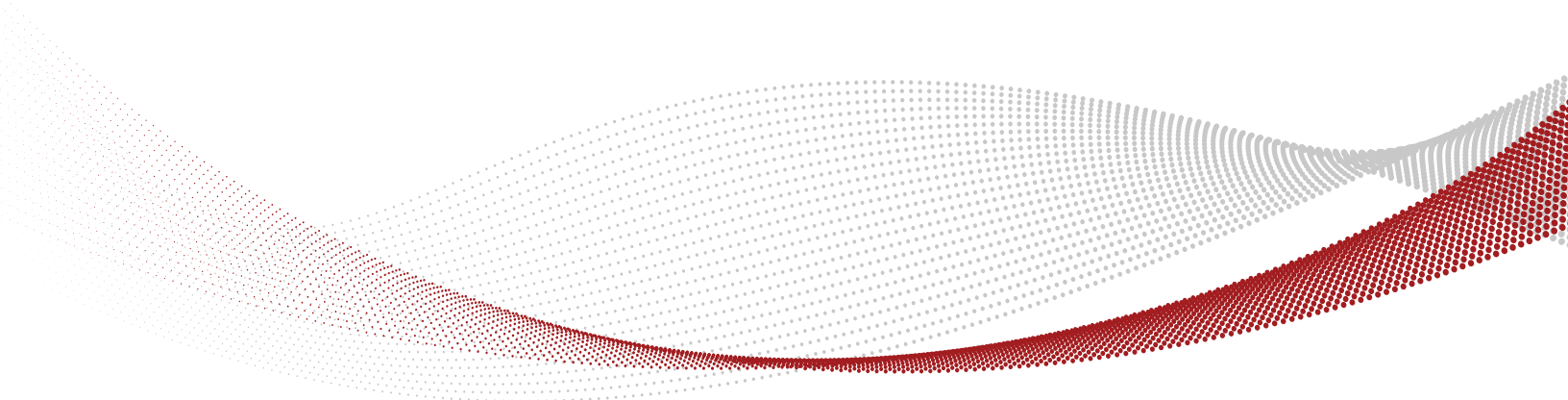
ShadowPlex Identity Protection integrates with an array of IT products to provide data and insights for security and identity management teams. Integrations with threat intelligence platforms, network monitoring tools, cloud security platforms, malware sandboxes, IAM solutions, and IT management tools enhance a variety of analytics capabilities, including:

- Attack path mapping to identify and reduce lateral movement to enterprise "crown jewels."
- Active defense to connect detection events to possible attacks on key assets.
- Blast radius analysis to identify the potential impact if a given endpoint or identity is compromised.
- What-if analysis to estimate the impact on security of making policy changes, applying software patches, and changing network routing.
- Ranked attack surface analysis to prioritize remediation actions based on the pathways to key assets.

Integrations to support response, remediation, and active defense

ShadowPlex Identity Protection also integrates with a range of incident response and system remediation tools such as security information and event management (SIEM), security orchestration, automation and response (SOAR), and endpoint detection and response (EDR) products, as well as configuration interfaces of enterprise directories like AD and Azure AD.

These integrations help security and identity management teams to stop credential-based attacks before they cause damage and automate time-consuming remediation processes.



Conclusion

IT organizations have more reasons than ever to strengthen their ability to protect credentials and swiftly detect identity-based attacks: to prevent data breaches, to enable zero trust security models, and to obtain better results and a higher ROI from investments in existing security and IT management tools.

Unfortunately, threat actors have developed very effective techniques to capture and exploit legitimate credentials, techniques that cannot be detected and neutralized by conventional directory management and passive defense security tools.

Acalvio's ShadowPlex Identity Protection solution is the answer. It is:

- The only comprehensive solution for identity attack surface management, bridging distributed endpoints and central identity repositories.
- An active defense solution that offers identity deceptions specifically designed to uncover credential-based attacks.
- Integrated with security and identity management tools that enhance advanced analytics, accelerate response and remediation, and automate enterprise-scale active defense.

LEARN MORE

ACALVIO

Acalvio, the leader in cyber deception technology, helps enterprises actively defend against advanced security threats. Acalvio Active Defense Platform, built on 25 issued patents in autonomous deception and advanced AI, provides robust solutions for Identity Threat Detection and Response (ITDR), Advanced Threat Detection, OT Security, Zero Trust, Active Directory Protection and Ransomware Protection. The Silicon Valley-based company's solutions serve Fortune 500 enterprises, government agencies and are available to deploy on-premises, in the cloud or via marquee managed service providers. For more information, please visit **www.acalvio.com**