ACALVIO

SOLUTION BRIEF

Acalvio ShadowPlex™ Active Directory Protection

ACTIVE DIRECTORY: THE MODERN ATTACK FOCAL POINT

Active Directory (AD) is at the core of most enterprise infrastructure, and it holds valuable and critical information about user identities, network assets, applications, services, policies, and authentication data. However, given the legacy architecture principles that AD was built upon decades ago, completely securing this crown jewel with today's diverse technology and infrastructure complexity has been a challenge for most organizations. This challenge is compounded by the rapid and sophisticated evolution of the threat landscape.

The Active Directory vulnerability vector is not limited to software defects, its distance from the network periphery, or isolation and firewall configurations. Most attacks against Active Directory stem from the way it is configured in any organization. Active Directory stores multiple types of objects, each with hundreds and thousands of properties for access, authentication, authorization, and transactional rules. Protecting Active Directory and reducing the attack surface comes down to intimately understanding the object configurations and how these rules can be misused by threat actors. This is not just a security responsibility but implies rewriting the rules of how IT management is carried out in every organization. This can perhaps explain why Active Directory protection is complex, involved, and takes continuous monitoring and course correction in policy definitions to minimize the attack surface.

This raises the question—what constitutes a compelling AD Protection solution?

CURRENT DEFENSE AND DETECTION SYSTEMS

Most detection and security systems today are built on agent-based behavioral detection solutions, EDR alerts, atypical behaviors flagged by UEBA, AD event log monitoring, SIEM-based event correlation, SOC triaging, and manual investigation and aftermath threat hunting. While these methods do offer a certain degree of defense capabilities, most malicious activities targetting the AD are performed with valid domain credentials that typically go undetected when such traditional methods of detection are employed. When it comes to securing critical infrastructure, components like Active Directory need a more compelling **Active Defense** strategy. **The MITRE Engage™** is an active defense knowledgebase that lists multiple tactics spanning channel, collect, contain, detect, disrupt, facilitate, legitimize, and test. Using **Deception techniques** across all of these tactics for detection, engagement, and counterattack takes center stage in the matrix. This is a compelling framework to build a stronger, proactive AD defense strategy.

ACALVIO SOLUTION FOR ACTIVE DIRECTORY PROTECTION

Acalvio ShadowPlex is an **autonomous deception platform** that provides an AI-based deception solution for Active Directory protection. ShadowPlex's strong capabilities include **preventing** attacks on Active Directory by providing **continuous visibility** into possible attack surfaces, **predicting** the attacker's path, slowing down, confusing or diverting the attacker, predicting and detecting the TTP at every stage, and ultimately, even selectively changing the attacker's perception of the network.

Active Directory attacks are performed in multiple phases—ranging from reconnaissance, discovery to lateral movement, establishing persistence, defense evasion to data exfiltration, and domain trust abuse. Each phase is related to a certain type of activity in a cyber attack. Each phase also presents an opportunity to stop the cyber attack in progress. ShadowPlex offers **advanced detection techniques** using novel **pre-built Deceptions** to detect attacks in real-time, at every stage of the kill chain.

PREDICTIVE ANALYTICS: REDUCE ACTIVE DIRECTORY RISK EXPOSURE & PREDICT ATTACKS PATHS

Active Directory InSights™

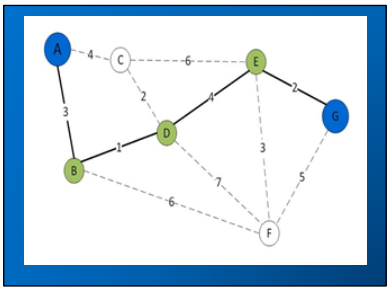
*ShadowPlex **Active Directory InSights™** presents an **Attacker's View** of the network and reveals the attack surface and risk exposure in the production domains.*

Advanced attacks targetting or using AD as conduits exploit domain-connected endpoints. This provides the attackers the ability to enumerate all the data in the AD domain. They can obtain visibility into specific misconfigurations of AD objects and they are used as vehicles for progressing the attack. For instance, tools such as PowerView have modules that can enumerate computer accounts marked for unconstrained delegation. Attackers use such offensive tools to find their targets in the domain for escalating privileges. The defense teams **need a dedicated "Attacker's View"** of the network to combat such offensive moves – and this capability is provided by **ShadowPlex AD InSights™.**

The first step in reducing the attacker's chance for success is to reduce the attack surface. ShadowPlex leverages the threat intelligence from various sources using pre-built integrations and builds an **attacker's view of the network** that can be invaluable for the defense teams to **proactively** reduce the attack surface. The ShadowPlex AD InSights provides security and IT administrators, continuous visibility into potential security risk exposure introduced by factors such as unprotected administrator accounts, shadow administrators, over-permissioned accounts, kerberoastable accounts, unmanaged SPNs, and service accounts, among other misconfigurations. ShadowPlex generates these extensive insights spanning user and computer accounts, groups, GPOs, ACLs, domains, forests and trust relationships, and other AD artifacts. The AD InSights engine is powered by AI Threat Models that use data from real and evolving attacks against the Active Directory.

Even in modestly complex Active Directory environments, it can often be a challenge to track objects and present the attack surface. ShadowPlex solves this **problem without requiring any manual intervention**. ShadowPlex **does not require** any special privileges or permissions on the domain to generate the attack surface insights.

Attack Path Analysis



In any enterprise, with continuous growth and restructuring, there is a complex and evolving ecosystem of users, computers, groups, GPOs, and other objects. Management blind spots, vulnerabilities, misconfigurations, and inadequate access controls in the AD present a significant security risk. Attackers leverage AD misconfigurations and vulnerabilities to identify attack paths that facilitate lateral movement and privilege escalation to compromise valuable assets on the network.

Attackers use tools such as BloodHound to analyze the attack paths on the network and even find the shortest path to their targets. **ShadowPlex Attack Path** provides the powerful capability for the defense teams to proactively predict these attack paths and remediate them to significantly reduce the exposure.

A typical enterprise may have many viable attack paths that can potentially lead attackers to their targets. ShadowPlex Attack Path combines AI-based **Advanced Deception** with **Graph Theory** to **identify** attack paths involving **exploitable chains of relations**. Each graph represents potential paths that adversaries can traverse from exploitable accounts or endpoints to reach valuable assets on the network.

These Predictive Analytics-based ShadowPlex features serve as powerful **Active Defense** tools to **proactively** disrupt viable attack paths to valuable assets and add deceptions to strengthen defenses.

ACTIVE DIRECTORY PROTECTION USING SHADOWPLEX DECEPTIONS

ShadowPlex provides a pre-built curated palette of non-fingerprintable deceptions designed specifically to detect advanced Active Directory attacks, such as:

Malicious activity against Active Directory are hard to detect using traditional methods since the attackers use legitimate domain credentials, SPNs and domain authenticated endpoints.

- **KERBEROASTING**
- **AS-REP ROASTING**
- **UNCONSTRAINED DELEGATION COMPUTER ATTACKS**
- **RECON ATTACKS**
- **DCSYNC**
- **AZURE AD CONNECT ATTACKS**
- **ADFS/GOLDEN SAML**

Acalvio offers an extensive **variety of deceptions that is fundamental to Active Directory protection**.

ShadowPlex provides **pre-defined** Active Directory Protection Deceptions that combine **targeted deceptions** with AI. Deceptions for AD consist of Decoy Computers, Services, User and Service Accounts, and SPNs that are **recommended by the AI engine** to seamlessly blend into the AD environment.

Attacks against Active Directory are hard to detect and sometimes even undetectable given that they use legitimate domain credentials, service accounts and domain authenticated computers. Detection using traditional triaging or event log monitoring does not surface conclusive malicious activity.

Let us consider the case of a Kerberoasting attack. This attack typically involves four steps:

SPN Discovery → **Request Service Tickets** → **Extract Service Tickets** → **Crack Service Tickets**

Of these, the first two steps are part of the normal Kerberos protocol function and do not indicate any anomalous behavior since legitimate SPNs are used. Extracting the Service Ticket to an attacker-controlled system and cracking the ticket by dictionary or brute-force is carried out outside the enterprise network and these steps do not generate any domain traffic or account lockouts, making them undetectable. ShadowPlex AD Deceptions are a novel way to detect such attacks since the SPNs or deceptive accounts are not meant to be used in the enterprise function workflow in the first place.

The deceptions are registered in the production AD. ShadowPlex supports on-premises AD deployments, Azure AD, and Hybrid AD deployments.

AUTO RECOMMENDATION AND PLACEMENT OF DECEPTION ENTITIES

An effective deception strategy should include deceptions that blend into the enterprise environment.

ShadowPlex Deceptions detect a wide range of TTPs spanning all steps from initial action or reconnaissance to exfiltration and impact.

In large, complex Active Directory environments, determining the type and placement of deceptions is a practical challenge for enterprises. ShadowPlex uses AI algorithms to auto-recommend the right type of entity names and attributes such as unique identifiers for SPNs, best-practice conventions for service accounts among others to make deceptions attractive to attackers. ShadowPlex also devises an effective deception placement strategy to divert attackers away from assets and toward decoys. This capability removes the burden of IT teams manually specifying the properties and placement of deceptions.

Auto recommendation and placement of deceptions is not a one-time activity. Active Directory environments undergo constant change. As a result, deception strategy, deployment, and placement must be reviewed periodically. ShadowPlex runs in autonomous mode, auto-discovers changes, and appropriately adjusts deceptions to blend with the network. It recommends relevant, new deceptions without requiring manual intervention. This is a unique capability aimed at ensuring that deceptions are current and dynamic.

ShadowPlex's dynamic deceptions combined with AI for blending and recommendation ensure that the deception quality and realism are best-in-class.

DECOY CONTAINMENT

ShadowPlex has the ability to contain Deceptions (Decoy Computers and Service Accounts/Users) to ensure that attackers cannot use these deceptions to cause harm to the production network. For example, Decoy Computers are contained using the patented *ShadowPlex Deception Farms Architecture*. **Attackers cannot disable ShadowPlex containment.** This ensures that attackers cannot leverage the Decoy as a pivot point to mount attacks against the production network. Similarly, Service Accounts have in-built containment to ensure that attackers cannot use these accounts to gain access to production assets.

AI-BASED TRAVERSAL ANALYSIS

ShadowPlex provides a capability for viewing real-time attack progression. ShadowPlex generates the traversal path by leveraging advanced AI techniques. The path shows possible routes that a threat may have taken to reach the asset under investigation.

AUTOMATED RESPONSE

Given the malicious nature of Active Directory attacks, robust containment of an attacker is a requirement. Acalvio ShadowPlex offers comprehensive and automated response mechanisms and leverages integrations with SOAR, EDR, and Network Management solutions for automated actions such as the ability to **isolate or quarantine compromised endpoints, kill a malicious process, or complete shutdown**. Additionally, ShadowPlex also offers effective responses such as **Diverting an Attacker** away from production assets to adjacent decoys to protect the real assets. Another response mechanism is to **Slow Down** the attacker's progress by deploying several identical deceptions to surround the production asset while ShadowPlex surfaces the **attacker's trajectory** for quick defense and IR actions.

CONCLUSION

Timely detection and response to Active Directory attacks are crucial in limiting the impact on business operations. Through a combination of Deception Technology and AI, enterprises can effectively thwart attackers' attempts to move laterally through the network to reach the AD.

Acalvio ShadowPlex is an autonomous deception platform that provides rapid detection, advanced threat investigation, analysis, and automated response capabilities. It is designed to proactively reduce the attack surface and protect the enterprise Active Directory against attacks without adding unnecessary complexity, cost, and IT overheads.

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