ACALVIO

SOLUTION BRIEF

Acalvio ShadowPlex for Public Sector Organizations

How government agencies can use cyber deception to advance Zero Trust maturity

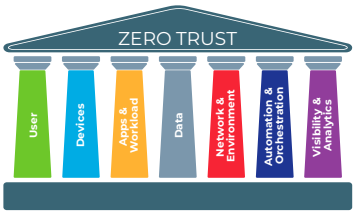
Zero Trust and the Assume Breach principle

Zero Trust is a security framework that assumes that no one inside or outside the network can be trusted unless their identity and access is verified. Zero Trust shifts the focus from a perimeter and prevention centric defense strategy to a strategy that is centered around protecting the critical assets and sensitive data. Zero Trust Architecture (ZTA) is based on the foundational principles of: least-privilege access, continuous verification and assume breach.

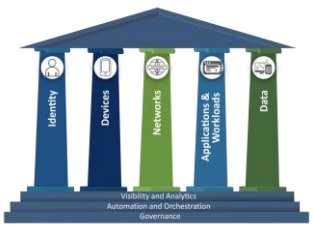
The *assume breach* principle of ZTA highlights that the organization must assume that an adversary has obtained an initial foothold in the environment. The goal of defense teams should be to detect threats and prevent the adversary from compromising the critical assets.

Zero Trust Models

Federal agencies, including the Department of Defense (DoD) and the Cybersecurity and Infrastructure Security Agency (CISA) have published reference models for Zero Trust. The DoD reference architecture has a 7-pillar model while the CISA model has 5 pillars with a set of 3 cross-cutting capabilities that span across the pillars.



DoD: Zero Trust Pillars



CISA: Zero Trust Maturity Model

Visibility and Analytics

Visibility and Analytics is a cross-cutting capability in the CISA Zero Trust model. This capability relates to providing defense teams with improved visibility to cyber threats. Traditional security solutions are focused on detecting known threats with specific attack TTPs. Modern adversaries are leveraging stealthy and evolving offensive techniques to evade traditional security solutions, resulting in gaps in threat detection. It is essential for defense teams to expand visibility for threat detection and eliminate these detection gaps. Additionally, traditional security solutions have a high rate of false positives, resulting in alert deluge for SOC teams. SOC teams are unable to keep pace with the high alert volume, resulting in alerts remaining uninvestigated and missing opportunities to detect threats.

What is Active Defense and Cyber Deception

Active Defense is a proactive approach to cybersecurity, based on predicting the goals of the attacker, changing the attacker's landscape, detecting and diverting/slowing down the attacker, taking the attacker away from the real assets. Cyber Deception sets relevant traps for the adversary through the strategic introduction of fake (deceptive) entities into the environment and observe for interactions with these traps. Deceptions are not used in existing IT or business workflows, any interaction with a deception is an immediate indication Deception-based threat detection is agnostic to attacker TTPs and enables defense teams to detect current and evolving threats,

Acalvio ShadowPlex

Advancing Zero Trust maturity through cyber deception

Zero Trust is a strategy and a framework. Organizations are at different stages of maturity in their implementation of Zero Trust. With the escalating volume of breaches and associated impact and cost, organizations are looking to strengthen their Zero Trust implementation maturity. Cyber deception plays an important role in this, improving the visibility for cyber threats and providing high fidelity, actionable alerts for SOC teams, reducing the alert deluge.

How deception improves cyber visibility

Organizations can deploy deceptions that represent assets across the Zero Trust pillars, including identities, devices, applications, data, and network. This provides improved cyber visibility for threats targeting assets across any of the pillars of the ZTA. Deception technology provides **expanded threat detection coverage** by detecting threats that evade traditional security solutions, **improves SOC efficiency** through high fidelity detection, and enables proactive **threat hunting** through deceptions to identify latent threats and confirm hypothesis. The improved cyber visibility makes **deception a necessary solution** for a **mature implementation of visibility and analytics** in a Zero Trust Architecture.

Acalvio ShadowPlex: Enterprise-scale Active Defense

Acalvio ShadowPlex is a robust and proven Active Defense platform that combines cyber deception and AI to provide proactive threat defense to organizations. The key capabilities of ShadowPlex are

- Offers a comprehensive and extensible deception palette that includes highly realistic decoys, breadcrumbs, baits, honey accounts, and honeytokens tailored for different computing environments and attack types
- Protect assets across all the Zero Trust pillars (identities, devices, applications, data, and network)
- Deploys distributed deception at enterprise scale, across on-premises IT and OT networks and cloud workloads
- Provides playbooks for pre-packaged solutions to use cases, providing immediate time to value
- Uses AI-driven automation to design, customize, deploy, and manage thousands of deception elements without burdening security teams
- Does not require endpoint agents or affect existing infrastructure or applications
- Auto triaged alerts that provide actionable intelligence for SOC teams and are mapped to the MITRE ATT&CK framework for standardized incident response
- Integrates with SOAR, SIEM, EDR, cloud security, network management, and other security and IT management tools to ensure interoperability with the enterprise security ecosystem

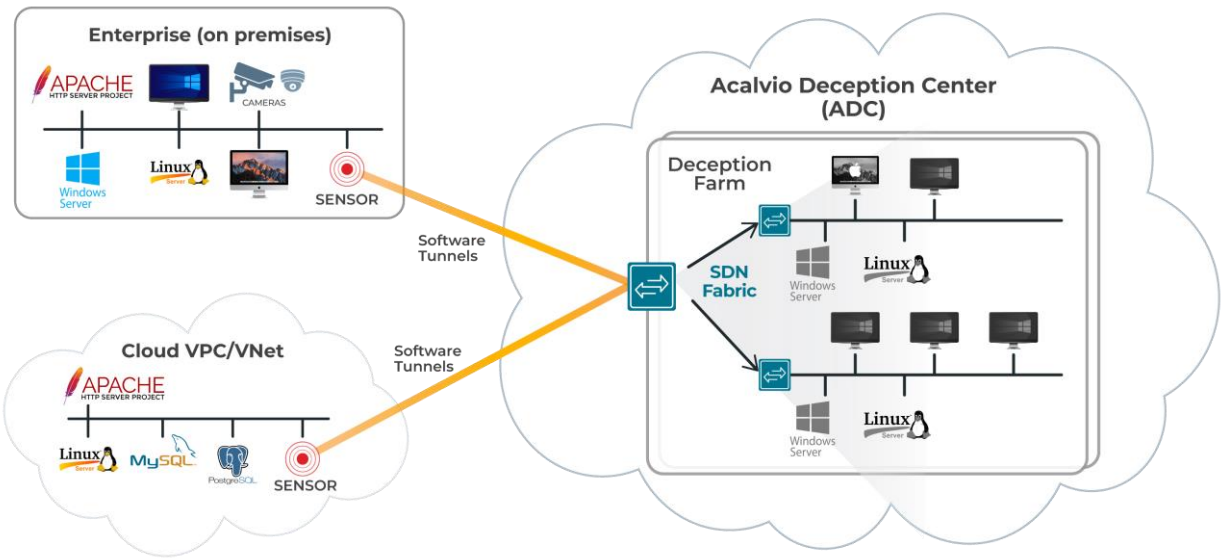


Figure 1: Acalvio ShadowPlex Architecture; ShadowPlex deploys deception elements to an organization's computing environment that are strategically placed to detect adversaries early in the attack lifecycle and with precision. The deceptions steer adversaries away from valid information assets and alert security teams to their actions.

Use cases of ShadowPlex deception to improve cyber visibility and advance Zero Trust Maturity

ShadowPlex deceptions support an extensive set of use cases to enable organizations to improve their cyber visibility and advance the Zero Trust maturity. **The primary use cases include:**

Living Off the Land (LotL) attacks, AI-fueled attacks, and zero days

APT threats and modern adversaries are using built in operating system utilities and tools for offensive actions, known as living off the land (LotL) attacks. Adversaries are increasingly leveraging AI for polymorphic malware variants that are unique for each execution cycle. LotL attacks, AI-fueled attacks, and zero days bypass traditional security solutions, resulting in detection gaps for defense teams. ShadowPlex provides purpose-built deceptions (baits, honeytokens) that detect these threats with precision, providing SOC teams with visibility to these evasive threats.

Identity threats

Identity-driven attacks are increasing, with adversaries targeting the identity architecture to elevate privileges and leverage the privileged identities for lateral movement. Traditional security solutions are unable to distinguish between legitimate and malicious use of identities. Identity threat detection and response (ITDR) is a detection approach focused on detecting identity threats. ShadowPlex provides honey accounts deployed into identity stores and honeytokens deployed on endpoints to provide an effective deception-based ITDR solution to detect identity threats early and with precision.

Insider threats

Insider threats range from accidental or careless insiders to rogue administrators with privilege. Insiders have trusted access to the resources in the organization. Traditional security solutions have gaps in detecting insider threats, with the trusted access of insiders making it hard to detect using anomaly or log analytics-based detection. Cyber deception is an effective approach to detect insider threats. By embedding ShadowPlex deceptions (honey accounts, honeytokens, baits) into the identity stores, critical assets, and data repositories, defense teams gain visibility to the stealthy insider threats and expand threat detection coverage.

Threats targeting and originating from unmanaged endpoints

Unmanaged endpoints (legacy workstations, printers, cameras) are not compatible with agent-based security solutions such as endpoint detection and response (EDR). Attackers target these endpoints as SOC teams have limited to no visibility to these threats. ShadowPlex provides decoys representing unmanaged endpoints to detect threats attempting lateral movement to such endpoints, providing visibility for threats targeting unmanaged endpoints . ShadowPlex honey accounts are added to identity stores to detect attacks originating from unmanaged endpoints.

Threats targeting OT, ICS and IoT assets

OT, ICS and IoT environments are increasingly subject to a wide variety of cyber threats. Specialized form factors of these devices, incompatible with agent-based security solutions (such as EDR) making these assets as attractive targets for attacks in the OT environment. ShadowPlex provides an extensive set of deceptions (decoys, breadcrumbs, baits) that detect threats targeting OT assets. ShadowPlex OT decoys represent OT specific assets, including PLCs, HMIs, Controllers.

Novel ransomware variants

Ransomware attacks are gaining in sophistication, with ransomware as a service (RaaS) groups generating novel ransomware variants to bypass traditional security solutions. ShadowPlex deceptions provide early and precise detection of ransomware, including novel ransomware variants through the strategic deployment of deceptions for each stage of the ransomware attack lifecycle. This provides improved visibility for SOC teams to isolate the threat and protect the critical assets.

Defense evasion to disable agent-based solutions

Modern adversaries elevate privileges and perform defense evasion to disable agent-based security solutions, clear logs to erase evidence of offensive actions. This results in detection gaps for defense teams. ShadowPlex is an agentless platform and the deceptions (honeytokens, baits) are deployed to caches on endpoints, providing independent detection capability and visibility for threats when agent-based defenses have been disabled and log evidence has been cleared by the adversaries.

Active Defense in Zero Trust Architectures and Security Frameworks

Organizations such as the NIST, CISA, and MITRE have created frameworks for zero trust concepts and IT security best practices for both public and private sector entities. Many of these require or recommend active defense and deception capabilities like those provided by ShadowPlex. For example:

- **The National Defense Authorization Act** of fiscal year 2023 states: "Not later than 1 year after the date of the enactment of this Act, the Chief Information Officer of the Intelligence Community shall conduct a survey of each element of the intelligence community on the use by that element of proactive cybersecurity initiatives, continuous activity security testing, and active defense techniques."
- According to **NIST SP 800-207**, Zero Trust Architecture: "the focus [of zero trust] is on authentication, authorization, and shrinking implicit trust zones… The system must ensure that the subject is authentic and the request is valid."
- **NIST SP 800-172** includes the following enhanced security requirement: "Using deception to confuse and mislead adversaries regarding the information they use for decision-making, the value and authenticity of the information they attempt to exfiltrate, or the environment in which they are operating."
- The **CISA *2022-2026 Strategic Technology Roadmap***, Version 4 recommends the widespread adoption of deception technologies and says: "Deception tactics help determine the presence of adversaries on systems, hamper their ability to accomplish their goals, and help defenders identify attackers and their tactics."
- **MITRE ATT&CK®** is a framework that describes more than 240 adversary tactics and techniques in 14 categories; ShadowPlex provides capabilities that help address 10 of the 14 categories enumerated in this framework.

Acalvio's ShadowPlex Active Defense Platform has obtained **FedRAMP Ready** status.

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**