Acalvio Advanced Threat Defense and Identity Protection for Public Sector Organizations

How government agencies can use cyber deception to implement zero trust and NIST frameworks, protect credentials, and out-think adversaries

Public sector organizations are working hard to modernize their IT infrastructure, implement zero trust architectures, build cyber resiliency, enable mobile and remote work, and improve digital services to citizens. Unfortunately, security concerns related to threats from well-funded cybercriminals and state-supported hacking groups are slowing those initiatives and increasing costs. Conventional passive defense security technologies are susceptible to social engineering and zero-day attacks and produce far more alerts than security teams can investigate and address. That is why government agencies are moving toward a new approach to security that detects cyberattacks with precision, regardless of their source, confuses and diverts the attackers, and provides real-time intelligence on the tactics, techniques, and procedures (TTPs) of threat actors.

That new approach is active defense based on cyber deception. Active defense solutions populate an organization's computing environment with a wide range of decoys and deception elements that attract the attention of attackers, lead them away from real data and systems, and alert security teams to their every step. Several government standards organizations require or recommend active defense, including the 2023 National Defense Authorization Act, NIST SP 800-172, and the CISA 2022 – 2026 Strategic Technology Roadmap (see the text box on the last page).

Acalvio is the industry leader in delivering comprehensive, enterprise-scale, automated active defense technology. It offers two products based on its Active Defense Platform.

ShadowPlex Advanced Threat Defense (ATD) provides an innovative active defense security layer that complements existing controls. It deploys and manages a wide range of deception tools in on-premises and cloud workloads across a distributed enterprise network. It attracts, misleads, delays, and monitors adversaries who have gained a foothold in the organization's environment.

ShadowPlex Identity Protection is the first fully-featured active defense solution specifically designed to protect credentials by reducing the identity attack surface and detecting credential-based attacks early, before they cause harm. It detects the misuse of stolen credentials and enables organizations to implement zero trust architectures with confidence.

All Acalvio solutions use artificial intelligence (AI) based automation to scale and continuously adjust active defenses with minimal effort from security teams. They challenge adversaries with dynamic, realistic deceptions and improve the effectiveness of security operations centers (SOCs) by generating only high-quality alerts.

ShadowPlex Advanced Threat Defense

The power of Active Defense

ShadowPlex Advanced Threat Defense (ATD) detects zero-day attacks and other threats that bypass existing security controls. It populates an organization's computing environment with thousands of decoys and a variety of endpoint deception elements that steer adversaries away from valid information assets toward realistic facsimiles. When adversaries interact with these deception elements, Acalvio's patented technology:

- Immediately alerts security teams to nascent attacks
- Tracks the activities of threat actors as they move laterally across networks, attempt privilege escalation, request access to subnets and information assets, and perform malicious actions
- Documents the TTPs of each attack in detail

Unique benefits

Unlike most detection technologies, active defense generates high-quality alerts with almost no false positives. Deception elements are not part of legitimate business processes, so any interaction with them is suspect and almost certainly related to malicious activity.

ShadowPlex ATD misleads and frustrates adversaries, slowing down attacks and giving defenders time to contain them before they do harm. It also provides critical threat intelligence so security teams can remove the attackers from the network and take steps to thwart future attacks.

Acalvio: The leader in enterprise-scale active defense

ShadowPlex ATD:

- Offers a comprehensive and extensible deception palette that includes highly realistic decoys, breadcrumbs, baits, and other deception elements, tailored for different computing environments and attack types
- Deploys distributed deception at enterprise scale, across on-premises IT and OT networks and cloud workloads
- 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
- Integrates with SOAR, SIEM, EDR, cloud security, network management, software management, and other security and IT management tools to multiply the effectiveness of attack detection, incident response, security analytics, and other security functions

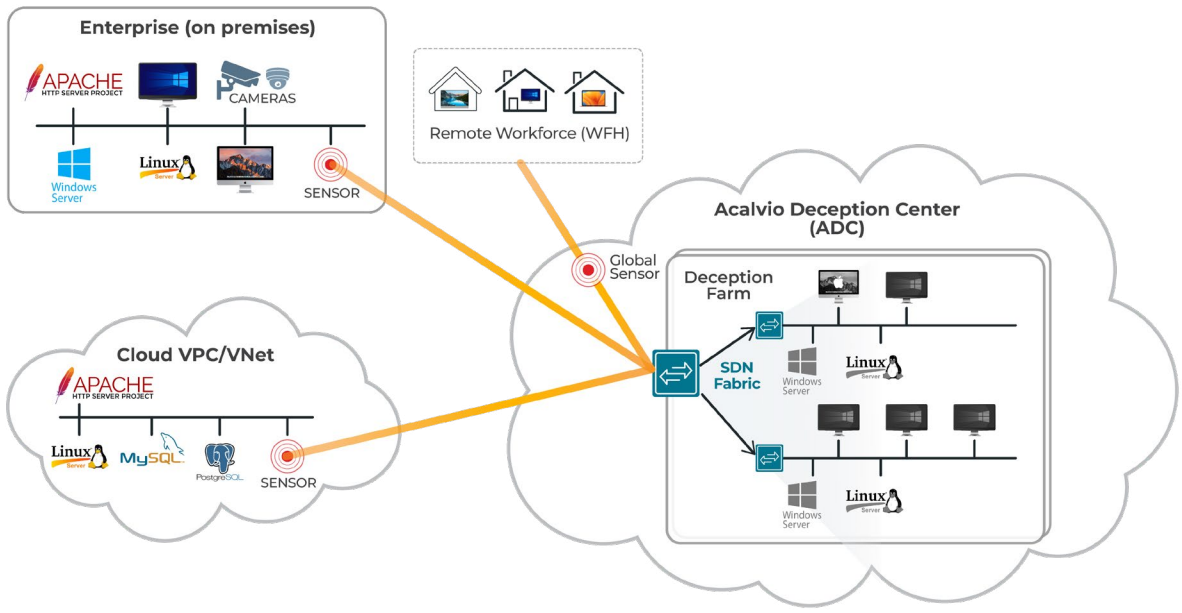

Figure 1: Acalvio ShadowPlex Architecture; ShadowPlex ATD populates an organization's computing environment with thousands of deception elements that steer adversaries away from valid information assets and alert security teams to their actions.

ShadowPlex Identity Protection

The attack surface of critical identity information and credentials is very large. In a typical government agency, it includes thousands of user accounts in identity repositories, application accounts on servers, and credentials cached on endpoints across the organization.

Excellent identity protection is a prerequisite for zero trust initiatives. Public sector organizations can have confidence in their zero trust security only if credentials are safe. Figure 2 illustrates that in a zero trust architecture, access policies are applied based on the requestor's identity. An adversary who captures credentials associated with a user will be granted access to all information assets available to that person.

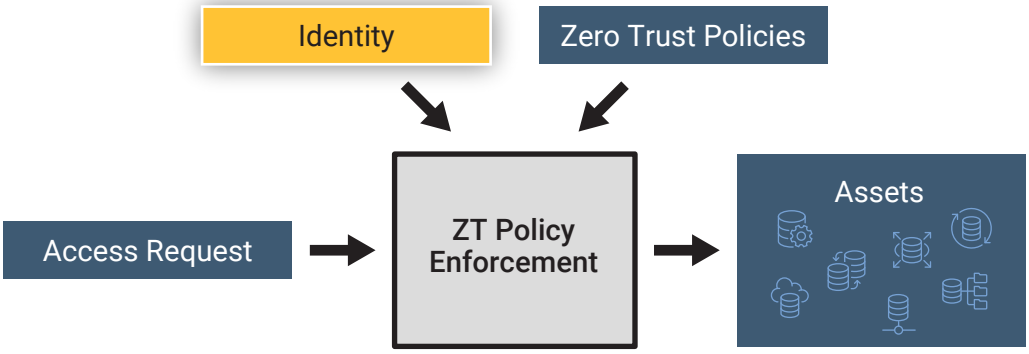

Figure 2: In a zero trust environment, policies are applied based on the requestor's identity; an adversary who captures credentials is granted access to all information assets available to that user.

Identity repositories

ShadowPlex Identity Protection employs advanced AI techniques and security domain knowledge to map the exploitable attack surface of identity repositories, including Microsoft Active Directory (AD) and Azure AD. It identifies potential security risks created by unprotected administrator accounts, shadow administrators, over-permissioned accounts, and other potential vulnerabilities. It also identifies misconfigurations and security weaknesses such as service accounts and vulnerable Service Principal Name (SPN) accounts.

Endpoint credential caches

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. It gives security teams options to delete vulnerable cached credentials or replace them with decoy credentials that can be used for deception.

Attack paths

A key feature of ShadowPlex Identity Protection is the ability to detect and map exploitable attack paths from endpoints and identities to the types of key assets targeted by adversaries, such as applications, databases, document repositories, and enterprise directories. Security and identity management teams can use this information to break the paths by removing credential caches, fixing misconfigurations, limiting permissions for privileged accounts, and tightening controls around key assets.

Active defense against credential-based attacks

ShadowPlex Identity Protection provides active defense against credential-based attacks. "Honey accounts" are decoy user accounts, tailored by AI to attract the attention of adversaries, planted in identity repositories like AD and Azure AD. "Honey tokens" are deceptive credentials and security tokens deployed in endpoint credential caches. Whenever adversaries attempt to access honey accounts or use honey tokens, security teams are alerted to their activities so they can respond immediately and contain the attacks before they succeed.

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 Advanced Threat Defense and ShadowPlex Identity Protection. 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 200 adversary tactics and techniques in 14 categories; ShadowPlex ATD provides capabilities that help address 10 of the 14 categories enumerated in this framework.

Acalvio's ShadowPlex Active Defense Platform was the first deception solution to attain **FedRAMP Ready** status. It includes the 325 controls required for FedRAMP medium certification.

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**