Acalvio ShadowPlex Advanced Threat Defense

Detect cyber threats early and with precision with active defense based on enterprise-scale deception technology and AI

Modern adversaries are evading traditional security

Adversaries have gained in sophistication and stealth, with threat actors leveraging living off the land techniques, AI fueled polymorphic malware variants, identity threats, insider threats, novel ransomware variants to bypass traditional security solutions. Adversary breakout time is falling rapidly, down to an average of 62 minutes in 2024 from an average of 84 minutes in 2023. Traditional security solutions are focused on detecting a set of known threats with known attack TTPs. These solutions are unable to keep pace with the advances in stealth and evasion of the modern adversaries. As a result, the number of breaches has reached an all-time high, with the number of zero days also hitting new records. Defenders need to expand the threat detection coverage to gain visibility to these stealthy and fast-moving threats.

Turn the Tables with Active Cyber Defense

Active cyber defense turns the tables on adversaries. It combines two powerful approaches to security:

- **Deception technology**, which populates an organization's computing environment with a wide range of deception elements that detect and mislead attackers.
- **Predictive analytics**, which anticipates attackers' actions and places carefully crafted deception elements directly in their path.

Active cyber defense enables defense teams to change the adversaries' landscape by deploying a set flow of strategically placed deception elements, tailored to the organization's industry and threat profile, in the places threat actors are most likely to target to achieve their goals and objectives. The deception elements are made enticing for adversaries to exploit, they detect the adversary actions while diverting the adversary away from the real data and systems and serve as an early warning system to security teams.

This predictive approach brings a proactive dimension to cyber defense, enabling security teams to detect cyber threats early and contain threats quickly. Active Cyber Defense and deception technology serve as a necessary layer for a defense in depth approach to cybersecurity, complementing existing solutions and expanding the coverage to detect threats that bypass traditional security solutions. Deception-based threat detection is agnostic to attacker TTPs, enabling defense teams to stay protected as adversaries continue to innovate and evolve new offensive techniques,.

Acalvio ShadowPlex Advanced Threat Defense

Acalvio delivers comprehensive, enterprise-scale, automated active cyber defense technology. ShadowPlex Advanced Threat Defense (ATD) is the leading cyber deception platform. It is built on Acalvio's industry-leading Active Defense platform, which leverages more than 25 patents on autonomous deception and AI.

ShadowPlex ATD populates an organization's computing environment with a wide range of deception elements that serve as traps for the adversary and protect identities, endpoints, network, applications, and data across IT, OT, and Cloud environments. The deceptions enable cyber defense teams to detect and document advanced attacker tactics and techniques for network reconnaissance, credential access, lateral movement, persistence, privilege escalation, defense evasion, data exfiltration, and other malicious actions.

ShadowPlex Advanced Threat Defense

A Rich Set of Realistic, Extensible Deceptions

ShadowPlex ATD offers an extensive palette of more than 350 pre-built deception elements aligned with specific attack types. Customer can also customize Acalvio's deceptions and create new ones.

The deception elements available with ShadowPlex ATD include:

Decoys – attractive, reachable targets added to the network, that lure attackers away from real data and applications, for example fake but realistic servers, endpoints, applications, databases, directories, cloud storage buckets, and OT networks.

Breadcrumbs – deceptive credential and connection profiles, added to existing legitimate assets, such as fabricated paths cached on servers, fictitious access credentials in user profiles and log files, and FTP, RDP, and SSH links.

Baits – objects that act as tripwires when accessed or moved, like counterfeit documents and files, honey accounts (deceptive user and service accounts), and honeytokens (credentials for honey accounts).

When adversaries interact with these deception elements, Acalvio's technology:

- Immediately alerts security teams to nascent attacks
- Collects detail forensics on compromised endpoints and documents the TTPs of each attack
- Performs automated response actions to isolate threats and protect the real assets
- Enables threat hunting actions through the deployment of additional deceptions to confirm threat hunting hypothesis

High-Quality Alerts and Rapid Containment

ShadowPlex ATD dramatically improves the ability of SOCs and incident response organizations to quickly find and contain dangerous threats.

Compared to conventional detection tools, active cyber defense solutions generate higher-quality alerts with far fewer false positives. Deception elements are not part of legitimate business processes, so any interaction strongly indicates malicious activity.

ShadowPlex ATD provides even more precision through auto triage. It leverages multiple data sources, AI, and advanced analytics to pinpoint deception events associated with the most serious threats to the organization.

ShadowPlex ATD also helps security teams contain attacks quickly. It can:

- Automatically quarantine affected systems
- Provide incident responders with answers to critical questions such as "what endpoint and user session triggered the alert," "what are the attacker TTPs" and "Has the attacker gained persistence on the endpoint?"

Threat Intelligence and Threat Hunting

ShadowPlex ATD also helps security teams reduce risk over the long term. It uncovers attacker TTPs so security teams can identify the most effective countermeasures. It also provides analytic tools to help prioritize remediation actions.

ShadowPlex ATD provides a dedicated threat hunting workbench. This provides an ability to deploy purpose-built deceptive elements to identify latent threats and confirm threat hunting hypothesis.

AI-Driven Automation That Boosts Effectiveness and Reduces Administrative Effort

ShadowPlex ATD uses AI-driven automation to design, customize, deploy, and manage thousands of deception elements without burdening security teams.

Attackers are smart. They aren't fooled by decoys that are simplistic, static, or out of place. To attract and mislead them, deception elements must be strategically placed, realistic, appropriate for the organization's industry and computing environment, and updated frequently. But security groups don't have nearly enough staff to perform these tasks manually.

ShadowPlex ATD addresses this challenge by:

- Providing a comprehensive deception palette with more than 350 unique decoys, breadcrumbs, and baits built on real network and application stacks
- Using AI and automation to configure and personalize deception elements for every individual subnet and asset
- Offering customizable deception playbooks that autonomously deploy, manage, and refresh decoys, breadcrumbs, and baits

Key Use Cases Include:

- **Early threat detection**, detect threats early in attack lifecycle to prevent adversary breakout
- **Deception-based identity threat detection and response (ITDR),** detect threats targeting identity architecture
- **Insider threat detection** detect accidental and privileged insiders with precision
- **Ransomware defense**, detect known and unknown ransomware variants with precision and speed
- **Advancing Zero Trust maturity,** improved cyber visibility for visibility and analytics in Zero Trust architecture
- **OT/ICS security** (operational technology and industrial control system)**,** detect threats targeting OT assets without production impact
- **Threat Hunting,** identify latent threats and confirm threat hunting hypothesis

Scalability, Control, and Fast Deployment

Acalvio's technology provides comprehensive active cyber defense across large-scale, diverse enterprise environments. It supports:

- On-premises and cloud workloads
- A wide range of operating systems, networks, and device types
- Operational technology (OT) as well as IT environments

No endpoint agents are required.

ShadowPlex ATD has been deployed in environments with over 100,000 endpoints and many subnets in multiple locations.

As shown in Figure 1, all ShadowPlex ATD decoys are hosted in the Acalvio Deception Center (ADC) in the cloud. This simplifies management. In addition, although adversaries "see" the assets on the network they are attacking, all interaction takes place in a contained environment isolated from actual data and business processes.

To speed up deployment and deliver value immediately, ShadowPlex ATD provides deception playbooks that encapsulate domain knowledge of how to deploy deception elements tailored for specific threats. Cyber defense teams can employ the playbooks to gain immediate coverage of their most relevant use cases. And thanks to the AI-driven automation in ShadowPlex ATD, you can deploy thousands of deceptions in minutes.

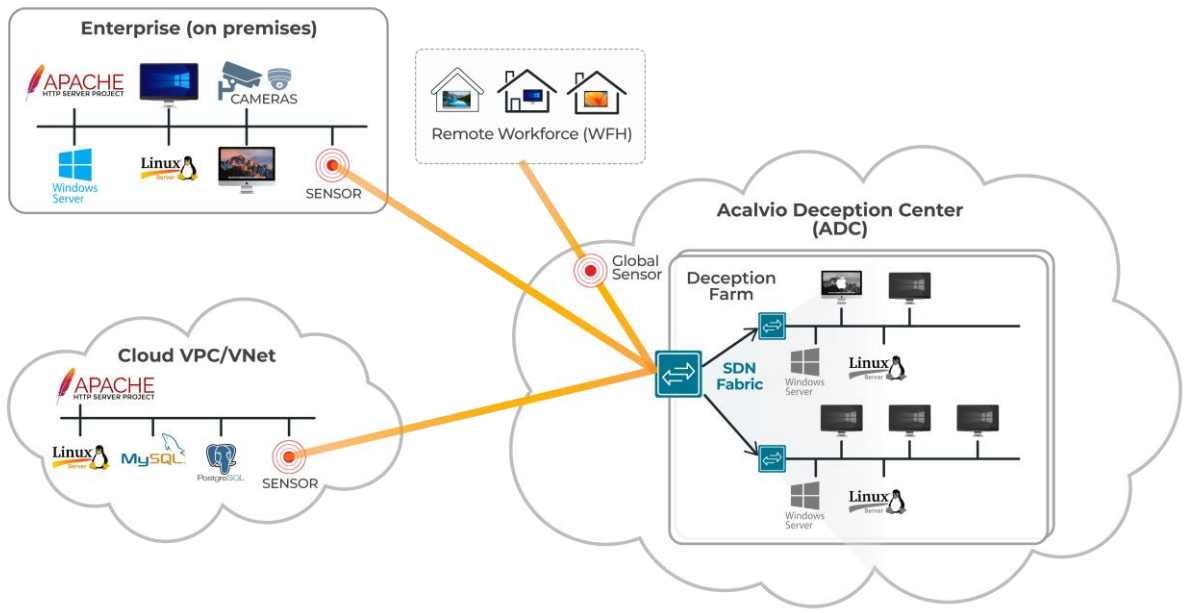

Figure 1: Acalvio ShadowPlex Architecture; ShadowPlex ATD populates an organization's computing environment with strategically placed deception elements that detect adversaries early in the attack lifecycle and alert security teams to their actions.

Integrations to Support Discovery, Response, and Remediation

ShadowPlex ATD complements and strengthens an organization's existing security infrastructure. It integrates with SOAR, SIEM, EDR, firewall, cloud security, network management, software management, and other security and IT management tools. It enhances the effectiveness of security workflows for detection, incident response, and remediation, and provides critical data for forensics, attack surface reduction, and security analytics.

Active Cyber Defense and Cyber Deception as a Necessary Defense strategy

An increasing number of standards bodies are recommending or requiring active defense and deception capabilities like those provided by ShadowPlex ATD. For example:

- **Gartner Reference Architecture for endpoint security and network security:** The Gartner reference architecture for network security and for endpoint security published in 2024 highlights the role of deception for early threat detection to protect endpoints and network.
- **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."
- **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 MITRE ATT&CK® framework** describes more than 240 adversary tactics and techniques in 14 categories; ShadowPlex ATD capabilities help address 10 of those 14 categories.

Create Diminishing Returns for Adversaries

Active cyber defense gives you an opportunity to detect adversaries early and isolate them to protect your organization. With ShadowPlex ATD, attackers have a dilemma of having to ensure that each step in the attack lifecycle does not land up tripping a deception, resulting in slowdown and confusion for the adversary. Threat actors will be even more discouraged If they suspect that you are using active cyber defense, knowing that they are facing hundreds of potential points of failure and that the best-looking targets are the ones most likely to be deceptions.

Don't let adversaries keep the upper hand. Learn how you can turn the tables.

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), Insider Threat Detection, OT Security, Zero Trust, 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**