Acalvio ShadowPlex Advanced Threat Defense

Turn the tables on adversaries with active cyber defense and enterprise-scale deception

Why Adversaries Have the Advantage Over Defenders

In cybersecurity today, sometimes it feels like adversaries have nearly insurmountable advantages over defenders. To breach an organization's perimeter defenses, threat actors can target hundreds of potentially vulnerable servers and devices, plant malware or ransomware on any one of thousands of endpoints, or acquire credentials from any number of careless employees and supply chain partners. Once inside, they can move laterally and access data in ways with little chance of being detected, especially if they have collected valid credentials. Most discouraging of all, adversaries only need to find one weakness to succeed, while security teams must defend a multitude of potential points of failure.

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 decoys and deception elements that attract 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 constant flow of new deception elements, tailored to the organization's industry and threat profile, in the places threat actors are most likely to touch. The deception elements draw the attention of attackers, lead them away from real data and systems, and alert security teams to their every move.

This predictive approach brings a proactive dimension to cyber defense, enabling security teams to detect cyber threats early and contain threats quickly. With active cyber defense, it is not defenders, but adversaries who face hundreds of potential points of failure.

Acalvio ShadowPlex Advanced Threat Defense

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

ShadowPlex ATD populates an organization's computing environment with a wide range of endpoint deception elements that steer adversaries away from valid information assets toward realistic facsimiles. They also enable cyber defense teams to detect and document advanced attacker tactics and techniques for network reconnaissance, persistence, lateral movement, privilege escalation, defense evasion, data exfiltration, and other malicious actions.

A Rich Set of Realistic, Extensible Deceptions

ShadowPlex ATD offers an extensive palette of more than 250 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, VM hosts, applications, databases, directories, cloud storage buckets, and OT networks.

Breadcrumbs – pointers to decoys, 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 honey tokens (user credentials for non-existent privileged users).

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

- Immediately alerts security teams to nascent attacks
- When attacks are under way, uses predictive analytics to deploy new deception elements in the paths attackers are likely to follow
- 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

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
- At the first sign of malicious activity, create new customized deception elements to divert attackers away from real assets
- Provide incident responders with answers to critical questions such as "what endpoint user session and process(es) triggered the alert," "what assets did the endpoint communicate with," and "what other endpoints have seen similar actions?"

Predictive Analytics and Threat Intelligence

ShadowPlex ATD uses predictive analytics to anticipate the next moves adversaries will make and place additional deception elements in their path. It also helps incident response teams isolate threats and protect high-value assets before attackers can find them.

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.

AI-Driven Automation That Boosts Effectiveness and Reduces Work

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 numerous, realistic, appropriate for the organization's industry and computing environment, and replaced 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 250 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:

- **Detecting zero day threats**, APTs, polymorphic and fileless malware, and other advanced threats that elude conventional detection and protection tools
- **Protecting endpoints**, including user workstations and servers
- **Protecting networks** from network-centric threats
- **Protecting key assets**, including critical databases and applications
- **Defending against ransomware**
- **Protecting OT/ICS** (operational technology and industrial control system) **environments**
- **Protecting cloud workloads** in hybrid and pure-play cloud environments

Scalability, Control, and Fast Deployment

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

- On-premises, cloud, and remote 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.

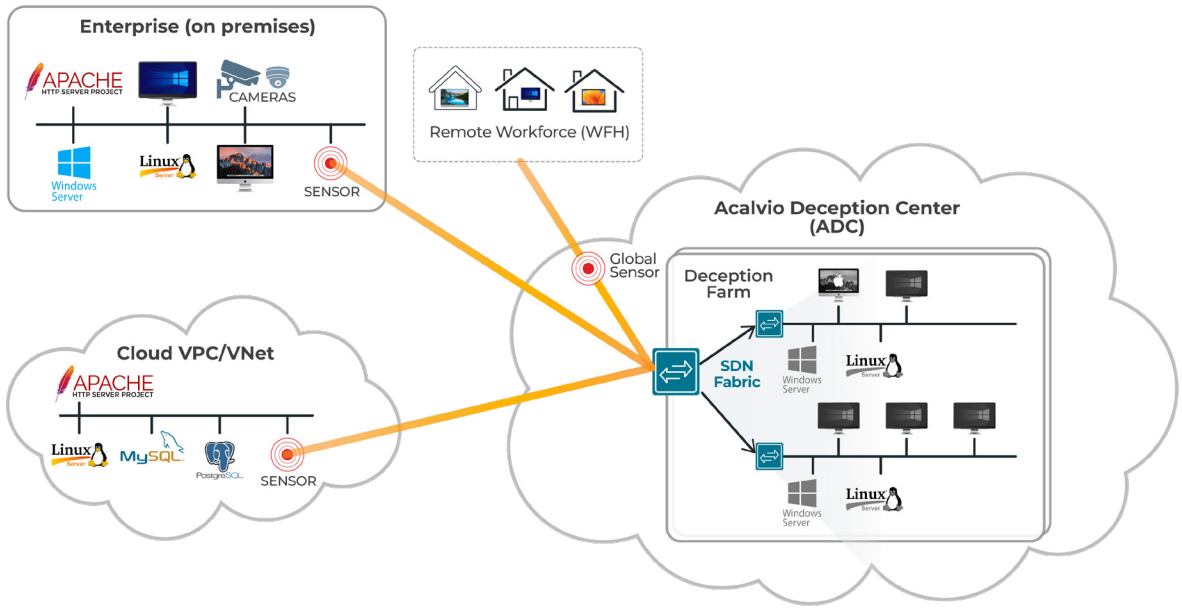

Figure 1: Acalvio ShadowPlex Architecture; ShadowPlex ATD populates an organization's computing environment with thousands of deception elements that steer adversaries away from valid information assets and alert security teams to their actions.

Integrations to Support Response, Remediation, and Threat Hunting

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. It can also help threat hunters define and test hypotheses, for example by placing deception artifacts in areas suspected of being targeted by adversaries.

Active Cyber Defense as a Best Practice

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

- **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 200 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 frustrate adversaries until they turn away from your organization. With ShadowPlex ATD, attackers won't notice anything different about your computing environment – except that it takes longer for them to make progress and they come away in the end with little or nothing of value. 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), 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**