ACALVIO
AI-POWERED DECEPTION

DATASHEET

Turn the Tables on Agentic Adversaries: Deception-based Advanced Threat Defense

ASSUME COMPROMISE SECURITY POSTURE

The rapid expansion of attack surface and the expanded set of attack pathways has resulted in security teams adopting an assume compromise security posture.

The operating principle is an adversary, whether a human threat actor, misaligned AI agent, or malware/ransomware, will gain initial access to an organization. After infiltrating the vulnerable perimeter, they proceed to target the enterprise's internal network, privileged identities, critical applications, data, and other key assets, causing extensive harm. Agentic AI attacks operate at machine-speed, moving from reconnaissance to data exfiltration within minutes.

Traditional detection and response solutions are unable to keep pace with fast moving agentic exploits.

TURN THE TABLES ON THE ADVERSARY

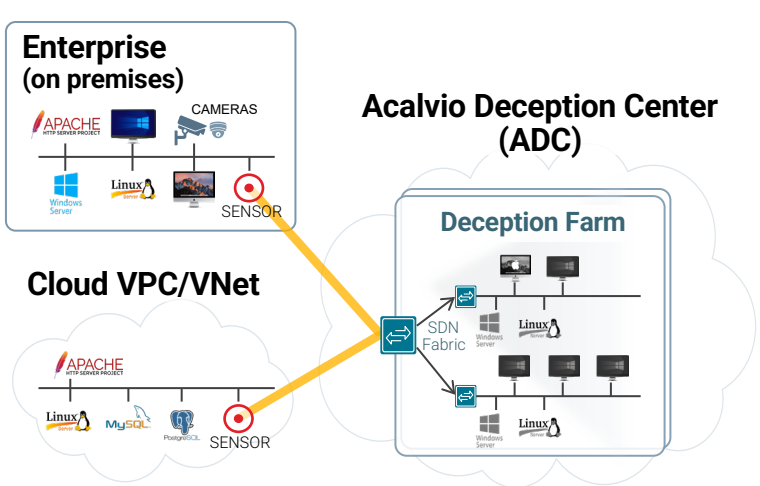
Security teams need a paradigm shift, one that anticipates threats and applies principles of early detection, adversary diversion and disruption.. Deception technology offers a distinctive and robust approach to countering cyber threats, empowering defense teams to effectively identify both known and new threats, including agentic AI attacks, zero-Day threats. Deception is the only defense approach that can change the attacker's perspective and brings a preemptive approach to cyber defense.

Deception-driven threat defense extends its safeguarding reach to applications, data repositories, cloud workloads, operational technology (OT) environments, as well as endpoints and networks. This holistic defense mechanism underscores the necessity of integrating deception technology as a foundational cornerstone within the cybersecurity strategy implemented by enterprises.

KEY BENEFITS

- Detect agentic AI attacks at the reconnaissance phase and stop propagation
- Divert and deflect agentic AI attacks
- Detect living off the land attacks with precision
- High-fidelity threat detection provides actionable intelligence for SOC and IR
- Ability to detect threats against resources where agents cannot be installed e.g. Printers, Routers / Switches, IoT Cameras, Legacy systems etc.
- Threat hunting for hypothesis testing and confirmation

DECEPTION-DRIVEN THREAT DEFENSE



Turn the Tables on Adversaries: Deception-based Advanced Threat Defense

ACALVIO
AI-POWERED DECEPTION

ACALVIO'S ADVANCED THREAT DEFENSE

The modern organization has a digital perimeter that can encompass the IT, OT/ICS, IIoT, and Cloud segments of the network. IT environments have important Applications and Data repositories; these are the target of attackers looking for sensitive data or intellectual property. The OT/ICS segment must be defended against threats that can target devices at any layer of the Purdue Model. This segment is often isolated from the rest of the network by airgaps or DMZs, which complicates monitoring and management. The devices used in the OT/ICS segment are often legacy or proprietary systems, so they cannot be protected using agent-based defenses. Along similar lines, an organization whose network extends to the Cloud has to defend their cloud workloads and associated identities, including storage buckets and IAM profiles. In summary, organizations must protect their key assets as those are the targets that the attackers go after.

Acalvio's Advanced Threat Defense is built on patented Deception Technology and AI. The solution offers a wide palette of deceptions that is specifically designed to protect each segment of an organization's network. The solution is independent of the tactics, techniques, and procedures used by attackers. It extends this protection without creating a big footprint in the network segments where it is deployed. It is also designed to carry out automated response actions, such as employing dynamic deceptions to divert and slow down the attacker, collecting forensic data from endpoints, and quarantining endpoints.

INTEGRATION WITH SECURITY ECOSYSTEM

ShadowPlex integrates with a wide range of solutions such as SOAR, SIEM, EDR, AD, Network Management Solutions, Email Servers, Software Management Solutions (such as SCCM, Chef, Puppet, and other platform-specific tools) among other solutions. ShadowPlex leverages integrations with these defense systems for network discovery, gathering forensic data from endpoints, breadcrumb and bait deployment on network endpoints and assets, as well as for automated response.

USE CASES

- Divert and deflect Agentic AI attacks
- Early threat detection
- Key Asset Protection
- Network Protection
- Endpoint Protection
- Protect OT/ICS networks
- Protect unmanaged resources
- Insider Threat Detection
- Protect Applications
- Protect Data
- Protect cloud workloads

Gartner® recognized Acalvio as the "Company to beat" in Preemptive Cyber Deception.

"After deploying ShadowPlex, we could see immediate benefits in the decoy and deception technology Acalvio brings to the table. Not only was the product extremely easy to deploy, we immediately recognized the value and began expanding our Shadowplex coverage which helped us detect lateral movement of any threats."

— Sean Oldham, CISO, Broadcom

Acalvio is an AI-powered preemptive cybersecurity company focused on countering AI-driven identity and infrastructure intrusion. Its 360 Deception platform combines Dynamic Deception, evolving HoneyPaths, and cloaking of production assets within deception fabric to disrupt automated reconnaissance, credential abuse, and lateral movement across identity systems, endpoints, cloud, network, and cyber-physical environments. By altering what attackers can perceive and trust, Acalvio shifts detection from post-compromise analysis to pre-impact exposure, enabling organizations to detect, delay, disrupt, and deny malicious activity at machine speed. The company serves enterprise and government organizations determined to break automated intrusion at its source. https://www.acalvio.com/