ACALVIO
CYBER DECEPTION LEADER

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

CYBER ATTACKS ARE PERSISTENT

Despite the use of various defense mechanisms, cyber attackers continue to achieve success in today's digital landscape, revealing a persistent and evolving challenge. Malicious actors exploit vulnerabilities, craft sophisticated attack campaigns, and quickly adapt to defense strategies, underscoring the complexity of the cybersecurity landscape. There is an enduring struggle between defenders and attackers - highlighting the adversaries' ability to breach even well-fortified digital perimeter. 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.

Defenders need an innovative solution that can detect advanced and sophisticated threats early and with high fidelity.

TURN THE TABLES ON THE ADVERSARY

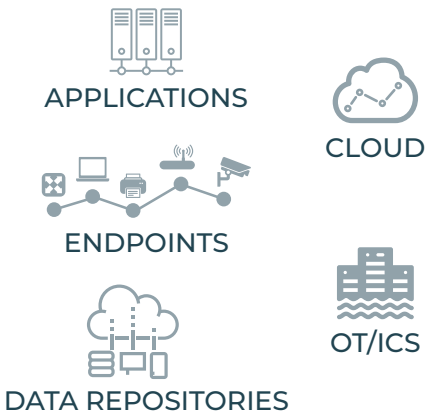
Enterprises today require an additional layer of defense as an integral component of their comprehensive cybersecurity strategy. Deception technology offers a distinctive and robust approach to countering cyber threats, empowering defense teams to effectively identify both known and new threats, including Zero-Day attacks. Deception is the only defense approach that can change the attacker's perspective and brings a proactive approach to cyber defense. Deception removes the blind spots left by conventional defense mechanisms.

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:

- Deception-based Detection complements CrowdStrike
- Detects known and unknown (zero-day) threats
- 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
- Ability to introduce new deceptive targets to attract latent threats
- Active – not just observe but engage, divert and delay attacks
- Integrated into CrowdStrike platform

DECEPTION-DRIVEN THREAT DEFENSE



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

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.

CROWDSTRIKE

PRE-INTEGRATED WITH CROWDSTRIKE FALCON

Acalvio's Advanced Threat Defense is an agentless solution and is integrated with the CrowdStrike Falcon® platform out of the box. Acalvio is a completely automated solution, which makes it very easy to deploy and manage.

The Acalvio integration with CrowdStrike provides significant benefits for enterprises. The integration enables Acalvio to blend the deceptions based on the discovery data from CrowdStrike Falcon, provides automated endpoint deception deployment and enables automated response actions.

USE CASES

- Network Protection (detect Lateral Movement and attacker propagation)
- Protect OT/ICS networks
- Protect unmanaged resources
- Protect Applications
- Insider Threat Detection
- Protect Data
- Protect cloud workloads
- Deception-based Ransomware protection
- Key Asset Protection

"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, the leader in cyber deception technology, helps enterprises actively defend against advanced security threats. The Acalvio Active Defence Platform, built on 25+ issued patents in autonomous deception and advanced AI, provides robust solutions for Identity Threat Detection and Response (ITDR), Advanced Threat Defense for IT and OT networks, 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 from the Cloud, on-premises or via marquee managed service providers.

WWW.ACALVIO.COM INFO@ACALVIO.COM @ACALVIOTECH ACALVIO-TECHNOLOGIES