

Acalvio ShadowPlex and Cisco® pxGrid/ISE:

ADVANCED THREAT DETECTION & RAPID CONTAINMENT

Acalvio ShadowPlex Autonomous Deception solution is now integrated with Cisco Identity Services Engine (ISE) using Platform Exchange Grid (pxGrid). This seamless integration into the Cisco ecosystem enables ShadowPlex to automatically quarantine any compromised enterprise hosts based on the deception alerts and user-configurable threat severity levels.

Acalvio ShadowPlex Autonomous Deception solution provides early detection of advanced threats with precision and speed. ShadowPlex is built on Acalvio's patented Deception 2.0 technology. Based on unique DeceptionFarms® architecture, ShadowPlex delivers distributed deception at enterprise scale, across on-premises and Cloud workloads. Advanced Threats have evolved to living-of-the-land, file-less, malware-less, becoming stealthier, persistent and making them very hard to detect. ShadowPlex combines breakthrough Deception Technology with Advanced Analytics, to detect, confirm, and investigate such advanced threats. A comprehensive deception palette, with customizable and extensible deception types, provides effective and authentic deception.

FEATURES:

- Leading edge Deception Solution based on **25 Issued Patents**
- Effectiveness – **high-fidelity detection**
- **Enterprise-Scale** – ability to scale to unlimited number of decoys
- **Easy deployment and management** – complete automation using integrated AI in every step
- Advanced **TTP Analysis**
- **Full life cycle:**
Detect -> Investigate -> Contain
- **Flexible deployment**
On cloud and on-premise

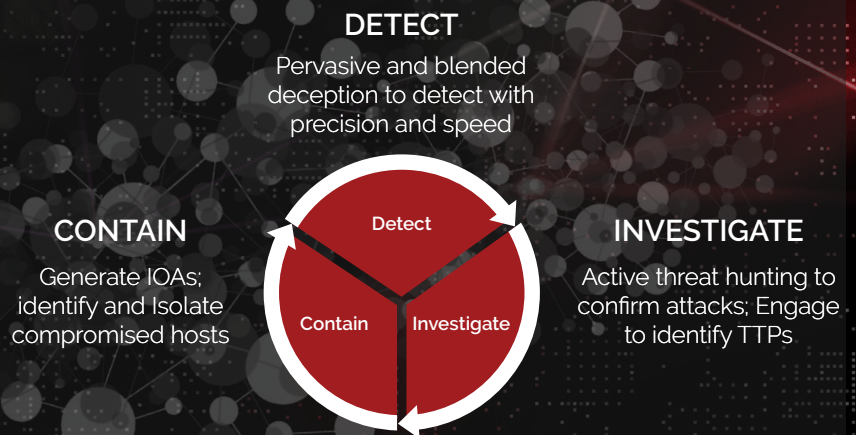
KEY BENEFIT

With ShadowPlex you can prioritize incidents, scrutinize through a multitude of suspicious activities and focus on convictions; then leverage Cisco ISE integration to invoke Rapid Threat Containment actions automatically with assurance.

COMPLETE DECEPTION PALETTE



DECEPTION TO SUPPORT 1/10/60 RULE



INVESTIGATE AND CONTAIN THREATS USING DECEPTION

USE CASE 1:

WEB APPLICATION BREACHES



PROBLEM:

Web Applications are the biggest source of breaches. Attacker typically breaches a web server, locates databases and file servers and credentials to log into them through various means – dumping credentials from memory/files, monitoring network connections, etc.

ShadowPlex SOLUTION:

Can project many authentic-looking database and file share decoys accessible from web servers.

Quickly deploy decoys: databases, file share credentials, S3 buckets, EC2 instances, and breadcrumbs on the web servers.

Automatically deploy and manage dynamic deception. This is especially relevant in a cloud deployment where systems come and go.



Check us out at
Cisco Marketplace SPP

USE CASE 2:

HUMAN THREAT ACTORS



PROBLEM:

Human Threat Actors constantly try to breach perimeter defenses by leveraging social engineering and phishing techniques. Once successful, they steal credentials and use them to pivot through networks searching for sensitive or confidential data. Traditional signature-based systems can detect only known malicious activity and anomaly detection methods require going through vast amounts of data and result in false positives.

ShadowPlex SOLUTION:

Automatically deploys and manages well-blended decoys relevant to each network neighborhood. Places baits and a variety of breadcrumbs in memory, registry and file system on the enterprise hosts to direct attacks to decoys.

Any access to the baits and decoys is recorded and can catch even zero-day exploits and unknown threats.

BENEFITS

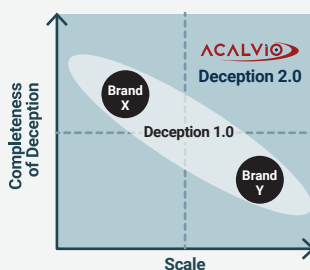
Detect unknown threats, lateral movement and zero-day exploits executed deep within your network by human threat actors and insiders.

Drastically reduce dwell times for unknown and zero-day attacks.

Offer non-repudiation measures and attribution against insider threat actors.

The ShadowPlex and Cisco pxGrid/ISE integration enables joint customers to speed detection with high fidelity and precision and automatically contain the threat, while diverting the attacker to the deception farm and away from real assets.

ADVANTAGE ACALVIO



COVETED AWARDS



ABOUT ACALVIO

Acalvio provides Advanced Threat Defense solutions to detect, engage and respond to malicious activity inside the perimeter. Acalvio's Autonomous Deception Platform, ShadowPlex is anchored on patented innovations in Dynamic Deception, Software Defined Networking and Data Science. ShadowPlex enables a DevOps approach to deploying enterprise-scale pervasive deception with low IT administrative overhead. ShadowPlex delivers comprehensive threat intelligence by integrating with other 'best in class' solutions in the security industry, enabling customers to benefit from defense in depth; lower false positives; and derive actionable intelligence for remediation.



WWW.ACALVIO.COM



INFO@ACALVIO.COM



@ACALVIOTECH



ACALVIO-TECHNOLOGIES