ACALVIO

SHADOWPLEX™
SOLUTION BRIEF

Autonomous Deception

WITH NOVEL CAPABILITIES ENABLED BY CROWDSTRIKE FALCON INTEGRATION

ADVANCED THREAT DETECTION:

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 from Cloud at enterprise scale, across on-premises and Cloud workloads. A comprehensive deception palette, with customizable and extensible deception types, provides effective and authentic deception.

Acalvio ShadowPlex generates a new stream of low volume, but high-fidelity signals based on dynamic deception, to add to the Detect capability of CrowdStrike's next-gen EDR.

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 -> Engage -> Respond
- **Flexible deployment** On cloud and on-premise

"ShadowPlex represents a very significant architectural advancement in the deception marketplace. Variable interaction deceptions, combined with its cloud deployment options, makes for greater efficacy and cost effectiveness, and makes ShadowPlex a best-in-class distributed deception platform."

—**Golan Ben Oni**
CIO, IDT Telecom

DECEPTION TO SUPPORT 1/10/60 RULE

DETECT
Pervasive and blended deception to detect with precision and speed

CONTAIN
Generate IOAs; identify and Isolate compromised hosts.

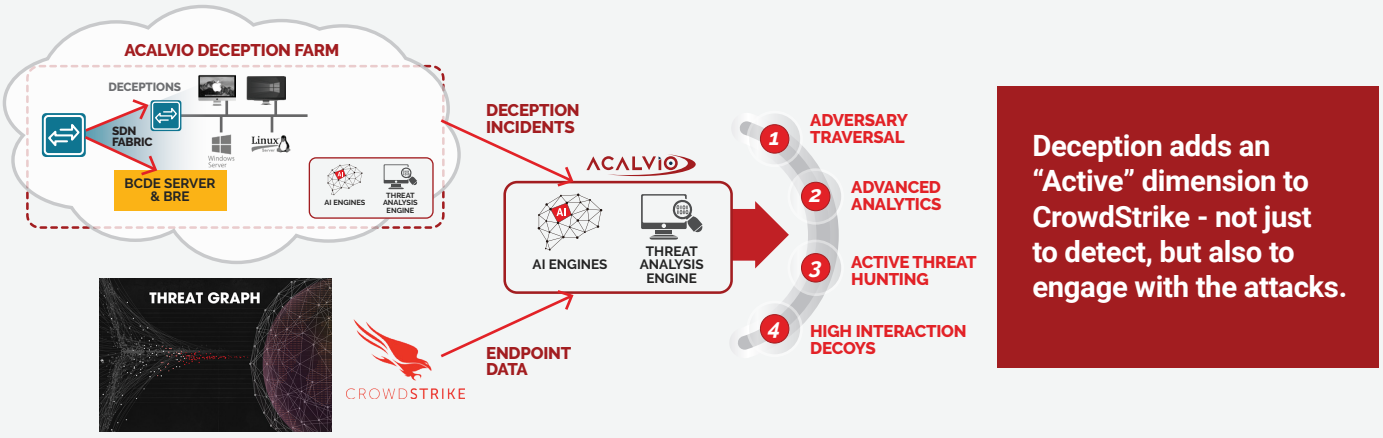
INVESTIGATE
Active threat hunting to confirm attacks; Engage to identify TTPs

COMPLETE DECEPTION PALETTE

ACALVIO

SHADOWPLEX™
AUTONOMOUS DECEPTION PLATFORM

INVESTIGATE AND CONTAIN THREATS USING DECEPTION



Deception adds an "Active" dimension to CrowdStrike - not just to detect, but also to engage with the attacks.

ShadowPlex provides a variety of capabilities for Rapid Incident Investigation.

Adversary Traversal — data from Threat Graph is used to automatically build the path of hosts adversary compromised before touching a decoy.

Analytic Tools — for analyzing memory snapshots and Powershell files, and includes integration with Falcon Sandbox.

Hypothesis Testing — deception-based Active Threat Hunting to expose advanced APTs and dormant malware.

High-Interaction Decoys — to engage with attacker and gather full TTPs.

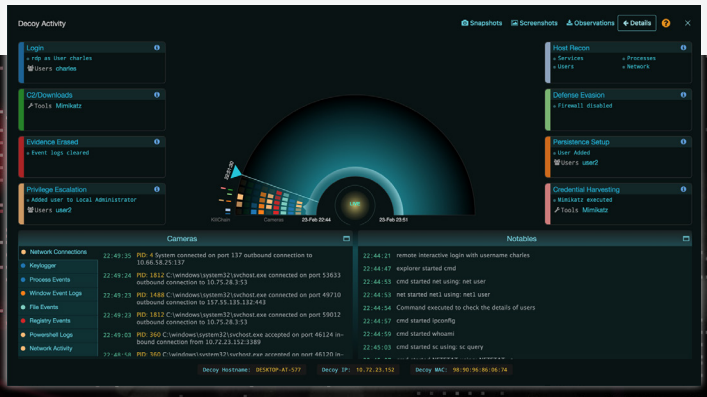
Deception Incidents are high-fidelity and enable Automated Response.

ShadowPlex can automatically isolate the compromised endpoint through integration with CrowdStrike Falcon agent.

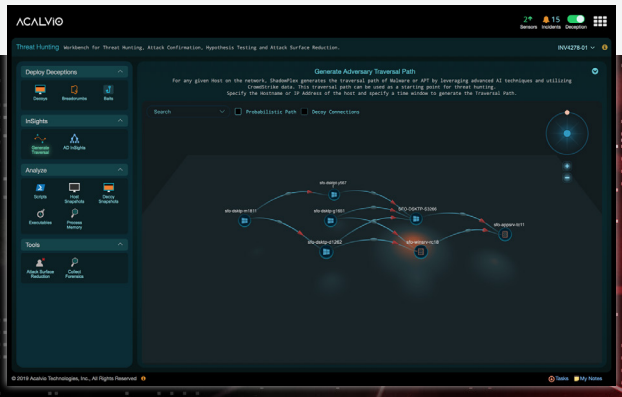
ShadowPlex has prebuilt integrations with SOAR, SIEM, email and Network Management products to alert and contain the attack.

Generation of IOAs – based on the attacker activity in the high-interaction decoys and compromised hosts.

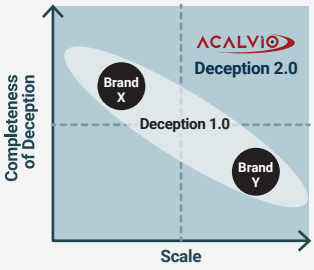
RICH FORENSICS FROM HIGH-INTERACTION DECOYS



ADVERSARY TRAJECTORY ANALYSIS



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