SOLUTION BRIEF

Fidelis Deception™

Change the Relationship with Your Adversary

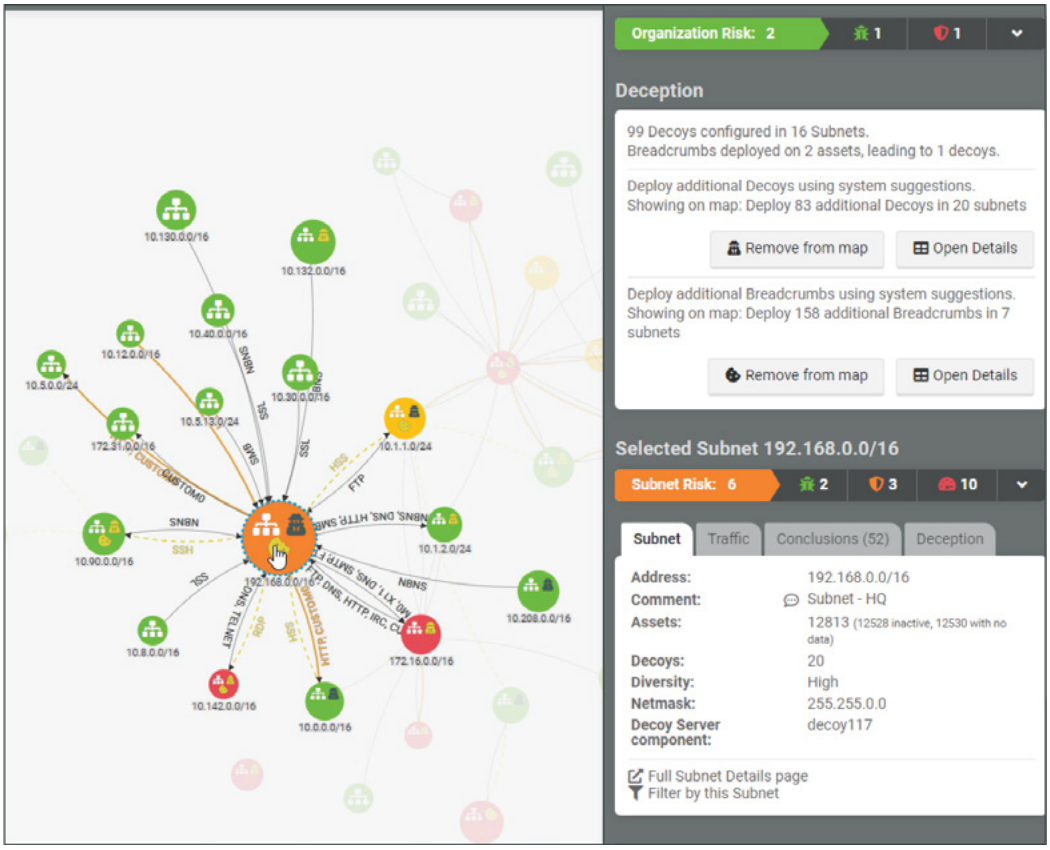
In defending your enterprise against attackers, you have one advantage—you know your cyber terrain better than they do. Deception-based security is a proactive detection technology that allows you to use that knowledge to turn the tables on attackers and expose data breaches quickly and accurately with minimal extra effort. Fidelis Deception® helps reduce cyber dwell time by altering the perception of the attack surface, which hinders an adversary's ability to move laterally undetected. Taking this Active Defense approach makes it harder for adversaries to accomplish their mission and increases the attacker's risk, giving you more time to understand TTPs, thwart the attack, and prevent future intrusions.

Use Deception to...

- Detect Lateral Movement
- Uncover attackers compromising Active Directory
- Discover attackers sniffing traffic (Man-in-the-Middle)
- Expose use of Stolen Credentials
- Find signs of Ransomware, even in encrypted files
- Identify infected IOT devices
- Gather TTPs (Sinkhole, RealOS Decoys)

Fidelis Deception

Fidelis Deception provides full situational awareness, with adaptive terrain analysis, intelligent deception technology, and security visibility so you can change the rules of engagement by re-shaping the attack surface. With authentic, interactive decoys and breadcrumbs on real assets and in Active Directory, you lure cyber attackers, malicious insiders, and malware to the deception layer and catch them before they damage enterprise operations or exfiltrate data.



How Deception Works

Deception publicizes decoys with breadcrumbs on real assets, luring attackers, malicious insiders, and automated malware away from valuable assets and traps them inside the deception layer. Instead of fruitlessly searching for bad actors within dynamically changing environments, you get high-fidelity alerts from decoys, AD credentials, poisoned data, and suspicious traffic that lead you directly to the attacker. While adversaries pursue lures, you can hunt, detect, and defend faster and with greater confidence.

Terrain Analysis

Provides accurate and continuous terrain mapping and analysis across the IT landscape to spot the unexpected faster.

- Profile and classify assets across on-premises and cloud environments to gain complete visibility.
- Remove blind spots for unknown assets, including legacy systems and shadow IT.
- Leverage intelligent risk assessments based on protection, activity, importance and more to protect valuable assets

Intelligent Deception

Automatically create and deploy authentic deception layers that attract sophisticated adversaries.

- Create authentic decoys for:
  - Hardware — laptops, servers, routers, switches, cameras, printers, enterprise IoT devices, etc.
  - Software — OS, apps, ports, services, applications, cloud assets, and similar data
  - Active Directory
- Automatically generate traps, breadcrumbs, and poisoned data to change the attack surface.
- Consume attacker time with high and medium interaction decoys that distract from real assets.
- Learn TTPs and improve asset defense with real-time threat intelligence analysis.

High-Fidelity Alerts

Improve alerting accuracy with decoys that are unknown, obfuscated assets not used by employees.

- Investigate alerts knowing network paths and asset profiles, communications, and decoy interaction for faster time-to-response.
- Eliminate the false positives that lead to alert fatigue.

Security Visibility

Stop attackers after the breach, but before they reach your valuable assets.

- Lure attackers with breadcrumbs on real assets to decoys to divert and defend.
- Detect lateral movement, attackers' reconnaissance and activities as they look for valuable data they can steal.
- Improve security posture by learning details of attack paths, resource interests, and initial compromised foothold systems.
- Enable Red Team and Blue Team risk simulations to determine enhanced decoy and breadcrumb placement.
- Seamlessly connect with Fidelis Endpoint and Fidelis Network for broader traffic analysis and DLP.

Fidelis Deception: The First Step in an Active Defense

Elevate your defenses and change the game. Fidelis Deception makes it difficult and costly for adversaries to succeed while improving SOC team efficiency and effectiveness.

While Deception can be used on its own, unifying it in the Fidelis Elevate platform delivers contextual visibility and rich cyber terrain mapping across the full IT landscape. These insights enable security teams to continually tune defenses and neutralize threats before they can damage business operations, and they form a foundation of intelligence to keep you ahead of the next attack. Find, stop, and remediate attacks with deception technology used by the DoD, US Intel communities, managed security providers, and Fortune 100 companies.

Key Benefits

Lure Attackers Away from Assets

Lure and distract adversaries with an authentic deception layer, including decoys, breadcrumbs, and traps that prevent attackers from discovering key assets.

Optimize Security Team Efforts

Automatically deploy deception with little to no configuration or administration and allow anyone on the SOC team, regardless of level or experience, to track deception alerts.

End Alert Fatigue

Rely on high-fidelity alerts from the distributed deception layers that let you detect post-breach attacks earlier while eliminating noise and false alarms.

Accelerate the Threat Response

Operate inside the adversary's decision cycle, keep them guessing, and dramatically reduce time-to-resolution from weeks and months to hours and minutes.

Prevent Post-Breach Damage

Recover faster and prevent costly damage from ransomware, malware, and insider threats.

Gather and Grow Threat Intelligence

Leverage decoy activity that is actively analyzed by sandbox and understand where each activity originated to improve your active defense strategy.

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity

Fidelis Cybersecurity combats the full spectrum of cyber-crime, data theft and espionage. A leading provider of threat detection, hunting and response solutions, Fidelis provides full visibility across hybrid environments, automates threat and data theft detection, empowers threat hunting, and optimizes incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense.

For more information go to www.fidelissecurity.com. Fidelis Cybersecurity is a portfolio company of Skyview Capital.