Fidelis®
Cybersecurity

DATASHEET

Fidelis Deception™

Wide Choice of Decoys from Real OS to Emulation VMs Provide High Fidelity Alerts

The Opportunity

Cybercriminals seek passwords and credentials to enter networks and applications in order to monitor and steal data. Capture the flag exercises highlight how human attackers analyze email, files, documents, and unstructured data for credentials, while automated malware mainly focuses on structured data in web browsers and apps. Access Credentials are a top priority for attackers to successfully enter and move laterally within networks. Each successful step helps an attacker or malicious insider to stay quiet, preventing digital “noise” that might otherwise give them away. *Knowing what attackers desire creates an opportunity for a deception defense with breadcrumbs and decoys; to lure, detect, and defend.*

The Challenge

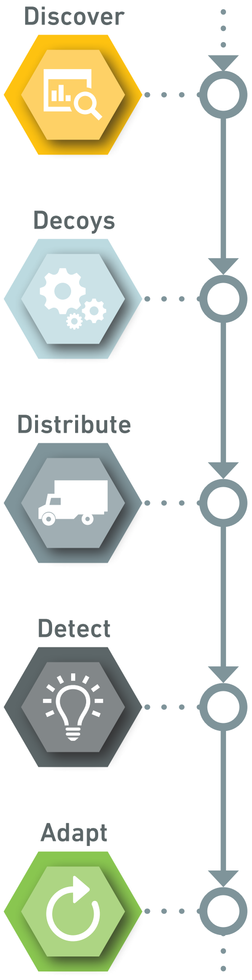
- Detect attackers, malicious insiders, and malware inside networks and cloud environments
- Deliver high fidelity alerts with few or no false positives
- Automate investigation and response workflow steps
- Increase effectiveness and efficiency of security analysts
- Learn TTPs of attacks to improve security defenses

The Solution

- Create a wide variety of decoys and breadcrumbs on-premises or in the cloud
- Deploy real OS decoys or emulate services and OS’s, including enterprise IoT devices
- Decoys run applications and services to engage attackers and consume time
- Detections created from decoy access, AD credentials, poisoned data, and traffic analysis
- No risk to resources or data, nor any impact to users or operations

“We found Fidelis deception to be very efficient. Its decoy aspect provided an excellent way to detect anomalies without having to sort through so much data as with other approaches.”

Weston Nicolls, SVP, Information Security Manager,
First Midwest Bank



Discover

- Continuously map networks, cloud, and assets
- Profiles created and updated for asset location, use, type, etc.
- **Result:** Automatically learns to create realistic deception layers

Decoys

- Automatically builds deception decoys from discovery
- Deception based on a wide variety of decoys
- **Result:** Real OS and persuasive decoys

Distribute

- Automatically deploys decoys in networks and cloud
- Seeds breadcrumbs in real assets and Active Directory
- **Result:** Rapid deployment and immediate effectiveness

Detect

- Alerts from decoy access and engagement
- Analysis and alerting of poisoned data use
- **Results:** High fidelity alerts with few false positives

Adapt

- Recognizes new assets, network, and cloud topologies
- Automatic updates to discovery mapping and decoys
- **Results:** Intelligent and active deception defense

How Deception Works

Deception becomes deterministic with breadcrumbs on real assets luring attackers, malicious insiders, and automated malware to decoys. Deception changes the playing field of security. Instead of searching in vain for the bad actor within an ocean of good data, deception delivers actionable alerts and events from decoys, AD credentials, poisoned data, and traffic analysis. These alerts have extremely high fidelity and few false positives. Using deception on-premises and cloud with fresh activity data creates persuasive deception layers that include devices, data, and behavior all designed to turn the tables on attackers. They pursue the lures to decoys so you can detect and defend.

Decoy Profiles

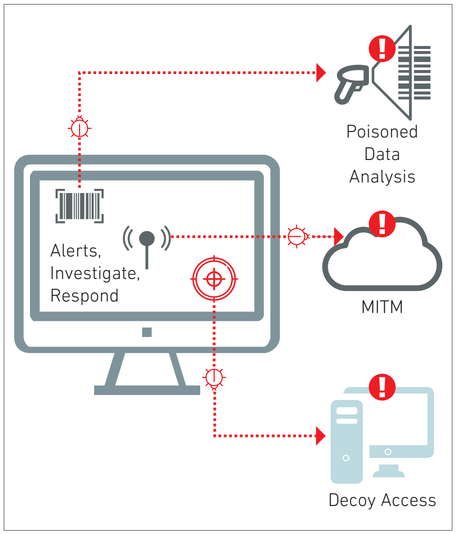
- Hardware — laptops, servers, routers, switches, cameras, printers, enterprise IoT devices, etc.
- Software — OS, apps, ports, services, applications, cloud assets, and similar data
- Decoys are unknown and obfuscated assets, no reason for employee access or use
- Consume attacker time with high interaction decoys and distract from real assets

Breadcrumb & Trap Profiles

- Traps: file, application, network, or credential based
- Breadcrumbs: files, documents, email, or system resources, etc.
- Poisoned data, credentials, and profiles that attackers use

Detection of Post-Breach Attacks

- Access of decoys as unknown assets (i.e. attackers, insiders)
- Data analysis showing the use of poisoned data (e.g. credentials)
- Monitoring attacker actions engaged with decoys and breadcrumbs
- Network analysis around decoys and data alerts



High fidelity alerts with very few false positives — on-premises or cloud

Active Deception

- Automates and adapts deployment of decoys and breadcrumbs
- Detects lateral movement, C2 traffic, and data exfiltration
- Visibility and forensics to learn TTPs (tactics, techniques, and procedures) and desired assets
- One console with complete deception telemetry for analysis and hunting, and action
- No impact to operations or users, no risk to data or resources

Why Choose Fidelis?

- ✓ Asset profiling and classification to determine deception layers
- ✓ Full automation of decoys including adaptation and freshness
- ✓ Real OS VM decoys, golden image OS decoys, or customer desired
- ✓ Emulation decoys for low risk interaction and file uploads
- ✓ Enterprise IoT decoys, plus web page loading into HTTP decoys
- ✓ Uploaded files sent to Fidelis cloud-based sandboxing
- ✓ Attacker path and security visibility from high speed sensors
- ✓ MAC address spoofing per decoy for authenticity
- ✓ Seamless workflows into Fidelis Network and Endpoint
- ✓ FIPS 140-2 Compliant for federal use

SC 2019 awards
Honored in the U.S.
Winner
Best Deception Technology Solution

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.

Fidelis-Deception-1903