DATASHEET

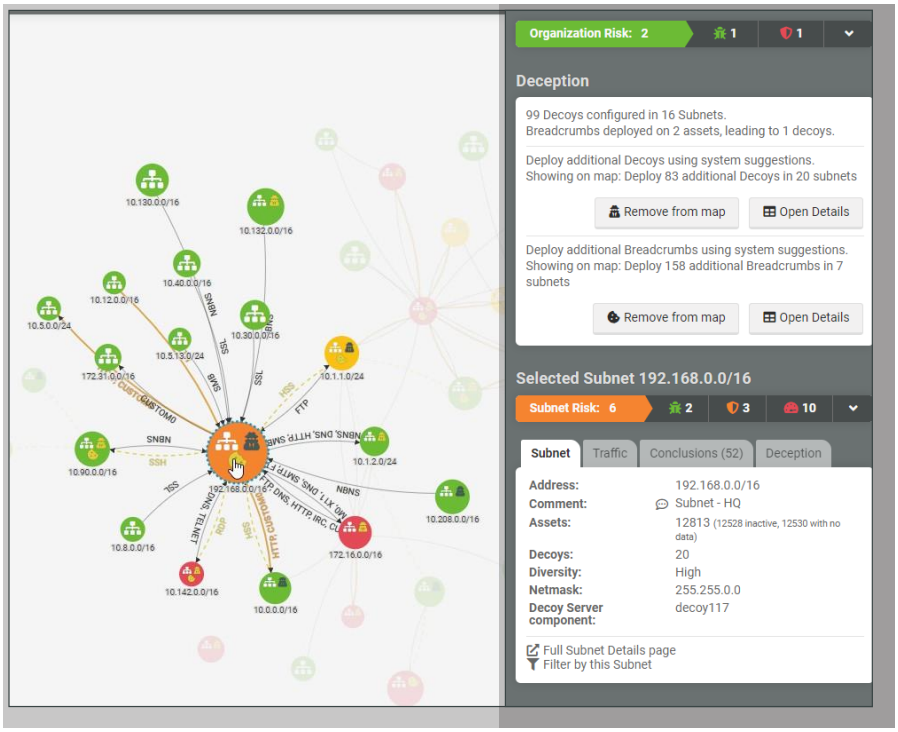
Fidelis Deception®

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

Outmaneuver Attackers with Dynamic Deception

Deception technology gives defenders an opportunity to reduce cyber dwell time by altering the adversaries' perception of the attack surface. Doing so slows down the attacker's ability to move laterally undetected, changes the economics and increases the attacker's risk, giving defenders more time understand TTPs and ultimately eradicate the threat from the environment.

Fidelis Deception allows organizations to quickly and accurately detect attackers, malicious insiders and malware already inside the network, engage with the attackers, and neutralize advanced cyber threats. With Fidelis, defenders can automatically create real, interactive OS decoys as well as emulated services and OS's, including enterprise IoT devices. Then attackers can be lured to the decoys via breadcrumbs that are continuously updated. Through a unique combination of adaptive intelligent deception, automatic terrain learning and visibility, Fidelis keeps the attackers guessing and dramatically reduces time-to-resolution from weeks and months, to hours and minutes.



Fidelis Deception leverages an organization's network terrain to automatically create decoys and suggested breadcrumbs to alter the perception of the attack surface.

Key Benefits

- ✓ Reduce dwell time with a smart alarm system to detect threats inside your network
- ✓ Detect external attacks and insiders to expose reconnaissance and lateral movement
- ✓ Learn details of attack paths, resource interests and initial compromised foothold systems
- ✓ Remove blind spots for unknown assets including legacy systems, enterprise IoT, and shadow IT
- ✓ Continuously profile and classify assets to facilitate deception layer creation and freshness
- ✓ Facilitate deception layer creation with full automation of decoys, including adaptation
- ✓ Decoy options to meet customer needs including real OS VM decoys, golden image OS decoys, and emulation decoys for low risk interaction and file uploads
- ✓ Lure attackers with breadcrumbs on real assets and Active Directory to divert and defend
- ✓ High fidelity alerts you can trust
- ✓ Enable Red Team and Blue Team risk simulations to determine enhanced decoy andbreadcrumb placement
- ✓ Seamless workflows into Fidelis Network® and Fidelis Endpoint®

How Deception Works

Deception becomes deterministic by publicizing decoys with breadcrumbs on real assets luring attackers, malicious insiders, and automated malware to the decoys. 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. 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 and medium interaction decoys and distract from real assets

Breadcrumb & Trap Profiles

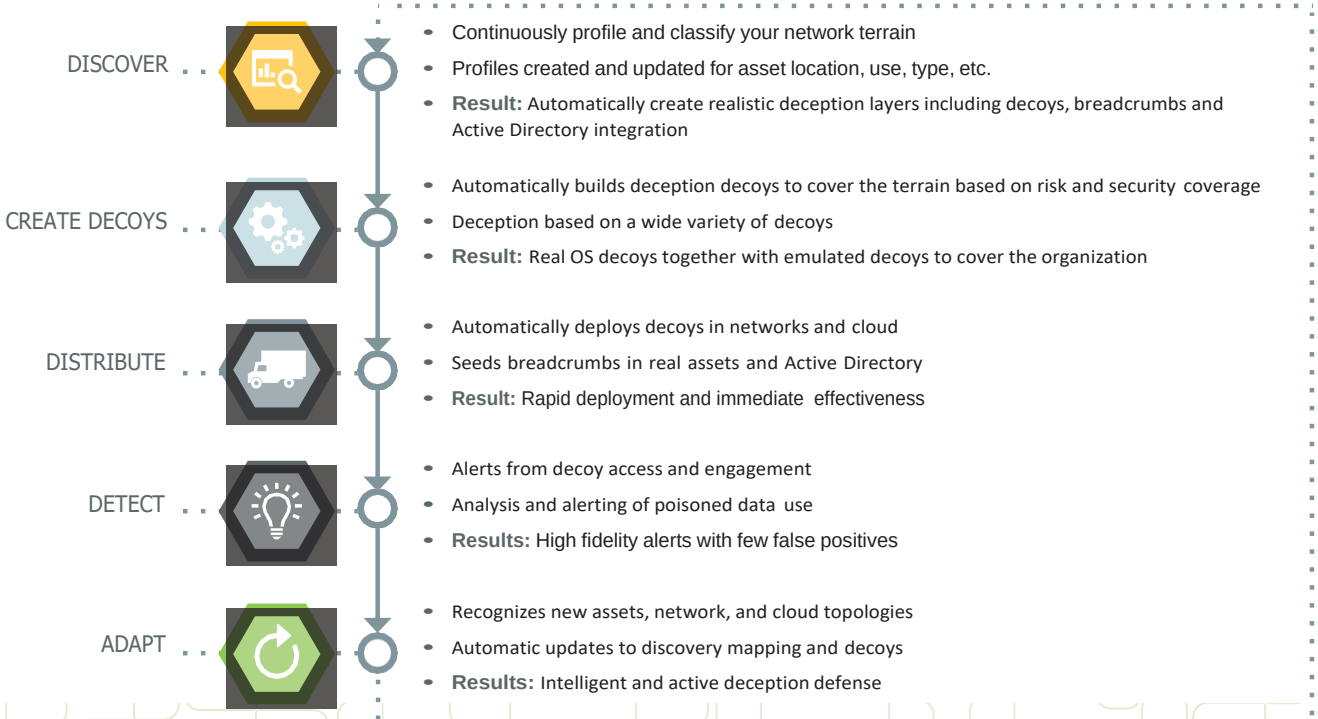
- Traps: file, application, network, or credential based
- Breadcrumbs: files, documents, email, or system resources, etc.
- Poisoned data, credentials, and profiles that attackers use

Detection of Post-Breach Attacks

- 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

Active Deception

- Automates and adapts deployment of decoys and breadcrumbs
- Detects lateral movement, attackers' reconnaissance and activities
- 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



Contact Us Today to Learn More

Three Wire Cybersecurity | 800.652.4020 | info@threewiresys.com