DATASHEET

Fidelis Deception®

Turn Adversaries into Targets

These days, it's a matter of when—not if—your network will be breached. Too often, organizations only realize an attacker is inside their systems after devastating data loss or ransomware detonation. Fidelis Deception® gives control back to cyber defenders. With its sophisticated and intelligent active deception capabilities and extremely high-fidelity alerts, organizations gain a solid foundation for proactive security and cyber resiliency. It shifts the advantage from the attacker to the defender by using decoys and lures to trap attackers in the deception layer, giving you time to detect attackers earlier, study their moves, and defeat them before damage can be done. You improve the effectiveness and efficiency

How Fidelis Deception Works

No security platform is impenetrable. Cyber adversaries constantly innovate and evade security defenses on networks,endpoints, and cloud environments. They only need one vulnerable point of entry, while cyber defenders must protect everything. The advantage for defenders, however, is knowledge of the environment and how the adversaries operate. It takes time and efforts for adversaries to find a point of entry, learn where valuable assets reside, impersonate user accounts, and move laterally undetected. That time is your opportunity to strike first—and strike hard.

Give Adversaries What They Came for – and Nothing They Can Use

Fidelis Deception automatically and continuously maps your cyber terrain, calculating asset risk, and determining where adversaries are most likely to strike. With minimal effort on your part, Fidelis Deception uses machine learning and intelligence to create decoys from real assets, emulated services, OSs, containers, cloud assets, and enterprise IoT (Internet of Things) devices. It continuously updates lures and breadcrumbs, decoys, and fake active directory (AD) accounts to keep the deception layer realistic and fresh. Attackers—both external and internal—believe they have found legitimate ways to impersonate users, escalate privileges, and gain access to critical assets, when, in reality, they're trapped at the deception layer.

Trust Your Alerts

Fidelis Deception delivers high-fidelity alerts and events from decoys, AD credentials, poisoned data, and suspicious traffic. Because there is no valid reason for anyone (or any process) to access a deceptive object, Fidelis Deception alerts are a true call to action. While the attackers or malware busy themselves within the deception layer, your security team discovers their presence and starts tracking their movements and actions.

Study an Attacker's Every Move

Fidelis Deception alters adversaries' perception of the attack surface. It slows down the adversary's ability to move laterally undetected, which increases the adversary's risk while giving your defenders more time to understand TTPs (tactics, techniques, and procedures).

Maintain Cyber Resiliency

Once an attacker or malware interacts with the deception layer, they pose a significantly lower risk to your organization. They believe they've found what they are looking for, which keeps your real assets, and access to those assets, intact. Your cyber defenders can then operate inside the decision cycle of the adversary, and use known and proven methods for mitigation and eradication—all without disruption to ongoing business operations.

Kick Them Out and Shut the Door

Once your cyber defense team understands attacker TTPs and gains perspective on the types of assets that are under attack, they can use that intelligence to stop the threat. With intelligence that learns and grows, and a foundation built on machine learning, Fidelis Deception can help your team improve security posture to prevent or significantly reduce the likelihood of success in future, similar attacks.

Fidelis Deception Includes

Active Threat Detection is an integral part of the Fidelis Elevate framework. Active Threats correlate data from Fidelis Network, Deception, Endpoint, and Sandbox alerts

Decoys

Convincing duplicates of high-value assets that give attackers exactly what they're looking for—or so they

- Hardware: Laptops, servers, routers, switches, cameras, printers, enterprise IoT devices, etc.
- Software: OS, apps, ports, services, applications, and similar data. Cloud: Cloud OS, cloud applications, OneDrive,
- SharePoint, AD users (including Azure AD), cloud user accounts

Breadcrumbs

Lures that draw adversaries away from real assets so that they get trapped in the deception layer or so they think.

- Breadcrumbs: Files, documents, emails, applications, memory credentials, registry keys, system resources, network activities, canary files, etc.
- Monitors IoT and cloud resources as deceptive objects.

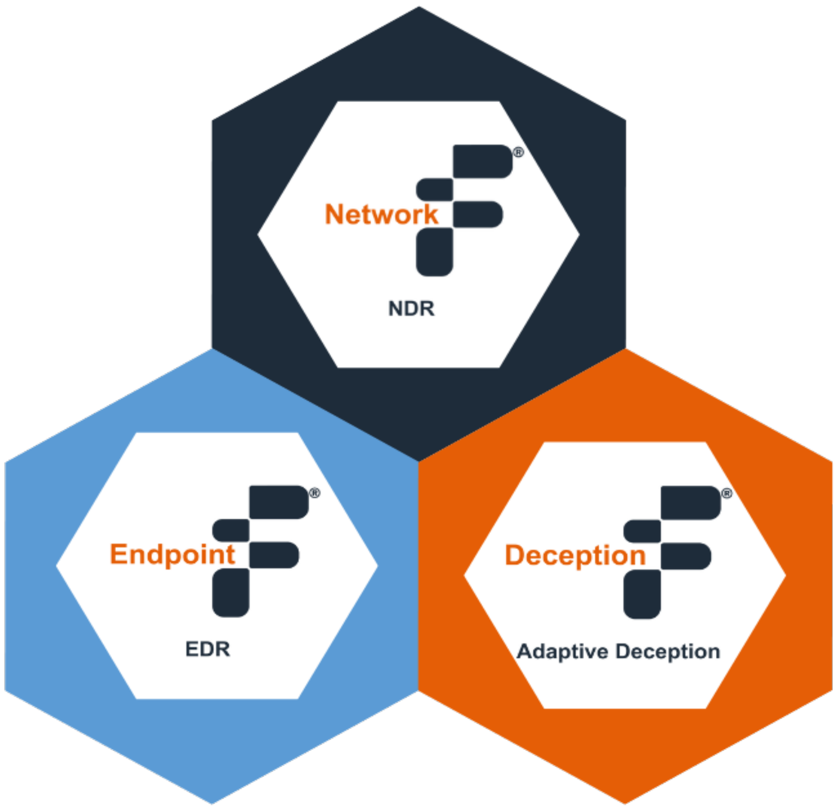
Active Deception

Automated, intelligent proactive cyber defense that alleviates operational burden while supporting cyber resiliency initiatives.

- Continuously maps cyber terrain and provides risk analysis across on-premises, cloud, endpoints, containers, and IoT environments.
- Uses machine learning to automate and adapt deployment of decoys and breadcrumbs based on asset risk.
- Proactively detects lateral movement, attackers' reconnaissance, and activities.
- Provides visibility and forensics to learn TTPs and identify targeted assets.
- Consolidates telemetry, analysis, hunting, and action on a single console.
- Runs without impacting operations or users, and does not increase risk to data or resources.
- Improves cyber resiliency by maintaining business operations through active cyber events.
- Provides Red Team and Blue Team risk simulations to determine enhanced decoy and breadcrumb placement for continual improvement.

Part of the Fidelis Elevate®

While Fidelis Deception can be used on its own, unifying it in the Fidelis Elevate® open and active eXtended Detection and Response (XDR) 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. They also form a foundation of intelligence to keep you ahead of the next attack.



About Fidelis Security®

Fidelis Security® is the industry innovator in proactive cyber defense, safeguarding modern IT for global enterprises with proactive XDR and CNAPP platforms. Fidelis Security consolidates IT security operations to shrink attack surfaces, automate threat detection, and accelerate analysis, forensics, and response so that organizations remain resilient through cyber-attacks and emerge stronger and more secure. Fidelis Security is trusted by top commercial, enterprise, and government agencies worldwide.