How Fidelis Deception® Strengthens Network Detection and Response

Network Detection and Response systems excel at monitoring network traffic and identifying patterns, but they face inherent challenges with sophisticated threats that mimic legitimate behavior. Fidelis Deception® addresses these NDR limitations by creating definitive detection points that eliminate ambiguity in threat identification.

What Are the Main Limitations of NDR Systems?

Traditional NDR relies on behavioral analysis and signature matching, which creates detection gaps when attackers use legitimate tools and protocols. False positives consume analyst time while true threats may blend into normal network activity. Unlike traditional security measures and traditional security approaches, which often struggle to detect sophisticated threats, deception-enhanced detection and response provides a proactive and resilient layer that identifies malicious activity with greater accuracy. Fidelis Deception® eliminates this uncertainty by deploying assets that legitimate users never access, making any interaction a clear indicator of malicious activity.

When integrated with Fidelis Network®, deception technology transforms the network environment into an active detection grid where attackers reveal themselves through interaction with strategically placed decoys and lures. This integrated security solution enhances network security by providing comprehensive detection and response capabilities across the organization’s infrastructure.

How Does Deception Technology Integrate with NDR Architecture?

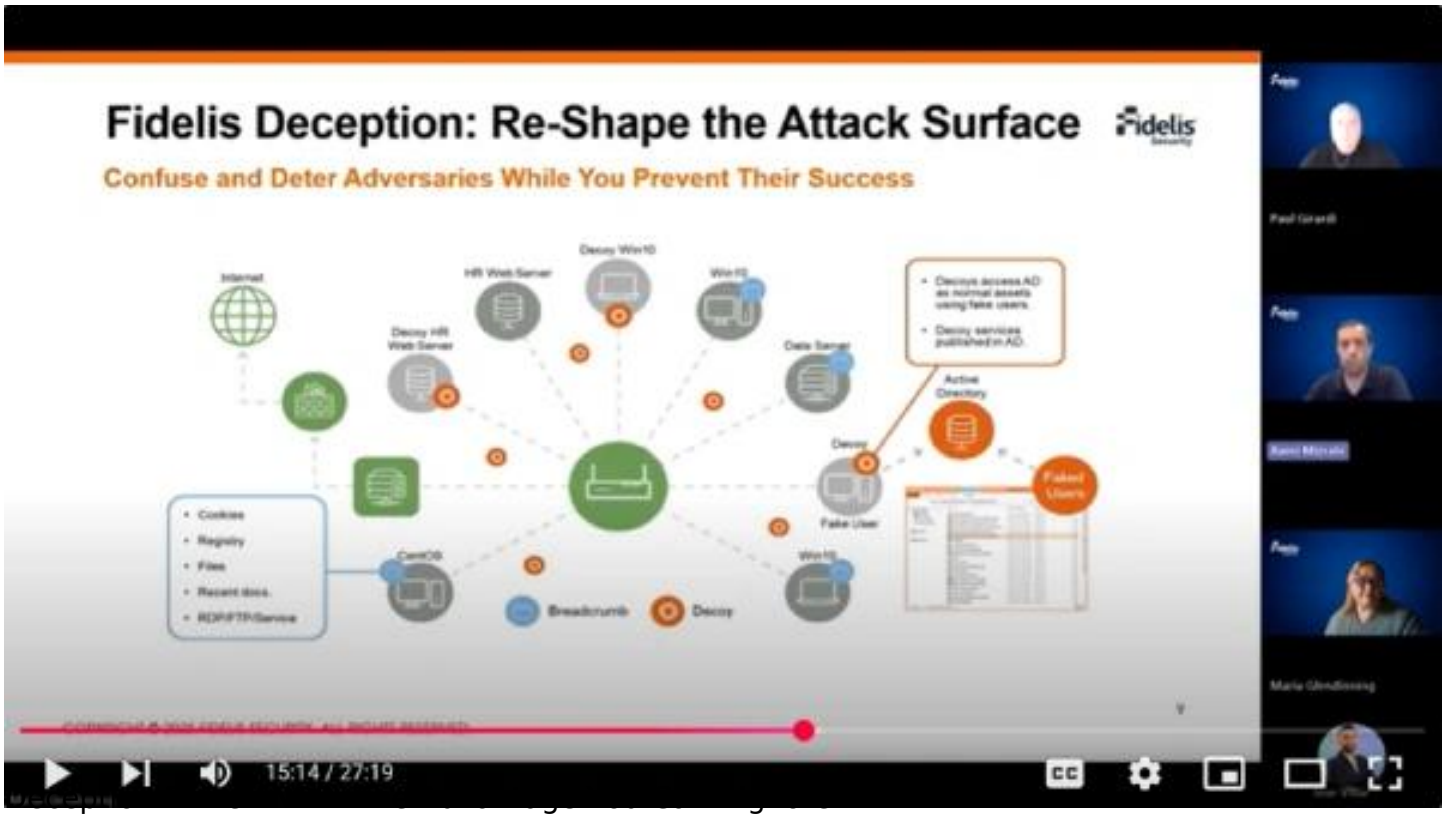
Fidelis Deception® employs automated terrain mapping to analyze network topology and asset relationships. Machine learning algorithms determine optimal placement for deceptive assets based on attacker movement patterns and high-value target proximity.

The system deploys three categories of deceptive assets:

- **Network Infrastructure Decoys** Emulated servers, workstations, and network devices that mirror production environments. These decoys run authentic services and respond to network reconnaissance with realistic behavior patterns.
- **Credential and Data Lures** Strategic placement of fake credentials, configuration files, and database connection strings that attract attackers seeking privilege escalation or lateral movement opportunities.
- **Active Directory Integration** Deployment of fake user accounts and service principals within Active Directory, including Azure AD environments, creating authentication traps for credential harvesting attempts.

Unlike real assets and legitimate assets, which are genuine components of the production environment, fake systems and fake assets are deployed as part of deception tools to serve as deceptive elements. These elements, such as deception decoys and lures, are designed to appear authentic and lure attackers away from actual resources, enhancing early detection and incident response.

Deception techniques, including the use of deception decoys and broader deception strategies, are integrated to proactively detect, engage, and analyze adversaries, making it more difficult for attackers to distinguish between real and deceptive assets.



- Discover the blind spots in traditional NDR
- Understand how deception improves detection precision
- Hear why Fidelis is trusted for advanced threat detection

Watch On-Demand Webinar Now

How Does Deception Strengthen NDR Detection Capabilities?

Eliminating Detection Ambiguity

Fidelis Network® monitors network traffic for suspicious patterns, but legitimate administrative activities can trigger false alarms. Deception integration provides unambiguous detection by creating assets that serve no legitimate purpose, including clear identification of unauthorized access attempts. When Fidelis Network® detects traffic to these deceptive endpoints, security teams receive definitive threat indicators.

Enhanced Lateral Movement Detection

Traditional NDR identifies lateral movement through traffic analysis and behavioral patterns. Deception assets are specifically designed to lure attackers and deceive attackers by presenting fake environments, such as honeypots and honey credentials, which entice malicious actors to

engage with them. Security teams can closely monitor how attackers interact with these deceptive assets, gaining valuable insights into their tactics and intentions.

Fidelis Deception® strengthens this capability by creating attractive targets throughout the network infrastructure. Attackers naturally gravitate toward these decoys during reconnaissance, providing early detection before reaching critical assets.

Improved Threat Intelligence Generation

Network traffic analysis provides technical indicators, but deception interactions reveal attacker's intentions and methodologies. By monitoring attacker behavior during these deception interactions, organizations gain valuable intelligence and valuable insights that enhance their understanding of threats and improve detection capabilities. The combination generates richer threat intelligence for NDR systems, improving detection rule accuracy and reducing false positive rates.

How Does Deception Improve NDR Performance?

NDR Component Traditional Capability Deception Enhancement Traffic Analysis Pattern recognition and anomaly detection Definitive threat confirmation through decoy interaction Behavioral Analytics Statistical modeling of normal network behavior Elimination of baseline uncertainty for deceptive assets Threat Hunting Hypothesis-driven investigation of suspicious activity Automated threat revelation through attractor deployment Incident Response Correlation of multiple weak signals High-confidence alerts enabling immediate response Forensic Analysis Reconstruction of network events and timelines Complete attacker methodology capture through interaction logs

Deception integration enables extended detection by expanding visibility across networks, endpoints, and cloud environments, going beyond traditional siloed tools. It enhances endpoint detection by providing early threat identification and attack chain visibility through decoy interactions on endpoints. Additionally, deception leverages advanced analytics for automated threat detection, incident triaging, and response, delivering high-fidelity insights and improving overall detection and response capabilities.

Real-Time Alert Correlation

Fidelis Network® correlates deception alerts with network traffic analysis, creating comprehensive attack timelines. When an attacker interacts with deceptive assets, the NDR system immediately contextualizes the threat with historical network behavior and infrastructure mapping.

This real-time alert correlation strengthens the overall security ecosystem by integrating deception technology with other security tools, enabling more effective threat detection and response across the entire attack lifecycle.

Automated Response Integration

The deception layer enables automated containment actions based on definitive threat indicators. Unlike behavioral alerts that require investigation, deception interactions trigger immediate response protocols, reducing mean time to containment and helping to stop attackers before they can cause significant harm.

5 Must-Haves to Rev Up

- Deep Visibility
- Historical and Real-time Context
- No Alert Fatigue
- Automated Response Playbook

[Download the Whitepaper Now!]

How Is Deception Technology Implemented with NDR Systems?

Terrain Mapping and Asset Profiling

Fidelis Deception® continuously maps network topology and calculates asset risk profiles. Asset profiling is a key element in effective deception deployment, as it helps identify which resources are most attractive to attackers and supports the recording of attacker activity for improved cyber defense strategies. This intelligence guides both deception deployment and NDR monitoring priorities, ensuring coverage of high-value attack paths.

Dynamic Decoy Management

The system automatically updates deceptive assets to maintain authenticity as network infrastructure evolves. This dynamic decoy management supports a moving target defense strategy, making it harder for attackers to adapt by continuously shifting and complicating potential attack vectors. This ensures NDR enhancement remains effective against reconnaissance attempts and prevents attacker adaptation.

Cross-Platform Intelligence Sharing

Deception events integrate with Fidelis Network® through standardized APIs, enabling bi-directional intelligence sharing. Network analysis informs deception placement while deception interactions validate NDR alerts.

Cross-platform intelligence sharing is a critical component of modern defense strategies, enabling organizations to proactively detect and mitigate threats before they escalate.

What Advanced Threats Can Deception-Enhanced NDR Detect?

Command and Control Detection

Traditional NDR identifies C2 communication through traffic analysis and domain reputation. Attackers often attempt to gain access to networks by exploiting vulnerabilities, and deception technology is designed to detect when attackers believe they have gained access or have gained unauthorized access to critical assets by monitoring their interactions with decoys and traps. Deception technology enhances this by deploying honeypot systems that attract malware beaconing, providing definitive C2 channel identification.

Insider Threat Detection

Network behavior analysis struggles with insider threats using legitimate access. Deception assets, including strategically placed fake assets such as decoy servers, databases, and credentials, are deployed throughout the infrastructure to create detection points for inappropriate access attempts, strengthening NDR coverage of internal threats.

Advanced Persistent Threat Identification

APT groups employ sophisticated evasion techniques that challenge traditional NDR. Artificial intelligence is leveraged by modern XDR platforms to automatically analyze and correlate data

from multiple sources, enhancing the detection of advanced persistent threats. Deception integration creates persistent detection opportunities throughout long-duration campaigns, revealing attacker presence regardless of evasion sophistication.

Deployment Considerations for Deception-Enhanced NDR

Network Integration Points

Fidelis Deception® integrates multiple network layers to strengthen NDR visibility. Strategic placement includes network segments, cloud environments, and endpoint systems to create comprehensive coverage.

Scalability and Management

The deception layer scales automatically with network growth, maintaining NDR enhancement as infrastructure expands. Centralized management ensures consistent coverage across distributed environments.

Performance Impact

Deception assets operate with minimal network overhead, preserving NDR system performance while enhancing detection capabilities. Automated management reduces operational burden on security teams.

What results can organizations expect from deception-enhanced NDR?

Organizations implementing deception-enhanced NDR report significant operational improvements including reduced false positive rates, faster threat detection, and improved analyst confidence in alert prioritization. The definitive nature of deception alerts enables security teams to focus their investigation efforts on genuine threats.

How Does Fidelis Deception® Integrate with the Broader Security Platform?

Fidelis Deception® operates within the Fidelis Elevate XDR platform, providing unified visibility across network, endpoint, and cloud environments. This integration ensures deception intelligence enhances all security operations, not just network detection.

The platform correlates deception events with endpoint telemetry, email security alerts, and cloud activity monitoring, creating comprehensive threat visibility that strengthens organizational security posture beyond traditional NDR capabilities.

Our Customers Detect Post-Breach Attacks over 9x Faster

Our Secret – Integrated #1 Deception Technology

- Cut threat detection time by 9x
- Simplify security operations
-

Provide unmatched visibility and control

Talk to Expert

Conclusion and Next Steps

Fidelis Deception® transforms NDR from a reactive monitoring system into a proactive threat detection platform by eliminating detection uncertainty and providing definitive indicators of attacker presence throughout network infrastructure.