How does Fidelis NDR Delivers Proactive Asset Risk Mitigation?

Organizations operating in sprawling, hybrid IT environments often lack complete visibility into all assets and their communication patterns. This gap creates blind spots where vulnerabilities go undetected, third-party components remain unpatched, and unauthorized lateral movement can occur without raising alarms.
When unknown assets slip through discovery processes, attackers exploit them quietly—probing for weaknesses, injecting malicious payloads, and moving laterally across network segments before any signs of compromise appear. Legacy security tools generate overwhelming alert volumes without clear prioritization, leaving teams to chase false positives while real threats slip by.

This blog will demonstrate a structured, proactive, risk-based asset protection methodology using advanced Network Detection and Response (NDR). Readers will learn how to perform comprehensive asset discovery and classification, apply contextual risk scoring, detect threats within encrypted traffic, and establish threat hunting and automated containment workflows—all designed to shift security operations from reactive firefighting to strategic defense.

Why proactive vs reactive asset risk mitigation matters now

Rapidly changing environments increase blind spots

Today’s digital infrastructure—hybrid-cloud, SaaS apps, IoT—expands your attack surface daily. Without continuous asset risk monitoring, new systems go untracked and become prime targets. For example, a recently spun-up cloud instance without active discovery could harbor unpatched software, quietly becoming entry points. Addressing this requires proactive asset protection, not just reacting once attackers have slipped through.

Threat volumes overwhelm reactive defenses

Cyber threats aren’t slowing down—they’re automating. Malicious traffic, lateral movement, or minor reconnaissance can herald a larger breach. By the time alerts surface in legacy systems, attackers may have already exfiltrated sensitive data. That’s why real-time asset detection and response, powered by proactive network threat detection, is essential to get ahead of risk buildup.

Asset value doesn’t equate to asset visibility

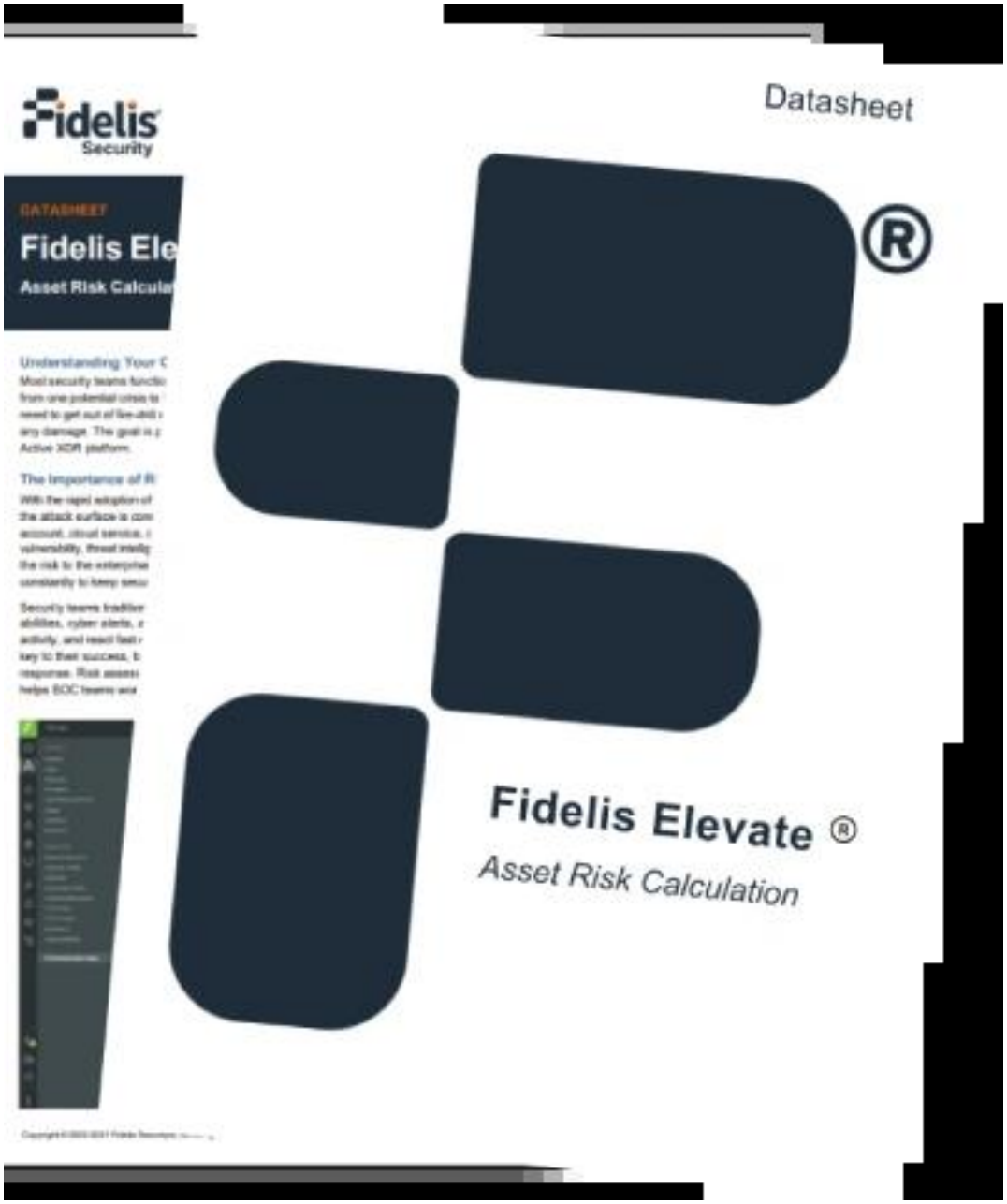
Not all assets are equally critical—but without risk-based asset security, everything looks equally risky. This leads to noise, fatigue, and scattered effort. Organizations need to score assets contextually, focusing on high-value systems seen in the wild. That’s the core of risk-based vulnerability management and deciding where to invest protection first.

Prioritize the right risks, protect what matters!

- Not all risks are equal—learn how to find the weak spots before attackers do:
- Understanding Your Cyber Risk

- How do you calculate risk?
- Protect your assets with risk assessment

Download Datasheet



What steps build a proactive, risk-based asset protection strategy?

Discover, classify, and map your entire cyber terrain

Asset risk security starts with visibility. If you're blind to 30% of your infrastructure, attackers aren't. Automated asset discovery identifies servers, workstations, IoT, and cloud instances—then profiles and classifies them based on sensitivity and vulnerability. That gives you a terrain map, revealing where high value assets sit—and where to focus first.

Apply risk-based vulnerability management across assets

Once assets are mapped, vulnerability scans add CVE context. But what matters is knowing which vulnerable assets are exposed or targeted. By overlaying detection data on vulnerability results, teams can focus remediation on the most actively threatened systems—aligning with proactive vs reactive asset risk mitigation best practices.

Establish behavioral baselines for threat hunting

Good defense relies on knowing what “normal” looks like. Behavioral analytics learn eastwest and northsouth traffic patterns, login behavior, file flows, and application profiles. Threat hunting with NDR becomes meaningful when deviations are flagged early—before reconnaissance or lateral movement escalate.

Orchestrate responses to threats immediately

Detection is just stage one—response must follow. Predefined playbooks enable immediate actions: quarantining suspicious hosts, blocking data uploads, or triggering forensic workflows. When configured correctly, this enables real-time asset detection and response—catching threats before they become breaches.

Keep adapting defenses over time

New assets are created; attack patterns evolve. Continuous tuning of asset risk scores, scan frequency, and response thresholds is essential. Proactive security isn’t “set and forget”—it’s iterative, informed by new insights and actual incidents.

How Fidelis NDR enables Proactive Risk-based Asset Protection

Now—how can Fidelis Network® NDR uniquely deliver these capabilities?

Deep Session Inspection enables full asset visibility

Problem: Encrypted and multi-protocol traffic hides signals.
Fidelis NDR uses patented Deep Session Inspection® to inspect all traffic—across ports, protocols, SSL/TLS—and extract rich metadata like file activity, credentials, or decoy interaction.
For example, a covert file transfer between asset groups triggers DSI—even if the session’s encrypted. You gain asset risk intelligence and detection capability in a single sweep, dramatically shrinking blind spots.

Fidelis DSI – Advanced Data inspection and Threat Detection Capabilities

- Content Inspection
- Content Identification
- Full Session Reassembly
- Protocol and Application Decoding

Download the Datasheet

Automated terrain mapping elevates high-risk assets

Problem: Asset sprawl leads to hidden critical systems.
Fidelis automatically discovers and classifies every asset—legacy servers, IoT devices, and cloud instances—while generating a risk score by identifying active vulnerabilities and network exposure .
If a new VPN-connected workstation exhibits unpatched services, it’s flagged—and prioritized, enabling risk-based asset security from day zero.

Behavioral analytics support proactive network threat detection

Problem: Unknown threats fly under the radar.
Fidelis NDR applies multiple machine learning models—across external, internal, application protocols, and data movement contexts—to identify anomalies such as unusual login patterns or lateral movement.
For instance, spiking connections from a legacy server to multiple internal endpoints late at night triggers alerts tied to MITRE TTP for lateral movement—empowering threat hunting with NDR backed by behavioral context.

Retrospective analysis empowers threat hunting

Problem: Fast threats evade real-time detection.
Fidelis stores rich metadata from each session and retroactively applies new threat intelligence or signatures .
That means if a new exploit is discovered, you can run historic asset traffic for matches—even without prior alerts. It exposes stealth attacks and deepens asset risk monitoring over time.

Automated response controls protects at pace

Problem: Manual workflows delay response and increase risk.
Fidelis NDR supports inline or out-of-band blocking, sandbox-based threat analysis, network DLP, and integration with endpoint isolation through Elevate playbooks.
For example, if data exfiltration is detected, the system can automatically drop the session, quarantine the host, block specific asset communications, and open a high priority ticket—all in real time.

What real-world benefits do security teams gain?

- ### Accelerated threat detection and reduced dwell time

  With full visibility and behavior-based detection, Fidelis NDR helps organizations identify and respond to threats up to nine times faster than competitors. That speed dramatically reduces dwell time and the risk of data exfiltration from high risk assets.

- ### Reduced alert fatigue through risk-based prioritization

  Alerts tied to critical assets or unusual behavior attract immediate attention, while noise from benign systems is silenced. Analysts focus on what threatens business continuity, improving efficiency and decision confidence.

- ### Broader coverage across hybrid architectures

  Sensors deploy on-prem, in cloud, and across email or web proxies—covering traditional and modern environments. The result: proactive asset protection wherever data flows, not just on the perimeter.

- ### Elevated threat hunting and forensic analysis

  With retrospective search across stored metadata, your team can hunt for artifacts tied to new CVEs or IOC feeds, even weeks later. Asset risk monitoring becomes forensic-grade, not just reactive.

- **Playbook-driven incident response streamlines operations**

  Prebuilt workflows reduce response latency—block connections, contain endpoints, alert stakeholders, and log tickets automatically. This orchestration empowers smaller teams to respond at scale.

What should your organization do next?

1. **Deploy Fidelis NDR sensors** across network chokepoints—cloud gateways, East-West segments, and perimeter links—to begin full-session capture.
2. **Enable Deep Session Inspection and behavioral analytics**, tuning model thresholds to align with your business environment.
3. **Activate asset discovery and risk scoring**, integrating vulnerability scan feeds for context-aware prioritization.
4. **Configure automated response policies**: asset quarantine, session blocking, endpoint integration via Elevate.
5. **Run retrospective hunts** using threat intelligence updates to evaluate past asset behaviour and fine-tune detection.
6. **Evaluate performance quarterly**, benchmarking detection timelines, containment success, and asset risk reduction metrics.

Give Us 10 Minutes – We'll Show You the Future of Security

See why security teams trust Fidelis to:

- Cut threat detection time by 9x
- Simplify security operations
- Provide unmatched visibility and control

Book a Demo Now!

Final thoughts

Shifting from reactive firefighting to proactive asset protection is essential in today's threat landscape. Traditional asset security tactics lack speed and context. By leveraging risk based vulnerability management, behavioral anomaly detection, and real-time asset detection and response, Fidelis NDR fills the gap.

Fidelis Network Detect and Response(NDR) offers full visibility, rich metadata collection, automated asset risk scoring, forensic-grade retrospective analysis, and real-time orchestration—all designed to empower security teams to detect, protect, and most importantly, respond before breaches take hold.