Fidelis Elevate® (XDR): A Proactive Way to Eliminate Blind Spots

The growing complexity of IT environments—across cloud, IoT, and hybrid settings—has ushered in new opportunities for innovation but also expanded the threat landscape for cyber vulnerabilities. These vulnerabilities, now known as blind spots, serve as areas within an organization's security posture that are ignored or poorly monitored.

Blind spots are extremely dangerous because they create an open backdoor for attackers, and they often go unnoticed until it is too late. To eliminate blind spots in modern cybersecurity, organizations need tools that can provide centralized visibility and proactive threat detection. Tackling these challenges needs strong, consolidated solutions. Rather than relying on point solutions, Fidelis Elevate® (XDR) is a holistic approach to unifying visibility, rapidly automating threat detection, and enabling organizations to detect and remediate threats quickly.

To further understand how Fidelis XDR solution can help eliminate blind spots, let's first answer your question – What is Blindspot?

What are cybersecurity blind spots?

"Twenty-nine percent of organizations admit to having "blind spots" on their networks that limit visibility for threat detection."

Understanding XDR requirement by Fidelis Security

Blindspots are undetected weaknesses or an area of organization infrastructure that is not monitored or protected properly. They can come from misconfigured devices, unregulated endpoints, or shadow IT (systems not approved by the IT department). And those gaps become the critical weak points in an organization's defense strategy.

Attackers hide in plain sight by taking advantage of blindspots in the security you deploy in place. An unmanned IoT device, or a forgotten server, may provide the means for malware or data exfiltration. Blindspots occur when parts of an organization's IT infrastructure are poorly monitored or overlooked, making it essential to adopt solutions designed to eliminate blind spots effectively. These hidden threats often lead to extended dwell times, where attackers remain undetected for weeks or even months, compounding the damage.

Challenges in Detecting and Mitigating Blindspots

- ### Lack of centralized visibility

  When organizations scale their infrastructure such as on-premises, cloud, IoT, and hybrid environments, keeping track of all assets becomes increasingly difficult. The lack of centralized visibility and overwhelming data volumes are primary reasons organizations struggle to eliminate blind spots in their cybersecurity framework.

- ### Overwhelming data volumes

  The large volume of data that modern IT systems generate can douse security teams in vast amounts of information, often obscuring it to the point that important anomalies are

missed that could indicate emerging threats.

- **Limited Resources**

  The reality is that a lot of organizations simply do not have the tools or manpower to monitor all components of their IT infrastructure—endpoints, networks, and cloud environments—a fact that leaves gaps that adversaries can take advantage of.

- **Insufficient Threat Intelligence**

  Without up-to-date threat intelligence, organizations find it hard to recognize new vulnerabilities or attack patterns that can be used to exploit areas of an organization that are not monitored.

What is Fidelis Elevate® (XDR)?

Fidelis Elevate® is an Extended Detection and Response (XDR) solution designed to maintain security infrastructure with Zero trust principle. The deception technology continuously monitors the encrypted traffic, detects anomalies and raises alerts to the SOC teams for any evasive attempt. It neutralizes threats or suspicious activity as an automated response to support its zero-trust access principle.

The integrated deception technology tune defense and cams change the attack surface to deceive adversaries and while the attackers focus on the deceptive path, defenders would have all the information about the attack and the source of the event. Moreover, its zero-trust architecture continues to monitor the cloud system, data centers, endpoints, IoT and disable threats in real time.

Fidelis Elevate® ensures seamless business operation thereby proving cyber resilience. It provides easy integration with tools like Palo Alto Cortex XDR, D3, Fireeye NX, SentinelOne, IBM Qradar, Devo, Zscaler and more. With all its advanced functionalities, Fidelis Elevate® can be proved as a worthwhile choice for XDR.

Shift the Advantage to Your Favor with Fidelis Elevate

Continually tune your defenses and neutralize threats before they cause damage to your business operations:

- Eliminate Blind Spots
- Understand Your Environment
- Control the Outcome

Download Solution Brief

Key Features of Fidelis Elevate® to Eliminate Blind Spots

In a world where cyber threats are increasingly sophisticated, eliminating blindspots requires more than just reactive measures—it demands proactive, intelligent, and integrated solutions.

Fidelis Elevate® (XDR) addresses these challenges head-on with a robust suite of features designed to deliver security. Here’s how its key features work to uncover and mitigate blind spots.

Centralized Visibility

Fidelis Elevate® continuously maintains a deep check within the network, endpoints, cloud assets, accounts and more to provide a real-time report and risk profiling. It details the data movement across the environment, maps IT resources and locates the data centers within the organization. The Zero Trust Architecture tracks any kind of external influence and also ensures safe authentication and logins to mitigate blind spots.

Automated Threat Detection and Response

Fidelis Elevate® is designed to detect suspicious activity within a network, monitor doubtful encrypted packets, quarantine infected endpoints by using heuristics and advanced technology and take actions as per the guided scripts. The advanced machine learning and endpoint metadata provide real time threat response to secure data and ensure smooth operations.

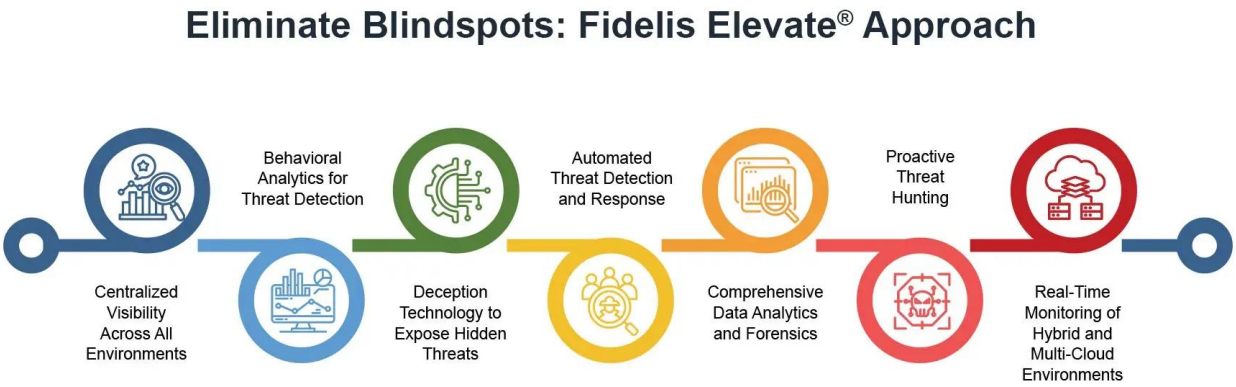
Deception Technology

Fidelis Elevate® activates its deception technology to mislead the attackers and creates a false pathway while collecting the source of the event. While it provides deceptive information to the attackers, the management got enough time to inspect the event and measure the intensity.

Data Analytics and Forensics

Fidelis Elevate® analyzes the data accessed by users and details the types of access request within the network. With its own evaluation system, Fidelis Elevate® provides internal and external threat forensics. It ensures data transmutation without leakage and prevents unauthorized exfiltration.

How Fidelis Elevate® Eliminates Blind spots: A Step-by-Step Approach



Fidelis Elevate® adopts a multi-faceted prevention approach to eliminate these vulnerabilities combining advanced technology with intelligent workflows. Here's a step-by-step look at how Fidelis Elevate® uncovers and removes blind spots to enhance security and resilience.

Centralized Visibility Across All Environments

What it does?

Fidelis Elevate® provides a unified dashboard that integrates data from endpoints, network and cloud.

How it Helps?

This means that every part of the IT infrastructure is monitored, which ultimately means that no assets or activities can slip through the cracks by breaking down silos.

Behavioral Analytics for Threat Detection

What it does?

It creates a baseline of normal activity and applies advanced analytics to detect anomalies.

How it Helps?

Fidelis instantly flags unusual behaviors, like new access points or sudden volume of data being transferred, exposing threats once hidden in blind spot.

Deception Technology to Expose Hidden Threats

What it does?

Fidelis Elevate® deploys decoy and to bait and traps an attacker.

How it Helps?

Decoys deceive attackers who are targeting blindspots into interacting with them, enabling our

security teams to detect and respond proactively.

Automated Threat Detection and Response

What it does?

Fidelis uses automation for the detection, classification, and mitigation of threats in real time.

How it Helps?

Rapid response minimizes dwell time; making sure threats in blindspots are neutralized before they can breach and cause any impact.

Comprehensive Data Analytics and Forensics

What it does?

Monitor and analyze large volumes of data across systems to identify hidden trends and vulnerabilities.

How it Helps?

Provides deep insights into potential blindspots, enabling preventive measures and better preparedness.

Proactive Threat Hunting

What it does?

Fidelis enables security teams to hunt for threats that may be bypassing traditional detection.

How it Helps?

Detects advanced persistent threats (APTs) and insider threats that frequently take advantage of blindspots.

Real-Time Monitoring of Hybrid and Multi-Cloud Environments

What it does?

Monitors diverse IT environments and maintains holistic protection on premises, hybrid, and cloud infrastructures.

How it Helps?

Eliminates visibility gaps introduced by complex and dynamic cloud setups.

By combining these steps, Fidelis Elevate® ensures comprehensive blindspot elimination, enabling organizations to maintain a secure and resilient posture against evolving cyber threats.

Why choose Fidelis Elevate® over other XDR solutions

Selecting the right XDR solution is crucial as it forms the backbone of your organization's security infrastructure. Fidelis Elevate® stands out by addressing both current and evolving security needs, offering several key advantages over other XDR solutions:

- **Threat detection and Response capabilities:** Fidelis Elevate® Detects threats across your network environment using machine learning, and advanced threat intelligence. It exposes blind spots, mitigates risk before it becomes a problem, and adjusts its response as threats evolve. Its customizable automated responses enable security teams to modify defenses instantly.
- **Integration and customization:** Fidelis XDR solution integrates with current vendors and security tools for smooth deployment. It has the ability to provide customized responses, filter out data and incident prioritization that may reduce the hassle of the security team.
- **Data centralization and visibility:** Fidelis security offers a centralized data center of XDR so that the SOC can have comprehensive network visibility of the data, and this will help security to detect and analyze reports with more accuracy.
- **Easy deployment:** Fidelis Elevate® is designed with an easy deployment option and user-friendly interface. The motive of implementing XDR should be providing strong infrastructure to the security team for navigating threats with more efficiency.

Conclusion

Blindspot Network is the silent enemies of your cybersecurity, lurking undetected until it's too late. Fidelis Elevate® (XDR) turns the tables by illuminating these hidden vulnerabilities and arming your defenses with cutting-edge tools like deception technology, centralized network visibility, and automated threat responses. It's more than just a security solution; it's a game-changer for organizations navigating complex IT landscapes. Fidelis Elevate® equips businesses with the tools they need to eliminate blind spots and defend against cyber threats, securing their digital future with confidence. If staying ahead of threats and protecting your assets is your goal, Fidelis Elevate® isn't just an option—it's the ally you need to outsmart attackers and secure your digital future.
Experience XDR in Action.
Get Your Personalized Demo Today!

- Deep Visibility
- Expert Forensics
- Resilient Defense

Get a Demo

Frequently Ask Questions

What makes Fidelis Elevate® (XDR) different from other security solutions?

Fidelis Elevate® stands out due to its integration of deception technology, centralized visibility,

and automated threat detection. It not only identifies threats in real-time but also misleads attackers, giving organizations the upper hand to remove blind spots proactively.

How does Fidelis Elevate® improve threat response times?

By leveraging advanced analytics, automation, and behavioral analysis, Fidelis Elevate® reduces detection and response times significantly. Its automated workflows and intelligent alerts empower teams to address threats before they escalate.

How do cybersecurity blind spots occur?

Security blind spots refer to those areas of an organization’s IT infrastructure that aren’t monitored or secured enough. They can result from misconfigured devices, unprotected endpoints and shadow IT (unauthorized systems or applications), but they most often occur when organizations are adopting new technology — such as IoT and hybrid cloud environments — without adequate controls.

Blind spots can also arise due to limited network visibility into how data is moved, the lack of integrated security tools, or the inability to track all assets comprehensively.

How to identify security gaps in a network?

In order to identify security gaps, you need to assess your IT environment. This includes:

- **Network Scan:** Map all connected devices and detect any unauthorized or unmonitored devices.
- **Vulnerability Assessments:** Conduct periodic scans identifying weaknesses (in configs, outdated software)
- **Log Analysis:** Analyze logs collected from endpoints, servers and networks to search for signs of abnormal behaviors/indicators
- **Penetration Testing:** Simulate cyberattacks to find weaknesses that can be exploited.
- **Centralized Overview:** Use XDR-type combinations to take a view of all activities on the network from a single point, which helps identify possible shortfalls.