FIDELIS XPS

FACE ADVANCED THREATS WITH CONFIDENCE

FIDELIS XPS™ SOLUTION OVERVIEW

Fidelis XPS™ is the only Comprehensive Advanced Threat Defense solution that stops advanced threats across all phases of the threat lifecycle. By focusing on real-time detection, prevention, and continuous response Fidelis XPS lowers enterprise risk, reduces remediation costs, and empowers you to stop advanced threat actors before they do irreparable harm.

Professional cybercriminals are so adept at cloaking their activities that they routinely go unnoticed for months, even years, without detection. They conduct detailed reconnaissance activities and develop custom tailored campaigns in an effort to penetrate your enterprise network to steal corporate sensitive data, intellectual property, business plans, and personal information.

Our decades-strong experience protecting the world's most sensitive networks has proven that full-spectrum network monitoring – not merely scanning for inbound malware – drastically improves an enterprise's ability to detect and thwart today's determined and well-equipped adversaries before they can achieve their objectives.

VISIBILITY AND CONTROL OVER ALL PHASES OF THE THREAT LIFECYCLE

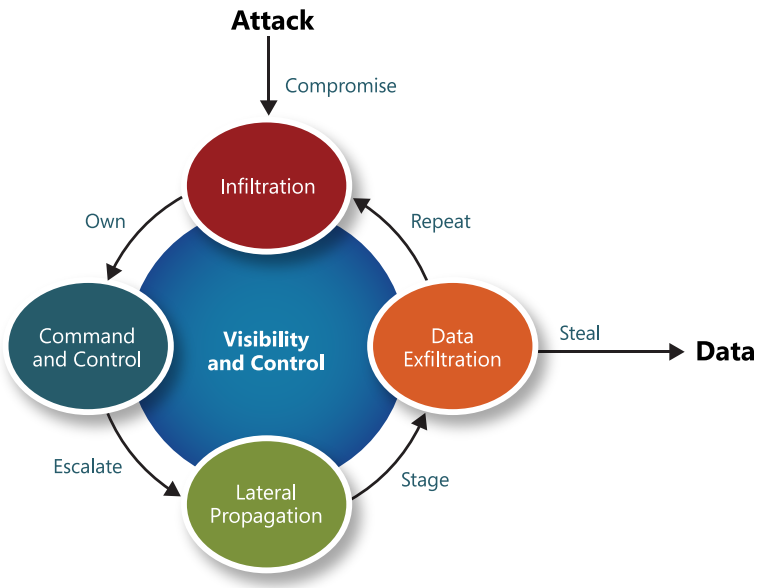
Advanced, targeted attacks are not instantaneous events; they are complex processes with multiple phases that occur over a period of time. The Fidelis XPS Comprehensive Advanced Threat Defense solution includes technologies and threat intelligence that enable the discovery, investigation, and containment of an attack across all phases of the threat lifecycle.

INFILTRATION PHASE: External threat actors need to get access to and gain control over one of your organization's computing assets, while malicious insiders already have authorized access to your computing and network resources.

COMMAND AND CONTROL COMMUNICATION PHASE: Once an adversary has compromised your assets, they will attempt to exercise complete remote control over your network.

LATERAL PROPAGATION PHASE: After successfully taking control, attackers find and infiltrate other connected assets inside your network looking for and staging sensitive, valuable, or classified information.

DATA THEFT/EXFILTRATION PHASE: Staged data is then obfuscated and sent out of the network by circumventing standard network security systems.



COMPREHENSIVE ADVANCED THREAT DEFENSE

To mitigate attacks across the threat lifecycle, Fidelis XPS provides Advanced Malware Protection, Data Theft Protection, and Network Security Analytics in a single, tightly integrated system for continuous protection and response across your enterprise.

Advanced Malware Protection

- Advanced Malware Detection
- Real-Time Threat Prevention
- Automated Threat Intelligence
- Flexible Policy (Rules) Engine
- Wire-Speed Performance

Data Theft Protection

- Data Exfiltration Prevention
- Intellectual Property Protection
- Complete Content Visibility
- Flexible Data Profiling
- Actionable Alerts

Network Security Analytics

- Full Metadata Capture
- Multi-Dimensional Analysis
- Advanced Visualization
- Customizable Reporting
- Correlated Alerting

By having these capabilities seamlessly integrated into a single system, under a unified management framework, you achieve a higher probability of detecting or preventing threats before they result in serious damage. Fidelis XPS also reduces incident response costs due to fewer incidents, faster containment and remediation, and lower post-incident legal and forensic expenses. In addition, enterprises can lower network security infrastructure costs as a result of having fewer boxes, minimal maintenance, and less analyst oversight.

FIDELIS XPS BENEFITS

- Mitigate enterprise risk through robust full-spectrum network visibility, control, and prevention.
- Reduce incident response costs with fewer occurrences and faster remediation.
- Diminish network security infrastructure costs through consolidation of the defense in depth stack.
- Lower operational cost with automated rules and real-time threat intelligence.
- Gain situational awareness and real-time prevention capability.
- Achieve higher detection rate across all phases of the threat lifecycle.

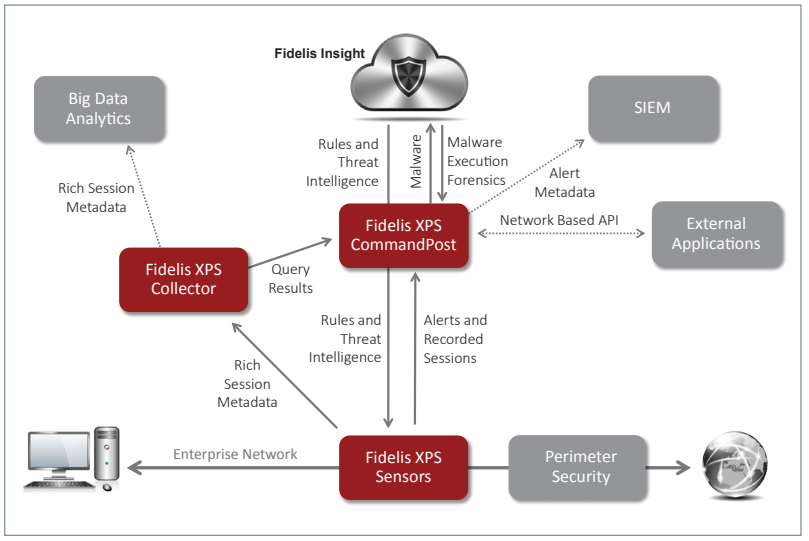
FIDELIS XPS SOLUTION

Fidelis XPS is an open and flexible platform designed for rapid deployment. Delivering proactive situational awareness with actionable threat intelligence, Fidelis XPS empowers analysts to focus on what matters by bringing important data to the forefront and allowing for the discovery, investigation, and containment of an attack across all phases of the threat lifecycle.

The Fidelis XPS Comprehensive Advanced Threat Defense solution is comprised of four major components.

FIDELIS INSIGHT: The cloud-based service providing a continuous stream of high-quality threat intelligence automatically consumed by the management system and operationalized by the sensors.

FIDELIS XPS COMMANDPOST: The management system and integration point between the Fidelis XPS solution and other systems in the enterprise network security infrastructure. The Fidelis XPS CommandPost is an intuitive, web-based graphical user interface for policy creation, alert management, sensor administration and configuration, and user/group administration.



FIDELIS XPS SENSORS: The workhorses tasked with reassembling, decoding, and analyzing traffic traversing the network boundary in real time using General Dynamics Fidelis' patented Deep Session Inspection® technology to detect and/or prevent advanced threats/attacks and data theft. Fidelis XPS sensors include an integrated Malware Detection Stack to identify and analyze thousands of objects per second (per sensor). The sensors also extract rich metadata from every network session that occurs on the network. Deployed in-line or out-of-band, the various sensors are designed for deployment at different points in the physical and logical network infrastructure.

Fidelis XPS Direct sensor sees and manages bi-directional traffic at ingress and egress points by monitoring and enforcing policy across all known and unknown network traffic, protocols, and applications.

Fidelis XPS Internal sensor monitors internal network traffic, providing an unprecedented level of visibility into, and control of, how information is used and misused across the enterprise.

Fidelis XPS Mail sensor monitors and enforces policy for email traffic, gracefully providing quarantine, sender notification, and redirection options.

FIDELIS XPS COLLECTOR: The Fidelis XPS Collector provides historical network memory by storing session metadata derived by Fidelis XPS sensors, enabling query and correlation of all sessions on the network, whether or not the session has been identified as threatening or malicious. This is done at a much lower total cost of ownership than full packet capture and provides a much richer index due to the deep protocol, application, and content decoding capabilities of the Fidelis XPS sensors.

HARDWARE SPECIFICATIONS

	CommandPost+	Direct/Internal (2500)*	Direct/Internal (1000, 500)*	Direct/Internal (250, 100, 50)*	Mail	Collector SA
Storage Capacity & Configuration	• Integrated 6Gbps hardware RAID • 1.6TB across 6x HDD in RAID-5	Mirrored 300GB HDD for application and data storage				• Integrated 6Gbps hardware RAID • 2.4TB across 6x HDD in RAID-5
CPU	2x 6 core 2.5Ghz Intel Xeon Processors	2x 8 core 2.9Ghz Intel Xeon Processors	2x 6 core 2.5Ghz Intel Xeon Processors	2x 6 core 2.1Ghz Intel Xeon Processors	2x 6 core 2.5Ghz Intel Xeon Processors	2x 8 core 2.9Ghz Intel Xeon Processors
Memory	48GB (ECC DDR3 1333Mhz)	64GB (ECC DDR3 1333Mhz)	48GB (ECC DDR3 1333Mhz)	32GB (ECC DDR3 1600Mhz)	48GB (ECC DDR3 1333Mhz)	64GB (ECC DDR3 1333Mhz)
Network Adapters	4x1Gb Ethernet ports (Copper)	• 4x10/100/1000 (Copper) • 2x10Gb-SR, Bypass Capable				4x1Gb Ethernet ports (Copper)
Out of Band Management	Integrated Management Module II (IMM2)					
Performance Power Supply	Dual hot-swap 550W/750W High Efficiency AC power supplies (80+ Platinum Certified)					
Form Factor	1U Rack-mount chassis					
Dimensions	Width: 440 mm (17.3 in)	Depth: 734 mm (28.9 in)		Height: 43 mm (1.7 in)		
Weight	15.6 Kg (35.5 lb)					
Operating Temperature	5°C to 40°C (41°F to 104°F)	Altitude: 0 to 915 m (3,000 ft)				

*Direct/Internal sensor performance ranges from 50Mbps to 2.5Gbps

VIRTUAL APPLIANCE MINIMUM REQUIREMENTS

The Fidelis XPS solution components are delivered as preconfigured purpose-built appliances. Some of these components are also available as virtual appliances, supported on VMware vSphere. Performance benchmarks have been performed on IBM x3550 M4 systems with Intel E5-2640 CPUs, DDR3 memory, Intel 1Gb NICs, and 10K SATA HDDs. Fidelis XPS virtual appliance performance is subject to the underlying hardware specifications and VM resource availability. For optimal system performance, a host system configuration with the following equivalent or better specifications is recommended.

	CommandPost VM	Direct 1000 VM	Internal 1000 VM	Mail VM	Collector SA VM
CPU	8 vCPU	8 vCPU	8 vCPU	8 vCPU	8 vCPU
Memory	32GB	32GB	32GB	32GB	32GB
Hard Disk	100GB	100GB	100GB	100GB	500GB
NICS	1 vNIC	4 vNIC	4 vNIC	1 vNIC	1 vNIC

CONTACT US TODAY TO LEARN MORE ABOUT FIDELIS XPS.

General Dynamics Fidelis Cybersecurity Solutions | 800.652.4020 | info@fidelissecurity.com