Fidelis Cybersecurity Overview

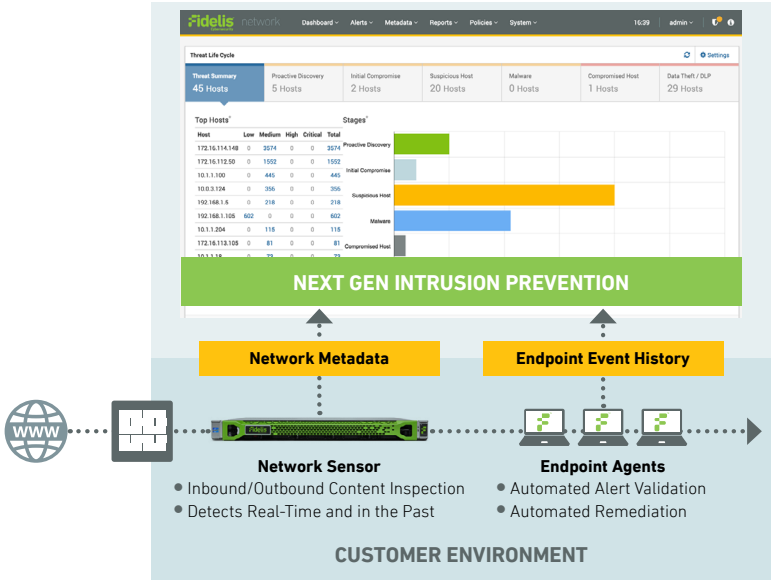
Next Generation Intrusion Prevention

The Challenge

Traditional intrusion prevention systems (IPS) were originally designed to identify attacks targeting known vulnerabilities. But the exploits attackers use have changed. Today they use unexpected pathways to target clients and distributed endpoints. While attackers innovate, the traditional IPS has stood still. It lives on largely unchanged in scope, generating low-value alerts for security teams while attackers slip past them in pursuit of high-value targets.

Fidelis Solution

Fidelis is the only next generation intrusion prevention solution that reassembles and analyzes network sessions — not just packets — in real time across all ports and protocols. Whether attackers are trying to gain a foothold in your network or accessing sensitive data on your laptops and servers, Fidelis detects it. Then, we tell you everything you need to find them and stop them in minutes, not days or weeks.



- **Detects Intrusions Your IPS Misses**
  Fidelis reassembles and analyzes sessions, not just packets. This lets us see attacks that slip by a traditional IPS.
- **Reduces Response Time**
  Automated alert enrichment and endpoint validation shrinks alert investigation from days to minutes.
- **Optimizes Your Security Stack**
  Unifies IPS, advanced malware protection, network forensics and DLP capabilities in one product.

STOP

PREVENT MORE

Detect at every stage of an intrusion
See modern threats, not just vulnerabilities
Detect intrusions in real time and in the past

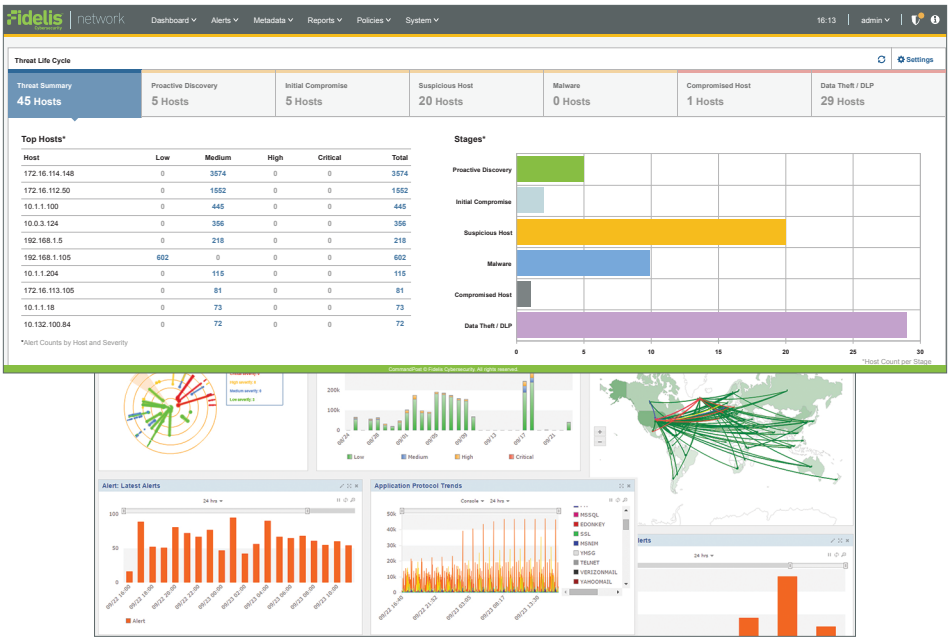
RESPOND FASTER

Automatically validate alerts on the endpoint
Automatically enrich alerts with integrated forensics
Automate response at the endpoint

Fidelis Network™

Fidelis Network stops modern threats. It solves the problem of alert fatigue and eliminates the investigative back-and-forth with IT teams that all too often consumes days or weeks.

Now, in minutes, Fidelis Network assembles all alert, content, execution, and behavior context — including endpoint information — in a single screen. Investigations do not need to wait on getting information from the endpoint and other teams. What used to take days or weeks now takes moments.



Capabilities

Sessions, Not Just Packets
Our session-based approach goes beyond packet-based signatures. We see the entire inbound and outbound communication stream, which allows us to detect attacks that slip by a packet-focused IPS.

Detect Intrusions a Traditional IPS Misses
In addition to advanced malware, exploits and command and control, Fidelis detects attacker behavior including lateral movement and the staging of data for exfiltration.

Automated Alert Enrichment
Integrated forensics with each alert shows what was happening before and after the alert and shrinks the time to detect, validate and triage alerts from days to minutes.

Detection in the Past and Present
New intelligence is automatically applied to rich metadata from your network and endpoints so you can detect attacks in the past and see additional context.

Gartner

"Fidelis also has the ability to have its appliances generate a rich flavor of metadata that is stored to allow for analysis that **enables effective near-real-time as well as historical incident investigation** capabilities. This integrated metadata storage and analysis capability is seen as **innovative in the IPS industry**."

~ Gartner Magic Quadrant for Intrusion Detection and Prevention Systems. 16 January, 2017

Fidelis Cloud
Managed by Fidelis

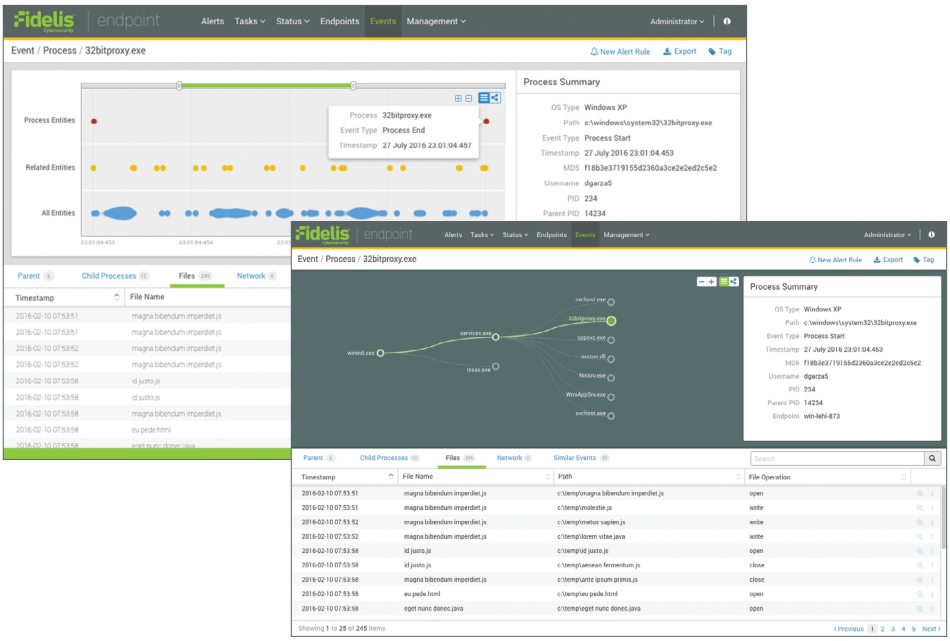
Get all the benefits of Fidelis Network and Fidelis Endpoint delivered from the cloud. With Fidelis Cloud, Fidelis maintains the infrastructure so you can focus on your core mission — protecting your organization.

- Infrastructure maintained by Fidelis so you can focus on security
- Rapid deployment and immediate implementation
- Scale up as you grow with as many software sensors as you need
- Uninterrupted service as you transition from a trial to production
- Simplified subscription pricing based on your bandwidth and storage needs

Fidelis Endpoint™

Fidelis Endpoint is an endpoint detection and response (EDR) solution that equips security organizations to confidently detect, respond to, and resolve security incidents in a fraction of the time it takes using traditional approaches.

Deep integration with Fidelis Network automates incident response activities that normally take days or weeks. Security analysts can perform tasks typically done by Tier II SOC analysts and incident response teams.



Capabilities

Detect Threats as They Happen
Continuously monitor and record key endpoint activity including file, process, network, registry, URL and DNS. Automatically apply new intel to all endpoints and get near-instant response.

Know What Happened Using Playback
Fully expose how an attack happened, what was taken and who else was involved with prioritized alerts and an automatically generated timeline for each suspected incident.

Automate Endpoint Remediation
Immediately halt data exfiltration and lateral movement by isolating endpoints, stopping processes, wiping files, running a script or using custom-scripted routines on the endpoints.

Automate Incident Response
Easily configure response workflows that automatically kick off remediation or deep analysis actions by defining trigger rules and actions with the alert response workflow engine.

Testimonial

"With Fidelis we are **60%** more efficient in identifying compromises. We reduced response-related costs by **17%** and are able to recover **50%** faster from incidents."

~ CISO, Financial Services Firm

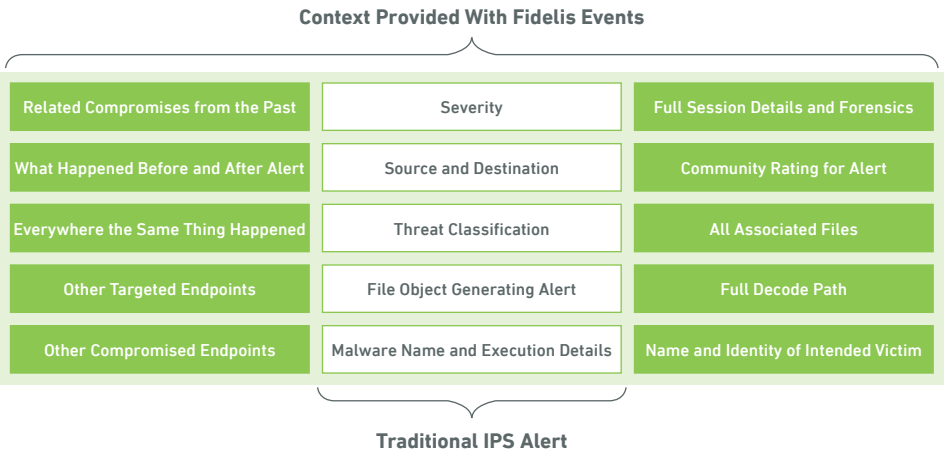
Fidelis Enterprise
On-Premise Deployment

Designed for organizations that prefer to deploy on-premise, Fidelis Enterprise offers you complete control over Fidelis Endpoint and Fidelis Network applications and appliances.

- You maintain and manage all appliances and software
- Fidelis professional services assists with deployment and training
- Available network senors include: Direct, Mail, Internal and Web
- Maintenance fees includes intel updates from Fidelis Threat Research Team
- License additional appliances, sensors as your needs grow

Alert Enrichment = Faster Response

Fidelis provides unmatched context with a 360-degree view of each alert that shows what happened before and after the alert triggered.



Fidelis vs. Traditional IPS Solutions

Fidelis uses a fundamentally different approach than a traditional IPS. This allows us to see exploits buried deep inside content that a packet-based IPS is blind to.

	Traditional IPS	Fidelis
Core Technology	Deep Packet Inspection	Deep Session Inspection®
Detection Focus	Exploits	Exploits, Threats **and** Data Theft
Attack Focus	Servers	Servers **and** Clients
Detection Timeframe	Real-Time	Real-Time **and** In the Past
Advanced Threat Detection	Sandbox	Rules, Sandbox and Analytics
Content Inspection	None	Inbound **and** Outbound
Alert Context	Limited	Rich **and** Actionable
Endpoint Response	Limited	Validation **and** Remediation

CASE STUDY

HEALTHCARE PROVIDER

Background

- 2,700 employees
- 10-person security team
- 10+ security solutions in place

Challenge

- Recent ransomware attacks prompted re-evaluation of security posture
- Existing IPS solution was a "noise generating machine"
- Advanced Malware Detection solution was missing threats.
- Investigating critical alerts took 3+ days on average

Results

- Can now detect exploits legacy IPS and malware solution missed
- Shrunk alert resolutions times by 15X
- Replaced IPS and advanced malware detection solution

See what you've been missing. Request a Demo Today **www.fidelissecurity.com/demo**

Contact Us Today to Learn More About Fidelis

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

We prevent intrusions. And we do it relentlessly. Whether attackers are trying to gain a foothold in your network or accessing sensitive data on your laptops and servers, Fidelis detects it. Then, we tell you everything you need to find them and stop them in minutes (not days or weeks). To learn more about our products and incident response services, visit www.fidelissecurity.com and follow us on Twitter @FidelisCyber.

