The Fidelis Platform Overview

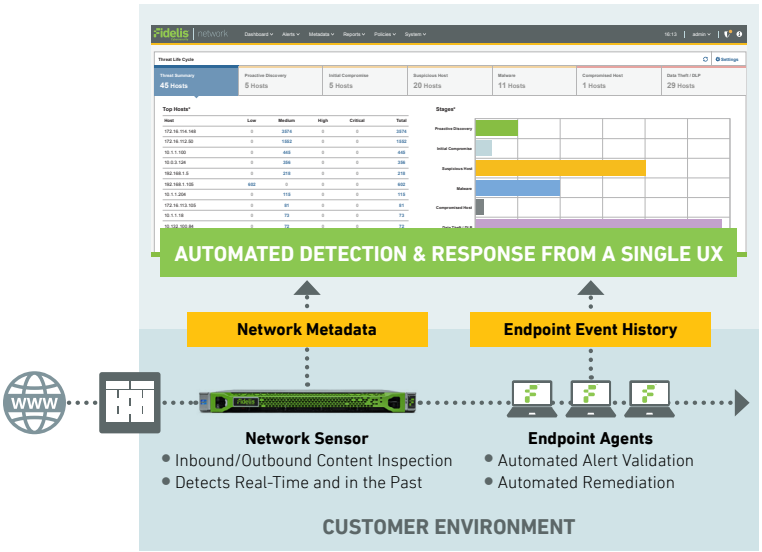
Automated Detection & Response

The Challenge

Modern attacks make it through the firewall and penetrate the perimeter. Security operations teams lack the complete, visibility-enhancing and automated technology to both see and respond to these kinds of modern and advanced compromises. Instead, they have patchwork systems strung together that create more work and complexity than solutions. We have changed all that.

Fidelis Solution

The Fidelis Platform is the first fully-automated and complete compromise detection and response system designed to improve security operations. Engineered to deliver comprehensive visibility, alert validation and increased response velocity across networks and endpoints with our unique real-time and historical compromise intelligence, Fidelis creates 10-20X improvement in the effectiveness and efficiency of security teams.



- **Completeness.** The Fidelis Platform is complete. Engineered for complete visibility across networks and endpoints, the Fidelis Platform delivers complete compromise intelligence, detection and response automation.
- **Visibility.** The Fidelis Platform is built upon a foundation of visibility that is both deep and wide. Fidelis is designed to deliver unique depth-of-field visibility that analyzes packets and sessions on the network as well as processes, memory and files on endpoint. Fidelis delivers both real-time and historical visibility that spans all ports and protocols and operating systems so that organizations can see what they've been missing.
- **Automation.** The Fidelis Platform is automated. By automating the actions and insight of a skilled analyst, hunter and incident responder, Fidelis delivers the power of experience at the speed of light.

AUTOMATED DETECTION

Our Universe of Detections — Engineered for Insight & Action

- **Automated & Integrated** static, dynamic & historical detection
- **Detection Triangulation** for precise attack intelligence
- **Multi-Factor Detection & Determination Includes** machine learning | atomic signatures | behavioral anomaly detection | threat intelligence applied against historical metadata | sandbox

AUTOMATED RESPONSE

Accelerate Security Ops Workflow Time & Effort

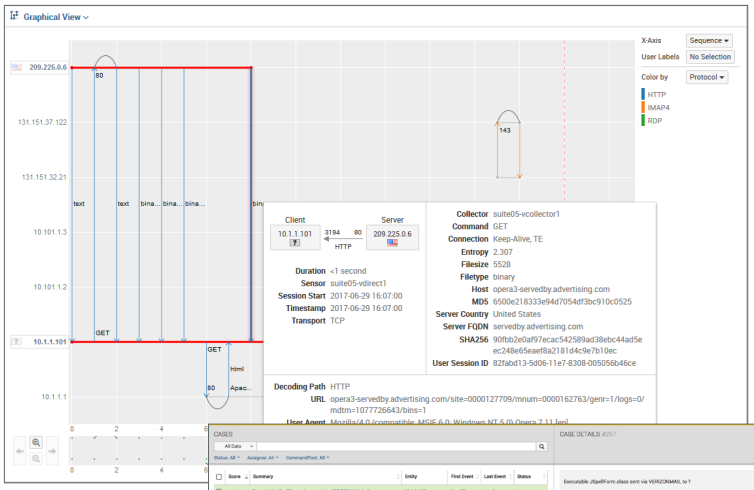
- Automate research, validation & response on advanced attacks
- Automate response workflows, isolation, expulsion & analysis
- Automate manual data manipulation tasks & achieve better security

Platform Pillar: Fidelis Network 9

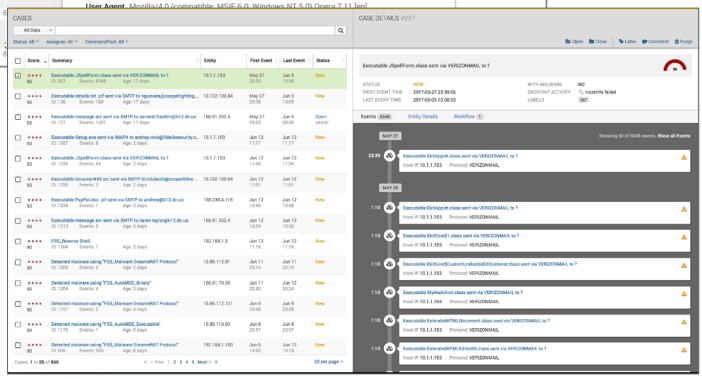
Fidelis Network™ stops modern threats that make it past the perimeter. It solves the problem of alert fatigue by automatically validating alerts and grouping related alerts together. Analysts respond with powerful guidance and automation.

Fidelis eliminates response and investigation back-and-forth with IT teams. With one-click investigations and built-in response automation from a single, comprehensive UX, even junior analysts have the power of experienced Incident Response pros.

Fidelis Network assembles the complete history of threats, compromises and intrusions. All alert data, content, execution, and behavior context — including endpoint information — is delivered to a single screen. Complete visibility mans the entire alert constellation is seen, through time and across dimensions. Conclusions are rapid. Responses are instant. Security is no longer dependent on other teams.



Fidelis assembles multi-dimensional attack data into a single, complete view. You see the constellation, not just points of data.



Fidelis assembles all related alerts into a central alert pane giving analysts rapid response ability.

Capabilities

We Detect What Others Miss Because We See What They Cannot

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

Sessions, Not Just Packets

Our session-plus-packet inspection goes beyond packet only based signatures. We see the entire inbound and outbound communication stream, including deeply buried content. We are the only security company to assemble and analyze network sessions in memory which grants unprecedented visibility, detection and determination.

Automated Alert Enrichment

Fidelis automates the collection, correlation and integration of forensics with each alert to show what was happening before and after the alert. Fidelis shrinks the time to detect, validate and triage alerts from days to minutes.

Detection in the Past and Present

New threat intelligence, signatures and rules are automatically applied to stored network and endpoint metadata so you can detect attacks that happened in the past and prepare for the future.

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.

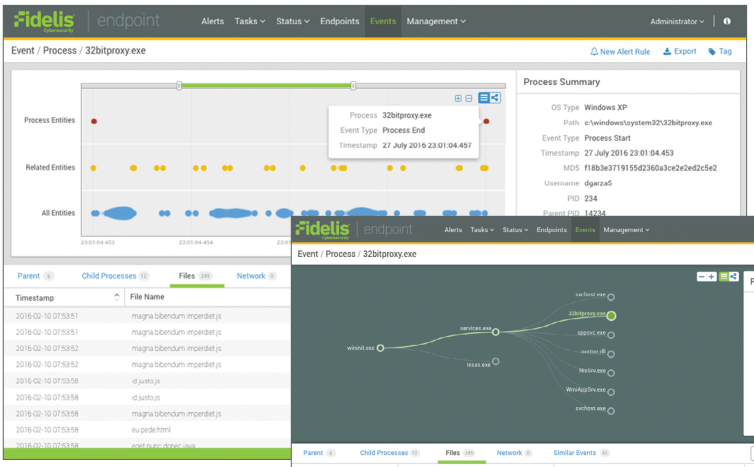
- Infrastructure maintained by Fidelis so you can focus on security
- Rapid deployment and immediate implementation
- Scale up as you grow with as many software sensors as you need
- Uninterrupted service as you transition from a trial to production
- Simplified subscription pricing based on your bandwidth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

Platform Pillar: Fidelis Endpoint 9

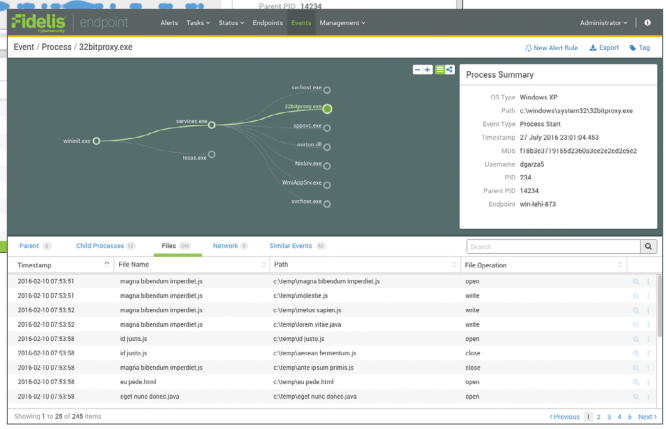
Fidelis Endpoint™ is our combined endpoint detection and response (EDR) and endpoint protection (EPP) solution that equips security organizations to confidently prevent, detect, respond to, and resolve security incidents in a fraction of the time it takes using traditional approaches.

Purpose-built to work hand-in-hand with Fidelis Network, Endpoint 9 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.



Interactive attack timeline lets you pinpoint stages and machines for response.



Interactive visualizations of process trees & attack pathways.

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.

Customer Quote

"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-Premises 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 intelligence updates from Fidelis Threat Research Team
- License additional appliances, sensors as your needs grow

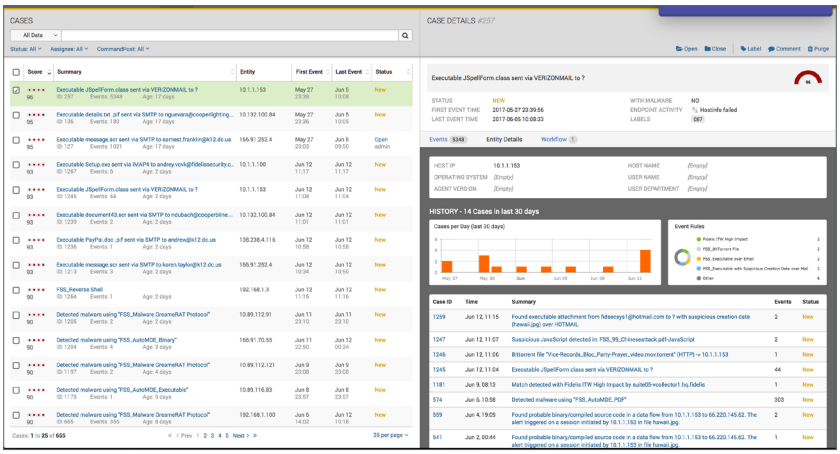
Move From Alerts to Action

Fidelis automates the work of an experienced security professional. With automated alert validation, investigation, correlation and aggregated display, even junior analysts are equipped to make quick decisions and execute rapid responses.

The key questions answered are:

- Did the attack reach the target?
- Was the attack activated?
- What else happened prior to and after the attack?
- Did this activity occur on any other system in my environment?

Fidelis 9.0 automatically delivers the answers. Fidelis runs validations against every endpoint in the environment. Results provide critical information that accelerate analyst's understanding of the trajectory and scope of the attack.



Fidelis automates the collection, correlation and analytics of complex attacks across network and endpoint and through time.

CASE STUDY

HEALTHCARE PROVIDER

Background

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

Challenge

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

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

Fidelis is the industry's only completely integrated, automated network and endpoint detection and response platform. Fidelis improves the efficiency and effectiveness of security operations teams by 10-20X by condensing alert data into actionable threat summaries and then automating response and investigation actions instead of piling more alert data on already fatigued security staff. With automatic validation, investigation and prevention of attacks, Fidelis is engineered for visibility, designed for response and trusted by the most important brands in the world. See what you've been missing.

