Fidelis Cybersecurity

SOLUTION BRIEF

Stop Ransomware

Thwart Attackers with Deception and Fast, Automated Detection and Response

Ransomware is the fastest-growing form of cybercrime. In a Ransomware attack, cybercriminals hold your data for ransom, demanding payment, with a threat to either publish or perpetually block access. These malicious and costly attacks cause downtime, data loss and IP theft, business disruption, and they harm your business's reputation. After successfully executing a ransomware attack on your organization, the attacker has a map of your entire system and network and often leaves behind a backdoor to enable them to regain access in the future and extract another ransom.

1 in 3
attacks are Enterprise ransomware
Cybersecurity Ventures

Every 2 seconds
Ransomware is expected to attack a business, consumer or device by 2031
(up from every 11 seconds in 2021)
Cybersecurity Ventures

$8,500
lost/hour due to ransomware-induced downtime
Purplesec

$265 Billion
Estimated cost of ransomware incidents by 2031
Cybersecurity Ventures

80%
of those that pay ransom are victims of another attack
ZDnet

Don't Let Ransomware Lock You Down

Ransomware gets in and goes after everything. With preparation and the right platform in place, you can take proactive steps to re-shape the attack surface so you can detect, hunt, and respond to ransomware, and improve your chances of locking down the threat before it locks you out of your valuable data. Find and engage earlier using deception technologies such a traps and decoys to lure and confuse attackers so you can detect and stop adversaries before they stop your business.

Know What You're Defending

By creating a map of your cyber terrain, from the data center to the cloud and out to your endpoints, you can keep track of critical data sets, workflows, avenues of attack, and high-risk assets across all your environments.

Stay Ahead of Known Vulnerabilities

Diligence in applying updates and patches, particularly for your high-risk assets and for systems that support work-at-home users, protects and defends those assets that are most critical to your business operations.

Improve Security Posture with Network Segmentation

Building firebreaks into your architecture isolates critical infrastructure systems and services and helps contain attacks by making it harder for ransomware attackers to penetrate critical systems.

Enforce Identity and Access Management Best Practices

Enforcing good account and password management, including complex passwords and two-factor authentication, helps reduce the likelihood of an identity-related breach.

Enable Robust Endpoint Protection

Keeping endpoints up to date with the latest software updates, patches, and anti-virus software improves your ability to catch signature-based threats. Endpoint Detection and Response (EDR) capabilities enable your security operations team to identify more stealthy attacks, quarantine compromised systems, provide remote diagnosis, and return endpoint devices to a secure state faster.

Improve Email Security and User Best Practices

Phishing attacks continue to be a go-to technique for Ransomware gangs to gain access into your environment. Bolster e-mail security and provide user training to help your organization detect and block phishing attacks.

Fidelis Reshapes the Attack Surface

Fidelis integrates deception technologies and unified cloud security with traditional detection and response capabilities for Endpoint (EDR) and Network (NDR) to help SOC teams proactively find, deceive, and neutralize advanced cyber threats, including ransomware. With the Fidelis Elevate® and Fidelis CloudPassage Halo® platforms, your organization can engage ransomware adversaries earlier in the attack lifecycle and quickly identify and block potential breach points or areas of exposure across all threat vectors. As a result, your defense posture becomes a proactive threat hunting engagement using analytics, automation, and real-time alerting on security events for endpoints, networks, clouds, servers, and containers.

Gain Full Situational Awareness

Fidelis Cybersecurity provides comprehensive visibility across all your assets — endpoints, networks, clouds, servers, containers and in email — even in rapidly changing cloud environments. It can also stop email borne threats by adding a layer of security that inspects content buried deeply within email messages and attachments. You will eliminate blind spots and prepare your SOC team for battle against ransomware attackers with full situational awareness of active events as they occur.

Lock Down Your Assets

Fidelis delivers detection and response to advanced threats at line speed by operating inside the adversary's decision cycle. You'll make faster, more informed decisions with comprehensive detection data that is actively validated between the endpoint and network. Then, you can automatically quarantine potentially compromised resources and erect preventative measures so that compromised systems don't become gateways to your high-value data and workloads.

Counter with Intelligence

Fidelis continually gathers intelligence to help you better prepare for future attacks. Automatically use threat intelligence to help identify previously undiscovered compromises, and to better understand attack origins, and how adversaries perpetuate across your environment. Armed with data and Fidelis Deception® technologies, you can lure and distract adversaries with decoys, traps, and breadcrumbs; identify and track their presence within your enterprise; and stop them from discovering and compromising your high-value, ransom-worthy assets.

Enforce Security Best Practices

Fidelis automatically detects new and updated configurations of servers, networks, cloud accounts, and other assets that represent potential exploitation points. By monitoring for configuration compliance and known vulnerabilities, Fidelis can alert system owners to issues in real-time and integrate and track remediation efforts as part of the team's natural workflows.

Achieve a Proactive Cyber Defense

Create decoys and traps to lure attackers toward the decoy systems and away from IT assets. That — plus robust threat intelligence, including threat- and behavior-based analytics, configuration security monitoring, file integrity monitoring, and log-based intrusion detection — fuels faster intervention. And with Fidelis automation, system owners are alerted to indications of compromise (IoCs) as they happen, which helps accurately detect and neutralize attacks earlier in their lifecycle.

Prevent Data Leakage and Loss

Fidelis combines threat detection, asset discovery, and deception to prevent the data exfiltration that typically occurs with ransomware attacks. The Fidelis Elevate platform includes powerful data loss protection and anti-malware engines, providing protection and detection against internal and external threats so you can detect and disrupt malicious attacks before they can steal your data, disrupt operations, or extort your business.

End-to-end Ransomware Protection

Fidelis Endpoint®

Unmatched detections, investigations, forensics, and response, on and off the network, detect stealthy attacks, speed investigations, and automate response.

Fidelis Network®

Detect and respond faster to ransomware anywhere on the network by eliminating blind spots and gaining visibility into all network and email traffic – including encrypted traffic.

Fidelis Deception®

Reshape the attack surface and lure, detect, and defend earlier in the attack lifecycle with automatic, realistic deception layers based on accurate discovery profiles.

Fidelis CloudPassage Halo®

Automate cloud security controls, compliance, and vulnerability management across servers, containers, and IaaS in any public, private, hybrid, and multi-cloud environment.

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity

Fidelis Cybersecurity, the industry innovator in proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via rich, dynamic cyber terrain mapping and multi-faceted context and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. With Fidelis, organizations emerge stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide. For more information, please visit www.fidelissecurity.com