Cybersecurity for Government Agencies: The Best Defense is an Impenetrable Offense

New threats target global governments every single day. To improve cybersecurity for government agencies, updated digital strategies include best practices and solutions delivered through the Federal Systems Integrator (FSI) community. But an FSI needs the right tools to deliver the impenetrable office that government organizations needs to safeguard the public sector, private sector, and the American people's security and privacy.

The US Federal government recently issued an Executive Order on Improving the Nation's Cybersecurity. Agencies must follow the mandate that is heavily focused on the prevention, detection, assessment, and remediation of cyber incidents. However, when it comes to cybersecurity, government agencies—like private industry organizations—struggle with an ongoing cyber workforce shortage.

According to NIST, the global cybersecurity workforce shortage is estimated to be 3.12 Million in 2021. To automate cybersecurity and make up for the skill shortage, System Integrators, including Microsoft, Verizon, and AT&T, are now employing Enterprise-IT-as-a-Service or Cybersecurity-as-a-Service programs for government agencies. They rely on best-in-class tools that can stand up to the threats that government agencies face daily.

Leading the Way with Proactive Cyber Defense

Fidelis Security® is a leading provider of threat detection, hunting, and response solutions. At RSA 2021, Fidelis Elevate® brought home the Global InfoSec Award, "Best Product in XDR," awarded by Cyber Defense Magazine.

"We scoured the globe looking for cybersecurity innovators that could make a huge difference and potentially help turn the tide against the exponential growth in cybercrime. Fidelis Security is absolutely worthy of this coveted award and consideration for deployment in your environment."

Gary S. Miliefsky, Publisher of Cyber Defense Magazine

Fidelis Elevate is an open, extensible platform that is purpose-built for proactive cyber defense. It enables SOC analysts to engage adversaries earlier in the attack lifecycle, reshape the attack surface, and take control of enterprise security to proactively stop threats before they impact business.

Stop Cyber Threats with Fidelis

Talk to Expert

Fidelis Elevate unifies deception technologies with detection and response across endpoint detection and response (EDR), network detection and response (NDR), and cloud. This combination allows agencies to detect and trace an attacker's movement, understand what systems they have compromised, stop their advances, and restore the impacted system to normal operations as quickly as possible.

We aim to be a valuable partner for more FSIs by delivering unmatched data protection, threat

detection, intelligence, and incident response solutions.

With a deep bench of subject matter expertise developed and homed in on Government, Defense, and Intelligence environments, Fidelis has intimate knowledge of the unique challenges face by government cybersecurity teams.

Critical Components in Cybersecurity for Government Agencies

Fidelis Security offers decryption, digital forensics, network traffic analysis, and full visibility across hybrid environments with deep, dynamic asset discovery, 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. Below are some of the capabilities we use to deliver the decisive advantage to our government customers, including:

- Proactive capabilities with Fidelis Network and TLS Decryption that provide continuous, real-time visibility into traffic moving across your network. This allows you to detect signs of intrusion and respond before they do damage to your agency.
- Deceptive countermeasures with Fidelis Deception to take back your advantage and cause adversaries to waste time and money in their attempts. Fidelis Deception does this by altering the cyber terrain with hundreds or thousands of realistic decoys and breadcrumbs to lure and trap adversaries at the deception layer.
- Proactive data loss prevention, with patented Deep Session Inspection® that finds indicators of data exfiltration nested deep within files and emails.
- Reactive capabilities to include automated detections, threat hunting, and automating investigations and response actions before data is stolen.
- Predictive capabilities by machine learning and artificial intelligence to detect anomalies, determine the probability of compromise, and assist in metadata analysis when searching for known and unknown threats.
- Retrospective countermeasures that analyze threat intelligence and provide increased visibility and awareness to thwart future attacks.

Fidelis Security provides the roadmap for cybersecurity for government agencies with continuous, real-time visibility across the environment and automation to accelerate security operations, threat detection, and response. FSIs pave the way in arming the government community with the cybersecurity tools they need to protect against their most advanced threats, and we believe Fidelis is a critical component in their cybersecurity arsenal.