FCW | Threat Protection

Moving to a holistic cybersecurity fabric

How Fortinet's ATP approach can support federal networks

Federal IT systems are under constant attack. The U.S. Office of Management and Budget reported more than 28,500 cybersecurity incidents in FY 2019. It's not just the rising number of incursions that worry federal technology leaders, though. The greater concern is that attackers are becoming ever more sophisticated.

"There are new threats emerging all the time," said Syed Masood, a senior federal systems engineer at Fortinet. "Government agencies don't know where the next attack will originate. Is it going to be web-based? Is it going to be email based? Will it be insider threat, or something in the cloud?"

SPONSORED BY: FORTINET

NEW THREATS CONSTANTLY EMERGING

The bad actors themselves are changing, too. Defenders can no longer assume that nation-states alone represent the greatest peril. New players, including an expanding criminal element, add to the fluidity of the threat landscape.

At the same time, the nature of the attack surface is shifting in a way that could potentially open up new vulnerabilities. "The dynamic nature of communications in the workplace is making this more complicated," said Phil Moser, federal sales director at Fortinet. With the rise of work-from-home and the proliferation of Internet of Things (IoT) endpoints, "you have a very diverse work environment and an ever-expanding networking environment as well. Sophisticated attackers can leverage that to their advantage."

"You have a very diverse work environment and an ever-expanding networking environment as well. Sophisticated attackers can leverage that to their advantage."

The highly-publicized SolarWinds attack starkly illustrated evolving cybersecurity threats. In that exploit, attackers breached the supply chain of trusted software providers to infiltrate a range of federal systems. The success of that attack demonstrated to federal IT leaders that a more robust level of cyber resilience is needed to address the high degree of sophistication in some emerging threats.

This highly dynamic situation represents a new kind of threat landscape for those who secure federal systems. Government as a whole recognizes the threat as well. The proposed 2021 federal budget includes $18.7 billion for cyber defenses. However, money alone won't fix the problem, and neither does a single technology, according to Masood.

"There is no single solution out there that can claim to have a silver bullet," Masood said. Rather, federal agencies need a new approach to cybersecurity, one that incorporates a range of defenses. They need Advanced Threat Protection – a tightly-knit collection of resources that together provide a security fabric, a holistic ecosystem of interlocking defenses with a common platform that stretches from the end point to the cloud.

Such Advanced Threat Protection, or ATP, is a necessary response to today's heightened cyber risk environment. At a time when threat vectors are constantly shifting, "ATP solutions look for unknown behavior, unknown threats, undisclosed threats," Masood said. Through AI and automation, ATP enables interoperable systems to act quickly and in concert to head off even previously unrecognized threats.

PRESENT-DAY GAPS

While federal agencies have implemented vigorous cyber defenses in recent years, many of these deployments still come up short in a number of key ways.

In the absence of a "silver bullet" solution, most agencies have taken a widely heterogeneous approach to securing their IT operations. "They are throwing multiple solutions at the problem, without understanding how the different pieces should all come together," Moser said. "They keep piling on one solution after another, with minimal integration."

This is a problem for a number of reasons. First, a piecemeal approach is not wholly effective in addressing today's sophisticated threats. Without an integrated cyber infrastructure, IT systems may be vulnerable to a breach in gaps between solutions. At the same time, federal acquisitions processes make it difficult to keep these systems current. By building disaggregated components, agencies may lose the ability to readily access the latest and best protections.

Additionally, piecemeal systems require constant care and feeding, with skilled IT talent frequently bogged down in the routine work of patching and updating. It is labor intensive and time consuming. In addition, the fragmented approach may bump up against the skills gap, creating the need for a wider range of IT talent than is readily available in today's marketplace.

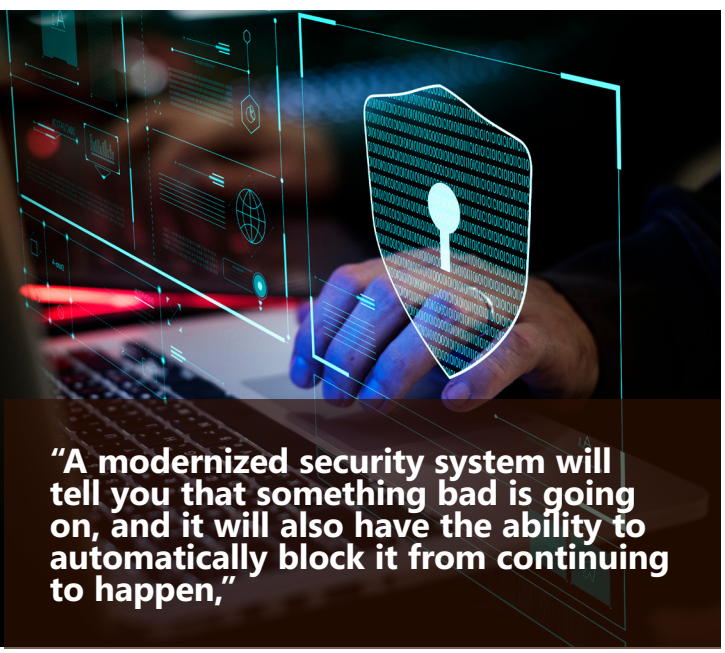
As a result, end users too often become the front line of defense. "If you're a federal employee, you're expected to choose the vigilant security action all the time, and that's an unrealistic expectation," said Masood. Agencies emphasize security awareness – telling people not to click on suspect links, for instance. If the email security system itself is not effective and lets those malicious emails through in the first place, perhaps it isn't realistic to put the burden of defense on the end user.

Federal agencies need a new approach to cybersecurity, a holistic, dynamic, and proactive architecture that can identify and address potential threats in real time. IT leaders require a suite of interoperable capabilities that address suspect actions across the entirety of the network — ATP tools that can act very quickly to deliver actionable intelligence in order to mitigate any emerging vulnerability.

"A modernized security system will tell you that something bad is going on, and it will also have the ability to automatically block it from continuing to happen," Masood said.

A "SECURITY FABRIC" APPROACH

To meet today's cybersecurity challenge, federal agencies need to take an architectural approach to their defenses. An increasingly dynamic, virtualized, and cloud-driven environment demands a security capability that extends seamlessly across on-prem, public and private cloud environments. In short, agencies require a "security fabric."



"A modernized security system will tell you that something bad is going on, and it will also have the ability to automatically block it from continuing to happen,"

Supported by multiple components, the security fabric concept is rooted in the next-generation firewall. On top of this sophisticated protection, the fabric weaves together multiple additional defenses, integrating the components and laying on intelligent automation.

"Having a multidimensional approach is key," Masood said. "You need to understand where your assets are and what assets you must defend and protect. You have to look at your organization from a user's laptop all the way to the cloud, and everything in between."

The security fabric encompasses all the elements of networking and network security, all the software and software security, as well as remote users and wireless

components. It's about putting in place security solutions at every level of the organization to address email threats, web threats, file-based attack threats and fileless attack threats.

"To do all this, you have to have visibility. You need tools that provide insight and response at all of these junctures within the environment," Moser said. "These tools can take action when they see something abnormal or malicious. They can automatically detect and mitigate those threats."

This integrated and automated approach to security helps federal agencies to make the most of their existing IT expertise. Interoperability and a shared platform help to reduce the manual requirements, freeing skilled professionals to focus on higher-level activities. More to the point, the security fabric is more adept at catching and remediating threats, stopping 99.8 % of attacks, according to third-party analysis by ICSA Labs.

The security fabric encompasses all the elements of networking and network security, all the software and software security, as well as remote users and wireless components.

At a high-level, the security fabric delivers protection across the entire network. "Security-driven networking means that security is always going to be front and center of everything in your environment," Masood said.

"If you're going to use your laptop, for example, you'll be protected with endpoint detection and response," he said. "If you're a remote user using remote access VPN, that network connection is going to be secure. There's a next-gen firewall in your data center. You're doing internal segmentation so that a breach cannot migrate from one segment of the network to another." Applications in the cloud are protected as well, with security built into the web application firewall.

The differentiator here lies in the integration of all these security capabilities. "The security fabric brings all those things together into a security-driven network," Moser said. "The power lies in the convergence."

A number of other key elements serve to differentiate Fortinet's ATP approach to creating a security fabric:

Research: As Fortinet's threat intelligence and research organization, FortiGuard Labs is comprised of experienced threat hunters, researchers, analysts, engineers, and data scientists who together provide customers with cutting-edge threat intelligence.

FortiGuard Labs' threat intelligence efforts keep Fortinet security products armed with the best threat identification and protection information available. FortiGuard Security Subscriptions enable users to tailor security to their specific environments, while FortiGuard Labs Consulting helps them to better understand the threats and identify gaps in their security infrastructure, while also ensuring their people have the skill sets they need.

AI & ML: Fortinet makes practical, real-world use of machine learning and artificial intelligence. From inline security controls, to centralized advanced threat detection and response in the SOC, AI-driven analytics help security teams keep pace with an accelerating threat landscape.

Machine learning is built directly into the Web Application Firewall and Endpoint Protection Platform to provide behavioral based prevention in complement to traditional techniques. Combining distributed sensors with centralized big data analytics, Fortinet enables organizations to apply machine learning, artificial neural

networks and other analytics in order to effectively detect the cyber threats.

Multidimensional capability: Fortinet offers workload protection across a multidimensional network environment. Its solutions extend security across remote, on-prem, and public-private cloud environments, ensuring organizations have robust protection across all elements of today's increasingly dynamic, virtualized, and cloud-driven environment.

In addition, Fortinet's solutions are designed to seamlessly integrate with a wide range of third-party tools and platforms. This ensures security is extended across even the most complex and heterogenous IT ecosystems.

A DEEPER DIVE INTO SECURITY

To understand the power of this approach, it's worth taking a deeper dive into the components that together comprise an ATP deployment:

Next-gen firewall (NGFW) – The basis for these wide-ranging protections is the next-gen firewall – in Fortinet's case, it's called FortiGate. Powered by purpose-built security processing units, these next-gen firewalls enable security-driven networking, and are ideal network firewalls for hybrid and hyperscale data centers. With multiple high-speed interfaces, high-port density, and high-throughput, they can be deployed at the enterprise edge, hybrid data center core, and across internal segments.

"If you have encrypted traffic coming in, you cannot really take action on it. The next-gen firewall can decrypt it, understand what's in the payload, and then determine if it's normal or malicious," Masood said. "If it is malicious or even suspicious, the firewall will block it."

Fortinet's next-gen firewall offering takes these protections further still using a purpose-built chip that contains a Security Processing

The ATP Advantage

This sophisticated "security fabric" approach supports the Advanced Threat Protection capabilities federal agencies need to effectively counter today's emerging cyber risks.

- **What it is:** ATP in general describes a category of security solutions that defend against the most sophisticated hacking efforts and malware intrusions. This approach is tailored to address the highly stealthy nature of advanced malware, Trojans, ransomware, and other cutting-edge attack forms.

- **How it works:** ATP addresses the need to protect against a never-before-seen level of complexity and sophistication among the bad actors' efforts. ATP solutions identify potential advanced threats before they impact critical systems, with rapid detection and automated response helping to minimize the damage of a potential attack.

- **Why it matters:** "ATP is a data protection strategy that focuses on actively studying and monitoring the networks, servers, and access mechanisms around sensitive information," according to the Identity Management Institute. "Most importantly, ATP sets up systems that enable automated software to react almost instantly to a threat with the support of security specialists."

Unit (SPU). Purpose-built processors deliver unmatched performance for network functions, ensuring that security devices never become a performance bottleneck within the IT architecture. When volume is heavy, the SPU delivers a persistent high level of security without the risk of dropped sessions or network performance issues.

Email security – Another key component of Fortinet's ATP offering is the email security gateway FortiMail. This mail security solution examines incoming emails and will block all suspect communications. It will halt spam in its tracks and will also detect and stop malicious messages that disguise themselves as internal communications.

"Email remains one of the foremost attack vectors," Masood said. "Agencies need a tool that will not only block these messages, but will also inform the other components of the solution. This is where the security fabric comes into play. FortiMail works hand in hand with FortiProxy, a tool that examines all the web traffic and defends against web attacks with URL filtering, advanced threat defense, and malware protection."

By working in close consort, these and other elements of the ATP deployment can block attempted intrusions and can also set up further defenses to ensure suspect activity does not propagate throughout the network.

Sandboxing – Fortinet's ATP also incorporates a sandboxing component, FortiSandbox. It provides industry-leading capabilities to stop and sequester threats the moment they are detected by network sensors, using Fortinet's patented anti-malware technology. Additionally, as part of the security fabric, FortiSandbox deploys indicators of compromise (IOCs) to other network sensors when it learns about new malware.

"If there's an attachment or a download from a suspicious IP address or a domain, we'll send that to the sandbox for analysis," Masood said. "The sandbox itself is constantly getting updates from FortiGuard Labs, our threat intelligence and research organization, and we also partner with third-parties that provide key intelligence, so it is a very comprehensive protection."

Artificial intelligence – The sandbox, in turn, works hand in glove with FortiAI, an artificial intelligence cyber capability. This "Virtual Security Analyst" provides IT teams with a sophisticated threat detection capability: It can quickly correlate an unknown threat and can take immediate action to block a threat from spreading.

Email remains one of the foremost attack vectors. Agencies need a tool that will not only block these messages, but will also inform the other components of the solution.

The FortiAI Virtual Security Analyst is the industry's first product to embed independent, self-learning AI on-premises to mimic the information security analyst's job function. To accelerate threat intelligence to machine speed, FortiAI learns and adapts to new attacks targeting a specific organization over time, continually improving and optimizing the threat protection life cycle.

"FortiAI supports security operations staff by identifying and analyzing fileless and file-based malware. It identifies compromised systems across the organization with near 100 percent certainty, in milliseconds," Moser said.

Driven by artificial intelligence, IT teams can deliver faster mitigation of attacks, with reduced organizational impact. Real-time response minimizes damage and shrinks the time window for exposure to threats. Security professionals also see improved productivity, with the virtual elimination of false positives.

"It basically acts like a cyber security professional," Masood said. "You can rely on the AI to do the work of an analyst, with the ability to notice anomalous behavior and to react in real time."

Endpoint protection – Another piece of the ATP infrastructure, an endpoint protection component, defends endpoints against signature-based and fileless attack. Fortinet's endpoint offering is based on unique code-placing technology: It works at the kernel level, at the operating system level, to detect and block suspect activity.

The endpoint protection component delivers pre-execution and post-execution security policies. "Let's say there was a bad file, or a file that starts executing and ends up encrypting a file and then attaching it to emails," Masood said. "Endpoint detection blocks all of that and prevents that from executing." This technology is especially effective against Ransomware as well.

Network access control – In keeping with the vision of a security-driven network, Fortinet's approach to ATP also includes FortiNAC, a network access control capability.

As the Fortinet network access control solution, FortiNAC supports a zero-trust approach to security. It enhances the overall security fabric with visibility, control, and automated response for everything that connects to the network. Network access control provides protection against IoT threats, and orchestrates automatic responses to a wide range of networking events. It also extends control to a wide range of third-party devices, with seamless integration across all the most popular IT platforms.

The FortiNAC solution protects both wireless and wired networks with a centralized architecture that enables distributed deployments with automated responsiveness. It delivers network visibility to see every device and user as they join the network; network control to limit where devices can go on the network; and automated response to speed reaction time to events from days to seconds.

Using FortiNAC, organizations can deliver agent and agentless scanning of the network for detection and classification of devices. They can create an inventory of all devices on the network and assess the risk of every endpoint connected to the network. They can use a centralized architecture for easy deployment and management, and can leverage extensive support for third-party network devices to ensure overall effectiveness.

AN INTEGRATED SOLUTION

Advanced Threat Protection requires a multiplicity of moving parts. There's the firewall and the email filter, the sandbox and the network access protections. A wide variety of vendors offer some or all of these capabilities. In fact, the sheer breadth of these offerings has been a complicating factor for some federal cyber efforts.

Fortinet differentiates itself by the integrated manner in which it delivers these multiple, powerful capabilities This is where the concept of the security fabric comes into play. With FortiOS, Fortinet delivers a common operating platform for its ATP components. More than just a single pane of glass, the shared operating system delivers:

- **Security-Driven Networking** that secures and accelerates the network and user experience.
- **Zero-Trust Access** that identifies and secures users and devices both on and off network.
- **Adaptive Cloud Security** that secures and controls cloud infrastructure and applications.
- **Artificial Intelligence (AI)-driven Security Operations** that automatically prevents, detects, and responds to cyber threats.

"Our products are integrated into a common operating system, which in turn has a direct impact on the speed with which you can detect and respond to threats," Moser said. There's seamless communication between the different parts, all of which are designed to work together. "The ATP components are all part of the security fabric, with every component is talking to every other component, each one benefiting from the others' threat detection capabilities."

Having a common platform also eases the burden on IT staff tasked with maintain a vigorous cyber posture. "It means that if you are trained on one of the components, it's very easy for you to be able to understand what the other components are doing," Masood said.

Having a common platform also frees up IT talent. Skilled professionals get to spend less time on the care and feeding of their cyber defenses. They can devote their efforts to doing higher-level work around security, as opposed to just putting out fires.

NEXT STEPS

Many federal IT professionals will readily understand the value proposition inherent in an integrated, "fabric" approach to cybersecurity in support of Advanced Threat Protection. Those who want to follow this road can ask themselves a number of key questions in order to help build the business case for an investment in a more comprehensive security solution.

"They need to ask themselves whether they have protection in place for all their assets," Masood said. "And they can consider issues of visibility and timeliness. If you detect a threat on your email security server, does that knowledge benefit your other protections? Does it help to automatically put a block on the next-gen firewall? Does it trigger an automatic block or filter on my web security gateway?"

Agencies need sufficient visibility to answer these kinds of questions, with integration to ensure a high level of transparency across the information landscape. They also need integration in support of automated response mechanisms. Simply put: that endpoint threat likely didn't stop at the end point, and reaction time will be key to mitigating risk. Timeliness lies at the heart of the business case for a security fabric in support of ATP.

A security fabric ensures the high level of interoperability needed to drive real-time response. When built on the FortiOS backbone, that fabric supports the security-driven networking needed to ensure protection against ever more sophisticate threats, with Advanced Threat Protection spanning from the end point to the cloud.