SOLUTION BRIEF

# AI-Driven Security Operations

## More rapid threat prevention, detection and response

### Executive Summary

**While the threat landscape continues to accelerate, the task at hand remains the same. Reducing cyber risk requires preventing as many cyber threats as possible while detecting and responding to successful intrusion as quickly as possible in order to minimize damage and expense.**

61% of enterprises say they cannot detect breach attempts today without the use of AI technologies.[1]

**Fortinet's investment in artificial intelligence (AI) enables organizations to increasingly leverage AI and other advanced techniques, deployed across the digital attack surface and along the cyber kill chain, to reduce their cybersecurity risk at a time that security staff are in short supply. As a result, the Fortinet Security Fabric offers the most comprehensive, integrated, and automated cybersecurity platform available in the industry.**

### Accelerating Volume, Velocity, and Sophistication of the Threat Landscape

From 2018 to 2019, the total amount of threat information, including new files, websites, exploits and more, received by FortiGuard Labs grew by 34% to a total of 940 TB. Undoubtedly, the sheer volume of cyber threats out in the wild continues to increase, in parallel with the expanding digital attack surface of most organizations.

Additionally, the velocity of cyber-attack campaigns continued to accelerate. In 2019, the average life cycle of a given threat campaign, from initial appearance to peak prevalence to emergence of a new variant or campaign, was often one month or less. A mature cyber-crime ecosystem exists in which exploit kits, Malware-as-a-Service (MaaS), bots for rent, and more have dramatically decreased the "time to market" for cyber criminals. It is fair to say that, overall, this industry has moved to agile development and delivery.

At the same time, the sophistication of many cyber threats has also increased and is not limited to highly targeted nation-state attacks. Malicious efforts across the board, including social engineering, open-source evasion techniques, and a host of other innovations, result in threats that become increasingly convincing to end-users and difficult to detect by traditional security controls.

**FortiGuard Labs Threat Data**

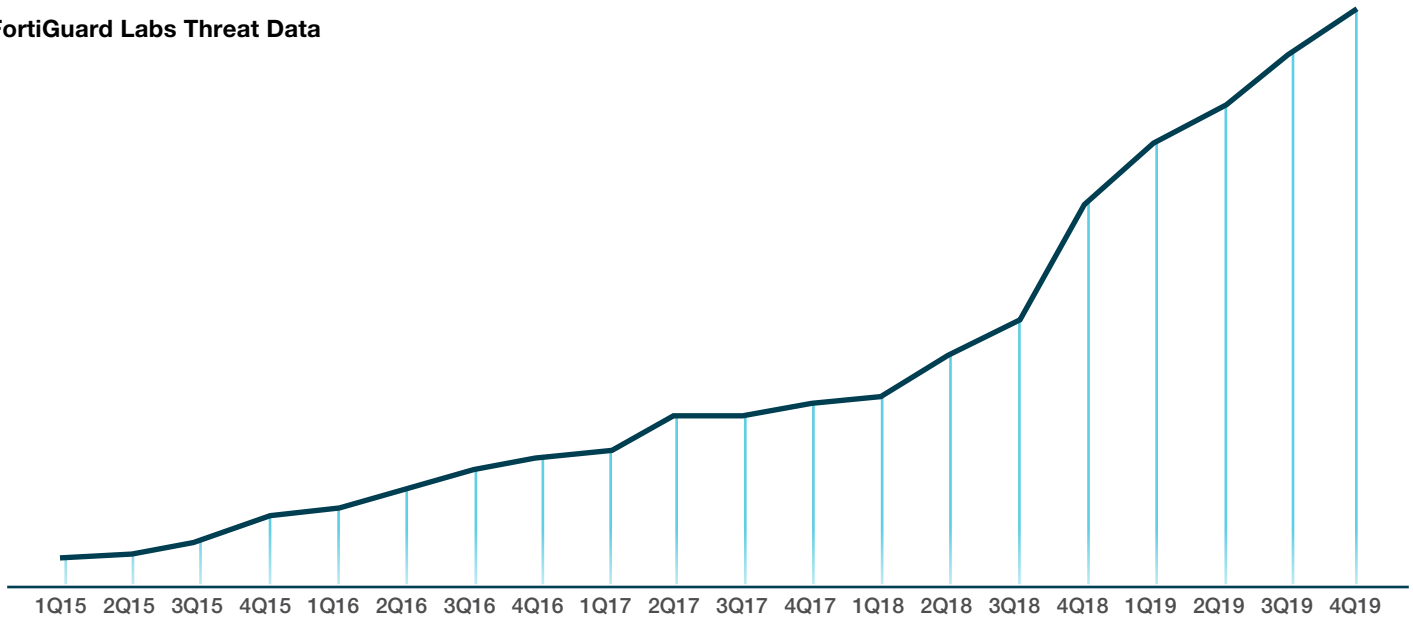



Figure 1: Cyber threat volume between Q1 2015 and Q4 2019.

## Utilize Machine Speed and Intelligence to Stay Ahead

Fortunately, advances in both AI and computing power make it possible (when properly trained and applied) to keep pace with this cyber-threat landscape. Whether the goal is to keep global threat intelligence current, identify organization-specific incidents before they become breaches, or even implement real-time prevention distributed throughout the security infrastructure, AI can and is indeed available to help.

### AI-driven Security Operations

Fortinet utilizes and delivers a range of advanced technologies, including AI, to help organizations prevent, detect, and respond quickly to the constantly changing cyber-threat landscape. Some of these technologies help generate the threat intelligence delivered to customers and utilized by in-line security controls that protect endpoint, network, application, and cloud attack vectors. Others are centrally deployed within organizations to continue looking for threats that may have bypassed these controls and to speed incident response. Yet more can be deployed throughout the organization, often in blocking mode to prevent attacks in real time.

These solutions can be used in various combinations to establish a coordinated defense against cyber criminals, along the entire cyber kill chain. This breadth of coverage gives organizations many opportunities to stop cyber threats at multiple stages prior to a data breach or other substantial impact to operations.

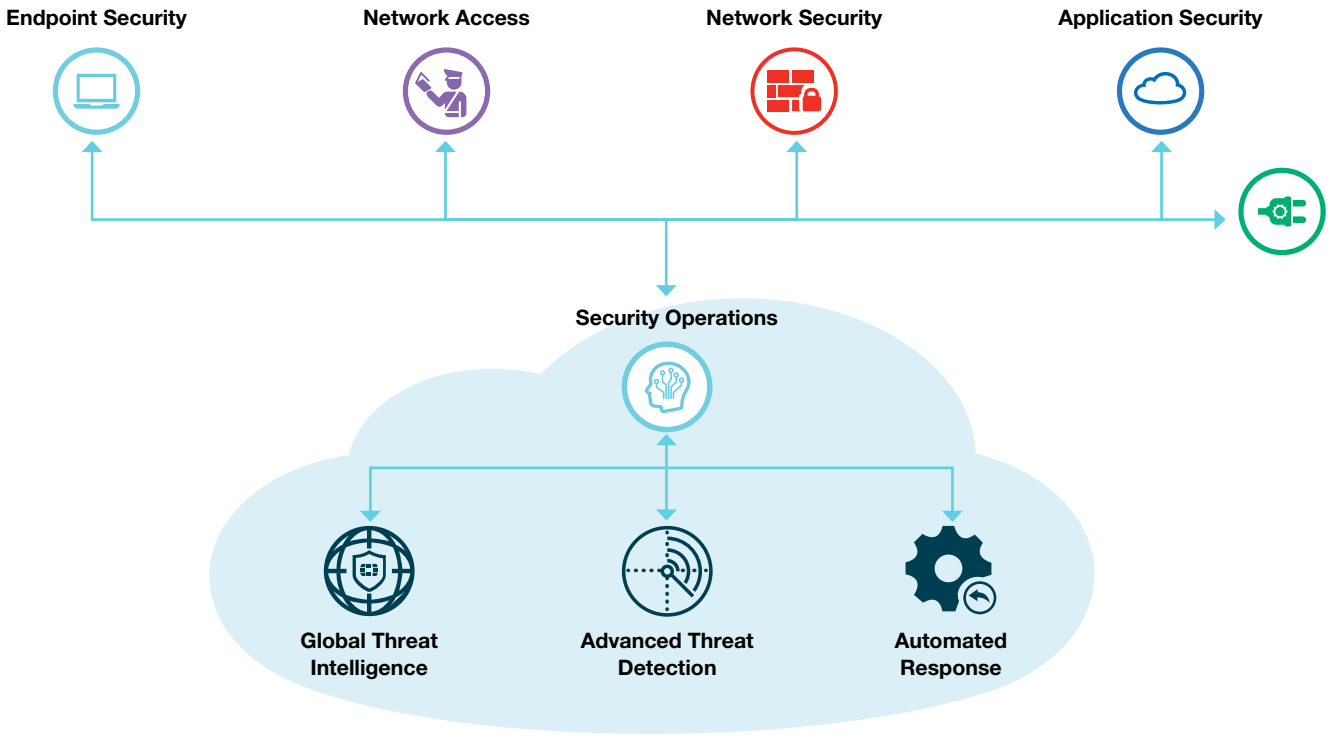



Figure 2: AI powers many of the Fortinet prevention, detection, and response capabilities.

### AI for Threat Prevention

Fortinet delivers independently, and consistently, top-rated security effectiveness from the endpoint, through the network, its applications, and the cloud. Fortinet products include the FortiClient endpoint protection platform (EPP), FortiGate next-generation firewall (NGFW), FortiMail secure email gateway (SEG), and FortiWeb web application firewall (WAF).

These are all powered by the threat intelligence of FortiGuard Labs, a global, multi-disciplinary threat research group. Spanning more than 10 different areas of cybersecurity, FortiGuard Labs maintains a comprehensive view of cyber threats, based on a combination of proactive threat collection, more than 200 cross-industry information-sharing partnerships, and a 5 million device sensor global network.[3]

**FortiGuard Labs generates threat intelligence from AI-driven analysis of over 100 billion security events per day.[2]**

In order to efficiently ingest, correlate, and analyze the large amount of raw data received on a daily basis, FortiGuard Labs has built a robust back-end infrastructure and highly automated process to quickly turn threat data into threat intelligence, which is regularly delivered to Fortinet threat-prevention products through subscription service updates.

Figure 3: Threat intelligence from FortiGuard Labs enables many Fortinet products to identify the latest cyber threats.

Fortinet's first AI system, developed in 2011, was designed to help screen the huge volume of new websites that appear daily, flagging those of highest risk for additional investigation by threat researchers. Today approximately 130,000 to 150,000 new websites are registered every day, making human assessment of each increasingly impractical. To manage the exponential increase in websites requiring inspection, four different machine-learning (ML) systems are used. These systems process the massive amount of website telemetry received by the Fortinet sensor network in order to prioritize high-risk websites, such as those hosting domain generation algorithms (DGA) or command and control (C2) servers, for further analysis.

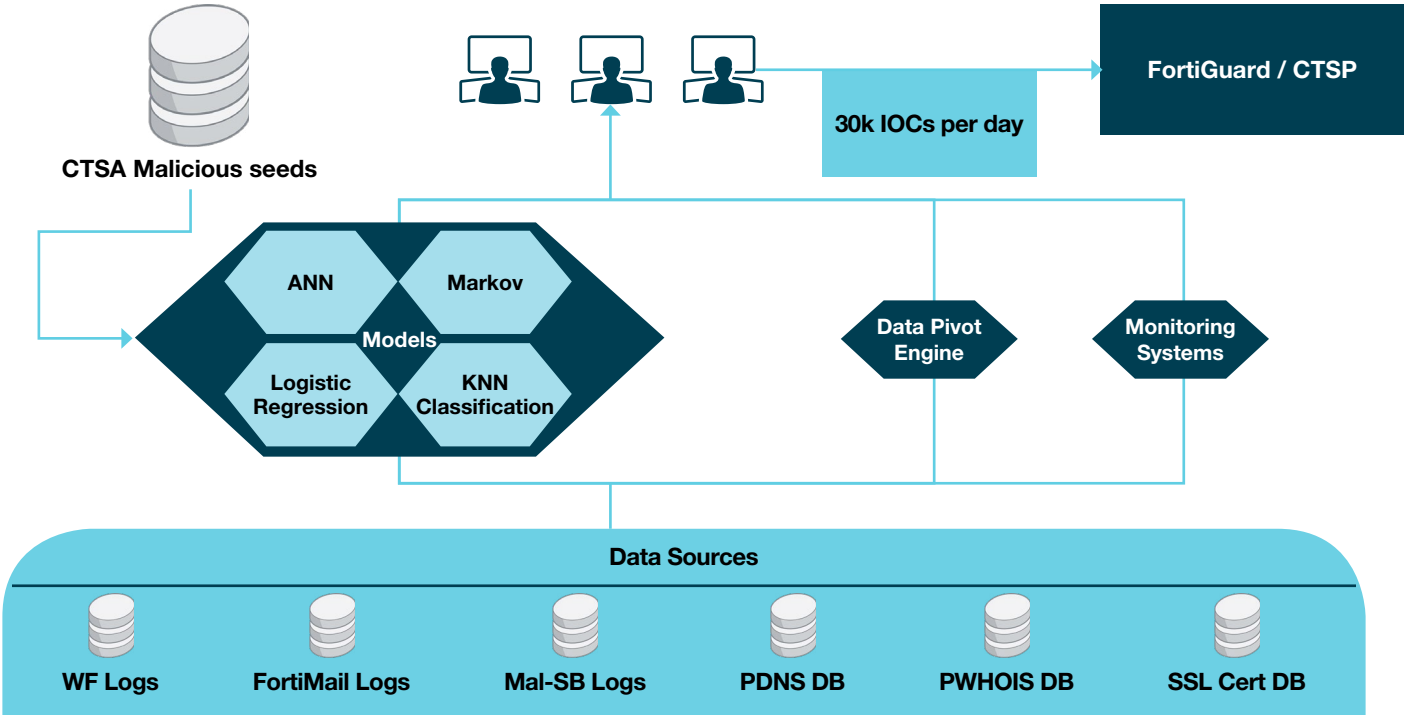


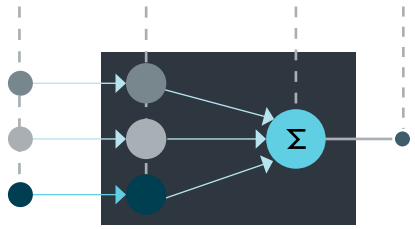

Figure 4: Fortinet collects a large volume of websites from multiple sources each day and applies four separate machine-learning models to prioritize sites for further analysis, ultimately generating 30,000 indicators of compromise (IOCs) per day.

The next major project, started in 2012, addressed the accelerating volume of file-based samples, which were more than 23 million per day at the end of 2019. This system also automates a malware analysis process, which requires eight hours or more of manual effort by a threat researcher. Specifically, an artificial neural network (ANN) facilitates the generation of new threat intelligence that is delivered to customers also on a roughly hourly basis.

## Approach

- **Layer 1 =** Process the input file
- **Layer 2 =** 15 billion+ nodes identify good and bad features
- **Layer 3 =** Mathematics aside (1 = malicious, 0 = clean)

**Sub-second file analysis**



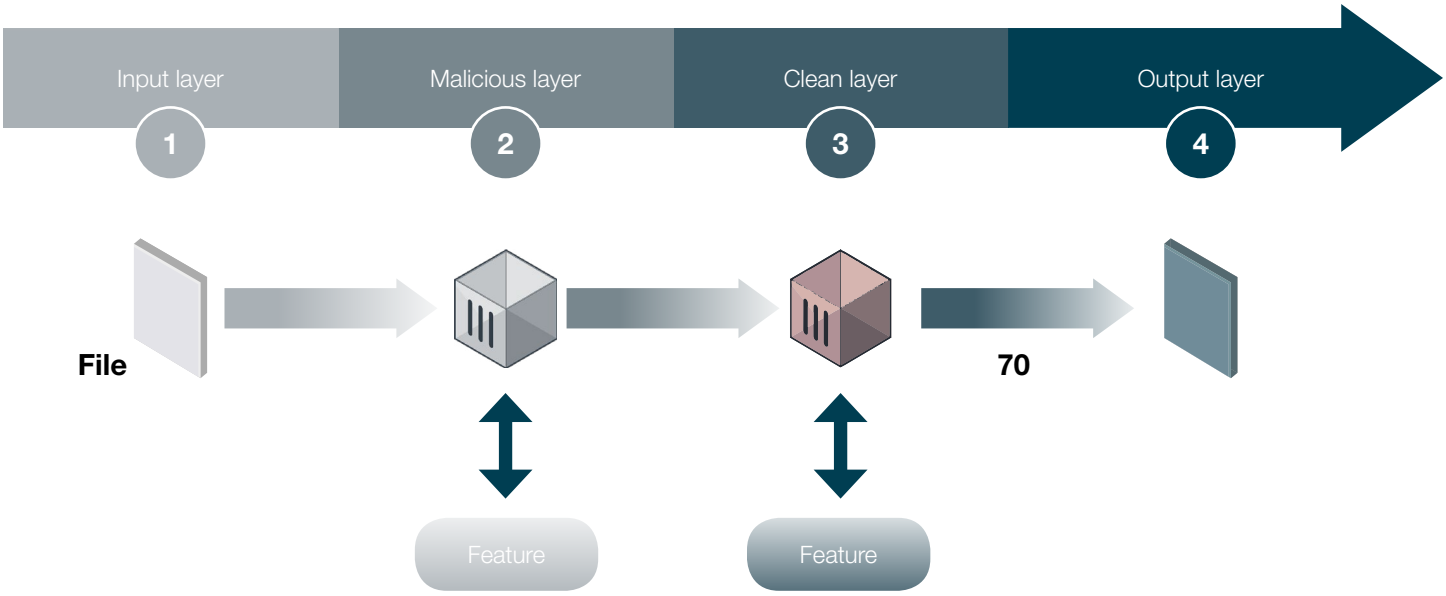




Figure 5: Fortinet artificial neural networks (ANNs) are comprised of 15 billion+ nodes, which learned from unique global threat data collected over many years. Using ML to train the model, threat detection is continuously updated as threats evolve, and overall accuracy is improved.

More recently, two layers of ML have also been integrated into the **FortiWeb WAF** to protect public-facing web infrastructure. One layer builds profiles for each parameter in a given web application and identifies deviations. The second layer determines whether the deviations represent a cyber threat (as opposed to human or other error) by examining them against predefined thresholds for malicious activity. This approach has helped substantially reduce the continual WAF tuning historically required. There are also multiple ML models powering the behavior-based, next-generation antivirus capability of **FortiEDR**.

**FortiGuard Labs provides customers with over 1 billion security updates each day.**[4]

FortiGate, FortiMail, and FortiClient are integrated with **FortiSandbox**, which complements traditional virtual execution analysis with two ML-based filters. One filter is used for static file analysis, and the other is applied to behaviors observed during sandbox execution. With these two filters, the ML-assisted sandbox is often able to return 10 millisecond threat determinations. In FortiMail and FortiClient, customers are able to quarantine suspicious content until sandbox analysis is complete and block even previously unknown threats with the help of FortiSandbox ML-based filters.

### AI for Organization-specific Threat Detection

A determined cyber criminal may evade even the strongest prevention-focused security controls. It is essential for organizations to apply similar advanced analytics to their own traffic and environment, identifying incidents before they lead to costly business impacts. Fortinet offers a number of products to detect incoming, installed, and active threats throughout the entire cyber kill chain.

**FortiDeceptor** deploys a series of high-value lures throughout the organization. These lures attract cyber-criminal reconnaissance, prior to the start of a cyber campaign, or attempts to move laterally throughout the network in order to steal or exfiltrate data.

**FortiSandbox** can be deployed in-line (as previously mentioned) or in the security operations center (SOC) to detect attempted delivery of weaponized payloads. It is complemented by FortiAI, which brings a version of the ANN developed for file analysis at FortiGuard Labs to the organization's own environment. **FortiAI** provides sub-second detection for previously unknown malware, automatically traces indicators of that malware throughout the organization, and provides a more complete threat life-cycle mapping, similar to that generated by a trained security analyst.

If malware delivery is successful, **FortiEDR** utilizes unique real-time code tracing that complements its next-generation antivirus for post-infection identification of suspect host behaviors. Those behaviors can be immediately defused to stop the potential threat, as well as submitted to the cloud where ANNs are used to quickly classify the suspicious behavior as benign or malicious. This allows for the host in question to either be properly investigated and remediated or returned to full operation with minimal operational impact.

Finally, **FortiInsight** focuses on data access and movement, a common late-stage cyber-criminal action. It applies Bayesian probability metrics to identify anomalous activity within (user or device) peer groups that may reflect insider risk or a compromised host. Security administrators can not only investigate the anomaly but also provide feedback on the value of each alert. This helps to train the ML model to become increasingly effective at flagging insider risk.

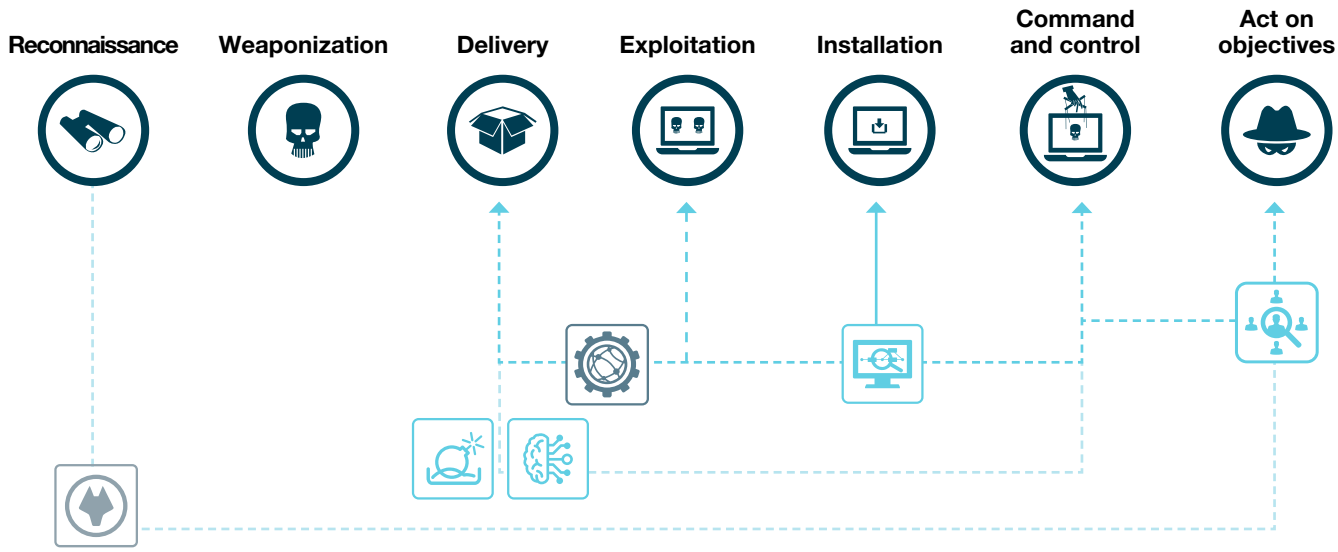



Figure 6: Application of Fortinet solutions to the cyber kill chain.

### AI and Automation to Speed Incident Response

Detection is simply a precursor to response. This is why Fortinet provides a range of offerings to help organizations of all levels of security maturity to orchestrate and automate response actions. **FortiAnalyzer** provides foundational analytics, as well as high-value baseline automations, across the Fortinet Security Fabric. It is suitable for even the smallest or newest security teams.

As organizations mature their security functions and look for multivendor visibility and response, **FortiSIEM** integrates with a wide range of IT and security products to ingest, correlate, and apply advanced analytics that can trigger automated remediation actions across heterogeneous environments.

**Fortinet solutions allow organizations to apply AI across the cyber kill chain to speed threat detection and response.[5]**

For the advanced SOC with well-defined operational processes, **FortiSOAR** can layer on top of any log collection or security information and event management (SIEM) tool to create playbooks that orchestrate and automate those processes. Of note, AI is used to determine prioritization of new alerts and even assign owners. As a result, response workflows are guided and become more efficient, with the option, in many cases, to automate key steps.


Figure 7: Fortinet solutions close security gaps and reduce remediation time by automating threat detection and response.

## Artificial Intelligence Across Attack Vectors, the Cyber Kill Chain, and the World

Fortinet has a long-standing and ongoing investment in AI to address the growing challenges of cybersecurity. ML models and more sophisticated ANNs, trained by the threat researchers in FortiGuard Labs, analyze vast amounts of raw telemetry and help generate global threat-intelligence updates. They are complemented by similar AI systems that can be deployed throughout an organization for in-line prevention, covering endpoint and email to network and cloud as well as ongoing detection and even response.

This enables Fortinet to offer a robust AI-driven cyber defense for security operations that utilizes the advantages of global, centralized, and distributed ML and other AI. With AI models trained and applied for each stage of the cyber kill chain, from reconnaissance through action on objectives, Fortinet solutions are able to manage both outsider and insider risk with advanced prevention, detection, and response.

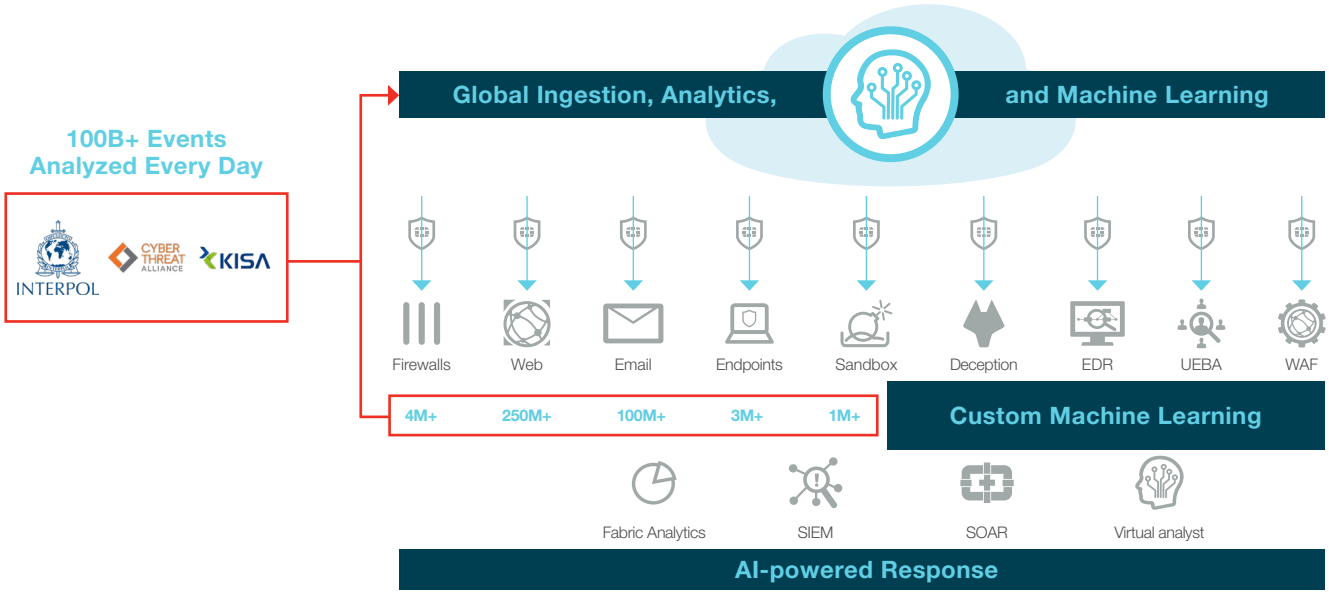



Figure 8: One hundred billion security events are processed by FortiGuard Labs' AI each day to provide threat intelligence updates to Fortinet products.

[1] "Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security," Capgemini, accessed March 23, 2020.

[2] "FortiGuard Security Services," Fortinet, October 2019.

[3] "Fortinet Security Fabric Enables Digital Innovation: Broad, Integrated, and Automated," Fortinet, February 13, 2020.

[4] "FortiGuard Security Services," Fortinet, October 2019.

[5] "Fortinet Introduces Self-Learning Artificial Intelligence Appliance for Sub-Second Threat Detection," Fortinet, February 24, 2020.

FORTINET

www.fortinet.com



April 15, 2020 12:51 AM

627225-0-0-EN

D:\Fortinet\Solution Briefs\teal solution briefs\AI Driven Security Ops Solution\sb-ai-from-fortinet-enables-broad-threat-prevention-V2.1-4152020-1251AM