FORTINET

# Strategies for Protecting the Enterprise from Advanced Threats

## How CISOs Can Lay a Solid Foundation with Security Integration, Automation, and Artificial Intelligence

# Table of Contents



FORTINET

# Executive Overview

The CISO faces an increasingly advanced threat landscape, rendering traditional approaches to security inadequate. Cyber criminals are bombarding organizations with relentless, highly targeted attacks that move at machine speed and overwhelm existing processes. They are using the most advanced technology to make their threats more effective at achieving their objectives.

CISOs must rethink their approach to cybersecurity in order to respond effectively to these trends. This eBook includes several elements that cybersecurity teams must seek in a comprehensive solution:

- **Automation of security processes.** Manual threat response is no longer adequate, and automation is only possible with an end-to-end, integrated security architecture that enables centralized visibility and control.
- **Breadth and scalability.** An organization's security architecture must be broad and flexible enough to incorporate new protections against threats that emerge in the future—and enable the integration of legacy security solutions still in use.
- **Real-time threat intelligence.** CISOs need to leverage technologies like artificial intelligence (AI), machine learning (ML), sandboxing, user and entity behavior analytics (UEBA), and decoys to detect zero-day and unknown threats, root out threat actors, and shrink the windows for incident response and event management when intrusions do happen.

To sum up, CISOs should be deliberate in designing a single, comprehensive security architecture, enabling them to take a risk management-based approach to cybersecurity that is proactive rather than reactive. With that in place, organizations can benefit from an automated approach to breach prevention.

**"The idea that the massive security issues facing businesses today can be resolved by putting more people on the job is naïve."[1]**

# An Increasingly Advanced Threat Landscape Brings Challenges for CISOs

Enterprises today face cyber threats that are increasing in volume, velocity, and sophistication. Threat actors now use emerging technologies like artificial intelligence (AI),[2] machine learning (ML), swarm technology,[3] and Agile development[4] to increase their capacity, make their attacks more effective, and refine their targeting. Consider these trends:

- "Malware-as-a-Service" portals now exist to automate the launch of threat campaigns—and enable nonspecialists to conduct attacks.[5]
- Attackers now use AI and ML to accelerate discovery of new vulnerabilities in applications—and to create new malware variants through polymorphism.[6]
- Threat actors are using Agile development methodologies to aid them in the cybersecurity "arms race." For example, Gandcrab ransomware used Agile to release a new encryption/decryption algorithm one day after security teams released a decryptor for the prior version.[7]

In a world where digital innovation can make the difference between profitability and unprofitability, organizations cannot afford to be impeded by a cyberattack—or by efforts to prevent one. This is why the CISO's challenge is to provide comprehensive protection in a way that facilitates an agile and well-functioning network. The good news is that this is possible with a strategic, integrated approach.

**“Today’s digital economy requires a security approach that allows data, applications, and workflows to move freely across a distributed network while avoiding an open environment where attackers can easily move and cause damage.”[8]**

# Automation and Integration: Building on a Stable Foundation

The current advanced threat landscape means that security teams are overwhelmed by the volume of alerts and the speed and sophistication of attacks. Even if it were possible to respond to each alert manually, threats now move at machine speed and even the fastest manual response could be too late. What is more, an increasing percentage of threats are unknown or zero day, rendering traditional, signature-based malware detection inadequate.

The only answer to all these challenges is to automate security workflows organizationwide. Specifically, CISOs should take steps to automate the following:

- Consistent security policy management across the infrastructure, from the core of the network to the edge
- Configuration management for all systems, from the data center to multiple clouds
- Threat detection and response, including automated ways to recognize unknown threats
- The orchestration of security so that DevOps teams can build security into applications from the ground up

At many organizations, years of filling security gaps with targeted but siloed solutions have created a barrier to automation. When systems do not communicate with each other, manual work is always required to correlate data between systems. Clearly, true automation of threat detection and response requires an end-to-end, integrated security architecture. CISOs need a solution that brings:

- Single-pane-of-glass visibility for the entire infrastructure, from the data center to IoT devices to multiple clouds
- Centralized control of the entire security architecture
- Aggregated threat intelligence from a worldwide intelligence network
- The use of AI, ML, and sandbox analysis to detect new threats by their characteristics
- The ability to take automated action in real time in response to incoming threats

**“Highly evolved organizations are 24 times more likely to always automate security policy configurations compared to the least-evolved organizations.”[9]**

# Breadth and Flexibility: Covering Current and Future Threats in a Practical Way

One aspect of the advanced threat landscape is that it is constantly evolving. Two examples: phishing has evolved into spear phishing,[10] and threat actors may be laying the groundwork to transform botnets into swarmbots.[11] No one really knows what the threat landscape will look like 5 or 10 years from now.

Given that uncertainty is the name of the game, how can an organization proactively prepare for what is to come? Put simply, an organization's security architecture must be broad enough to cover all current and emerging threats, and flexible enough to seamlessly accommodate new protections needed in the future.

Such flexibility is also needed for more practical reasons. While it might be ideal to "rip and replace" an entire security infrastructure in favor of an end-to-end, integrated solution, past investments in specific products may make a phased approach more practical.

For both of these reasons, the integrated architecture should make room for—and encourage—the full integration of third-party tools. An ideal solution would have the following:

- A centralized operating system upon which all security tools are built, enabling seamless integration of all parts into the whole
- An open ecosystem that enables the vendor to work with third-party providers to integrate their tools[12]
- An open and robust application programming interface (API) that enables individual organizations to integrate tools themselves

**"In the face of mounting global threats, companies must make methodical and extensive commitments to ensure that practical plans are in place to adapt to major changes in the near future."[13]**

# Real-time Threat Detection: Catching New and Old Threats

Underlying an effective cybersecurity strategy is information—namely, the most up-to-date intelligence on current and emerging threats. CISOs should look to build a two-pronged approach, targeting both malware and the attackers themselves.

**A malware-based defense.** Every file that attempts to travel on the corporate network, whether it originates internally or externally, should be subject to scrutiny. Signature-based malware protection is still effective for known threats, but an increasing percentage of malware is unknown or zero day.

For these threats, sandboxing is a critical behavior-based capability in which potential threats are observed in a simulated environment before being allowed through. But to avoid the slowing of other network activity, organizations should look for a solution that pre-filters a big majority of traffic based on other types of threat intelligence, and deals with secure sockets layer (SSL) and transport layer security (TLS) inspection without impacting network performance.

**An attacker-based defense.** To fight the attackers themselves, CISOs should look for a solution that provides an arsenal of tools to identify and neutralize them.

A critical network-based approach is a fabricated deception network. When used strategically as a part of the overall security architecture, decoys can provide an early warning system by luring attackers and combating new obfuscation methods used by threat actors.

UEBA is an important endpoint-based capability that detects insider threats and externally compromised internal systems. In a world where the notion of trust is no longer static, it identifies anomalies in the normal practices of trusted users and entities.

**AI-powered intelligence.** Both of these approaches depend on a robust threat intelligence. In a world where cyber criminals now use AI and ML to design the next generation of malware,[14] using AI and ML to identify threats is no longer an option for a CISO. Since systems trained by ML become more accurate as they process more data,[15] CISOs should look for an AI-powered threat-intelligence source that has been in operation for as long as possible and draws data from a large network of sensors. And the best solutions use all three learning modes of ML—supervised, unsupervised, and reinforcement learning.

**“Threat intelligence that tips your organization off to an impending cyberattack is timely. Putting together the indications that an attack was coming after it already happened is not.”[16]**

# Conclusion: A Proactive, Risk Management-based Approach

Increasingly, cybersecurity risk is an existential concern for organizations. And as the advanced threat landscape morphs and evolves, the CISO may feel that he or she is aiming for a moving target. The best approach, of course, is to be proactive rather than reactive, but that is easier said than done. CISOs should begin by asking high-level questions like these:

1. Are the organization's current security workflows adequate for the volume and speed of attacks?
2. Is the organization able to detect and prevent unknown and zero-day threats in near real time?
3. Can the organization identify insider threats before it is too late?
4. What would it take to fully integrate the existing security architecture?
5. What steps can be taken to automate security workflows and compliance tracking that are currently done manually?
6. How can detection and response to threats be automated and coordinated across the network?
7. Can an architecture be built that is agile enough to protect against current and future threats, without rebuilding it in the future?

Starting with these strategic questions can help the CISO build a security infrastructure that enables a proactive approach to security—and protects the organization against current and future threats. And it does so in such a way that the business is enabled rather than impeded. As a result, the cybersecurity team is transformed from a service provider role in the organization to a true driver of business results.

**"Bolt-on solutions are a thing of the past. Security is something you build, not something you do."[17]**

[1] Laurent Gil, "The Debate is Over: Artificial Intelligence is the Future for Cybersecurity," SC Media, March 22, 2018.

[2] Paul Gillin, "Report sees peril in cybercriminals' looming use of AI," SiliconANGLE, June 21, 2019.

[3] Derek Manky, "The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware," CSO, August 29, 2018.

[4] John Maddison, "Cybercriminals Are Leveraging Agile Development, Organizations Must Keep Pace," SecurityWeek, August 21, 2018.

[5] Sergiu Gatlan, "Cryptojacking Overtakes Ransomware, Malware-as-a-Service on the Rise," BleepingComputer, February 6, 2019.

[6] Paul Gillin, "Report sees peril in cybercriminals' looming use of AI," SiliconANGLE, June 21, 2019.

[7] Joie Salvio, "GandCrab Threat Actors Retire…Maybe," Fortinet Blog, June 24, 2019.

[8] Jonathan Nguyen-Duy, "Zero Trust is Not Enough: The Case for Intent-Based Segmentation," Network Computing, March 22, 2019.

[9] "2018 State of DevOps Report," Puppet, accessed May 17, 2019.

[10] Meg King and Jacob Rosen, "The Real Challenges of Artificial Intelligence: Automating Cyber Attacks," The Wilson Center, November 28, 2018.

[11] Derek Manky, "The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware," CSO, August 29, 2018.

[12] "What to Look for in a Cybersecurity Open Ecosystem," Fortinet, May 18, 2019.

[13] Steve Durbin, "Prepare Now for Next-Generation Cyber Threats," CFO, April 2, 2019.

[14] Zeljka Zorz, "AI is key to speeding up threat detection and response," HelpNetSecurity, August 14, 2017.

[15] "Using AI to Address Advanced Threats That Last-Generation Network Security Cannot," June 8, 2019.

[16] Zane Pokorny, "3 Key Elements of Threat Intelligence Management," Recorded Future, August 8, 2018.

[17] David Linthicum, "Put security in DevOps first, not as an add-on," TechBeacon, accessed May 19, 2019.

www.fortinet.com



440543-0-0-EN

November 6, 2019 9:57 AM

eb-advanced-threat-landscape