



COVERING THE BASES FOR ADVANCED THREAT INTELLIGENCE


5 Essentials for Addressing the Changing Threat Landscape

EXECUTIVE SUMMARY


The threat landscape for small and large organizations is growing more dire and complex every day. This requires a strategic response, and no network security strategy is workable without quality threat intelligence. Information on known threats remains critical as their volume increases at staggering rates. But no threat intelligence program is complete without the ability to detect unknown threats—which now make up close to one-third of all new malware. Companies building their threat intelligence infrastructure should look for solutions that use vast amounts of threat data, analyze that data using artificial intelligence (AI) and machine learning (ML), perform sandbox analysis when other methods are not definitive, and provide actionable intelligence for both strategic and tactical purposes.

THREAT TRENDS GIVE PAUSE

It seems that cybersecurity becomes more complex—and more important to the business—every day that passes. In the second quarter of 2018, FortiGuard Labs noted nearly 24,000 new malware variants and more than 4,800 new malware families—a nearly 60% increase over the prior quarter.¹ Over a longer time horizon, the number of daily threat alerts increased from fewer than 1,000 in 2007 to more than 1 million in 2017²—and continues to grow exponentially.



FortiGuard Labs noted nearly **24,000** new malware variants and more than **4,800** new malware families—a nearly **60% increase** over the prior quarter.



Total damages from cyber crime will reach **\$6 trillion** annually by 2021.⁵

Attacks are increasing not only in volume but also in complexity and scope:

- Up to 40% of new malware detected on a given day is zero day or previously unknown, according to estimates by FortiGuard Labs.
- The speed of attacks is accelerating, with exfiltration of corporate data now happening in minutes while the discovery of the typical breach still takes months.³
- The current cost of the typical data breach is \$3.86 million, and there is a 27.7% chance the typical company will experience a material breach over a two-year period.⁴
- Total damages from cyber crime will reach \$6 trillion annually by 2021.⁵
- Small and midsize businesses are targeted alongside enterprises and now comprise 58% of data breach victims.⁶

The complexity of the threat landscape mirrors the increased computing demands and IT complexity resulting from digital transformation (DX). Almost every DX initiative expands an organization's attack surface:

- Enterprises now use an average of 61 different cloud applications on multiple clouds.⁷
- One million Internet of Things (IoT) devices are now being added at organizations every day, and 25% of all attacks will target these devices by 2020.⁸
- Mobile devices and apps continue to grow in scale and importance at enterprises, and half a million routers are now infected with stealth malware.⁹
- Companies are rapidly moving to software-defined wide-area networks (SD-WAN), enabling network traffic to bypass the data center.¹⁰

The number of new malware variants and new malware families increased **almost 60%** in a single quarter, from Q1 2018 to Q2 2018.¹¹

FIGHTING BACK REQUIRES INFORMATION

Given the increasing complexity and risk of the current threat landscape, organizations need to take a strategic, proactive approach to network security. Underlying an effective strategy is information—the most up-to-date intelligence on current and emerging threats.

The dramatic increase in the sheer volume of malware means that real-time intelligence about known threats remains critically important. But the rapid evolution and increased sophistication of current threats means that unknown threats must also be a part of the mix. The increasing use of single-use malware by cyber criminals means that zero-day threats will continue to proliferate, and detection of malware by features and behavior is more important than ever.



97% of viruses now employ polymorphism.¹²

5 ESSENTIALS FOR ADVANCED THREAT INTELLIGENCE

When building a threat intelligence infrastructure, organizations need to consider a number of factors, including the amount and type of data collected, how well an organization's threat intelligence is integrated with external threat intelligence, and how well threat intelligence can be shared across the organization. Here are five essentials that organizations should look for in any threat intelligence solution:

1. A large intelligence network

While analysis of log data from an organization's own security infrastructure can provide a contextual picture, the best approach is to combine this threat intelligence with data from millions of other sources to provide a larger view of the global threat landscape. This is a case where more data is always better—as long as that data can be accurately refined into actionable intelligence.

2. Advanced threat detection using sandboxing

Sandboxing is a critical capability for detecting advanced persistent threats such as ransomware. With sandboxing, potential threats are observed in a simulated environment before being allowed onto the main network. The problem is that subjecting a large amount of traffic to full sandbox analysis is a time- and processor-intensive process, and it can slow network performance to a crawl. Organizations should look for a sandboxing solution that prefilters a big majority of that traffic safely, so that only the traffic that needs further analysis goes into the sandbox.

3. Advanced threat detection using AI/ML

When an organization depends on threat data from millions of sources over many years of time, analyzing that data and distilling it into something that can be used is daunting. Cyber criminals are now using AI and ML to design the next generation of malware,¹³ and making AI and ML a part of an organization's threat detection



infrastructure is no longer an option. Look for solutions that train their systems using all three learning modes of ML—supervised, unsupervised, and reinforcement learning—as such systems will become more and more accurate over time.

4. Actionable strategic intelligence of emerging threat trends

To be effective, threat intelligence must be distilled so that it can inform an overall network security strategy. It should be broad enough to disrupt an attack “somewhere along the kill chain, from initial system probing to network penetration to the final exfiltration of data.”¹⁴ Organizations should “[establish] a baseline of normal network behavior” so that they can “determine when something is behaving out of character.”¹⁵ Good information results in prevention of many threats, early detection of others, and fast mitigation of all of them.

5. Actionable tactical intelligence on the latest threats and best practices

Threat intelligence also must inform tactical actions on a day-to-day basis. The ability to identify and block an attack in real time is paramount: “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 In order to be legitimately called actionable, threat intelligence information must “be understood by people who are capable of taking action.”¹⁷

There are **1M+ threat types today**—up from 50 a decade ago.¹⁸



FROM DETECTION TO PROTECTION

Of course, threat intelligence serves no purpose if the information cannot be acted upon to protect an organization against the threats identified. “It needs to be integrated—in real time—with a larger platform that delivers a layered cybersecurity posture.”¹⁹ As the speed of advanced threats increases, moving from detection to protection requires the automation of security response. This does not eliminate humans from the process, and enables a more strategic use of scarce cybersecurity talent.

For known threats, organizations should ensure that they have a robust set of security tools that address threats across the entire attack surface. Ideally, these solutions will be a part of an integrated security architecture that allows for centralized visibility and control—and therefore true automation.

For advanced and unknown threats, organizations should have policies in place for automatic response to threats detected via a sandboxing solution, AI/ML, or other methods. The current threat landscape requires both detection and response to occur at machine speed. Companies should consider adding services such as virus outbreak prevention (VOS) to disable zero-day threats before their signatures are developed, and content disarm and reconstruction (CDR) to create sanitized copies of previously infected files.

CONCLUSION

Dealing with advanced threats requires a strategic, proactive approach, and every network security strategy is only as good as the threat intelligence it is based on. Actionable strategic and tactical information gleaned from a global threat intelligence network—and analyzed with AI/ML and sandboxing techniques—enables an organization to move into a proactive security posture. This, combined with a strategic and integrated security architecture, reduces risk and supports the business in its DX efforts.



48% of all data breaches are caused by hacking of web applications.²⁰

- ¹ [“Threat Landscape Report Q2 2018,”](#) Fortinet, accessed September 12, 2018.
- ² [“Dave DeWalt and David Petraeus, “The Cyber Security Mega Cycle Aftermath,”](#) Optiv, September 7, 2017.
- ³ [“2018 Data Breach Investigations Report,”](#) Verizon, April 10, 2018.
- ⁴ [“2018 Cost of a Data Breach Study,”](#) Ponemon Institute, July 2018.
- ⁵ [“Steve Morgan, “Top 5 cybersecurity facts, figures, and statistics for 2017,”](#) CSO, January 23, 2018.
- ⁶ [“2018 Data Breach Investigations Report,”](#) Verizon, April 10, 2018.
- ⁷ [“Threat Landscape Report Q3 2017,”](#) Fortinet, accessed April 5, 2018.
- ⁸ [“25% of Cyberattacks Will Target IoT in 2020,”](#) Retail TouchPoints, accessed September 11, 2018.
- ⁹ [“Andy Greenberg, “Stealthy, Destructive Malware Infects Half a Million Routers,”](#) Wired, May 23, 2018.
- ¹⁰ [“Andy Patrizio, “Enterprises are moving SD-WAN beyond pilot stages to deployment,”](#) Network World, May 7, 2018.
- ¹¹ [“Threat Landscape Report Q2 2018,”](#) Fortinet, accessed September 12, 2018.
- ¹² Kevin Williams, [“Threat Spotlight: Advanced polymorphic malware,”](#) SmarterMSP.com, June 13, 2018.
- ¹³ Zeljka Zorz, [“AI is key to speeding up threat detection and response,”](#) Help Net Security, August 14, 2017.
- ¹⁴ Derek Manky, [“The Critical Need for Threat Intelligence,”](#) CSO, April 19, 2018.
- ¹⁵ Ibid.
- ¹⁶ Zane Pokorny, [“3 Key Elements of Threat Intelligence Management,”](#) Recorded Future, August 8, 2018.
- ¹⁷ Ibid.
- ¹⁸ [“Dave DeWalt and David Petraeus, “The Cyber Security Mega Cycle Aftermath,”](#) Optiv, September 7, 2017.
- ¹⁹ Bill Conner, [“Real-Time Cyber Threat Intelligence Is More Critical Than Ever,”](#) Forbes, May 22, 2018.
- ²⁰ [“2018 Data Breach Investigations Report,”](#) Verizon, April 10, 2018.