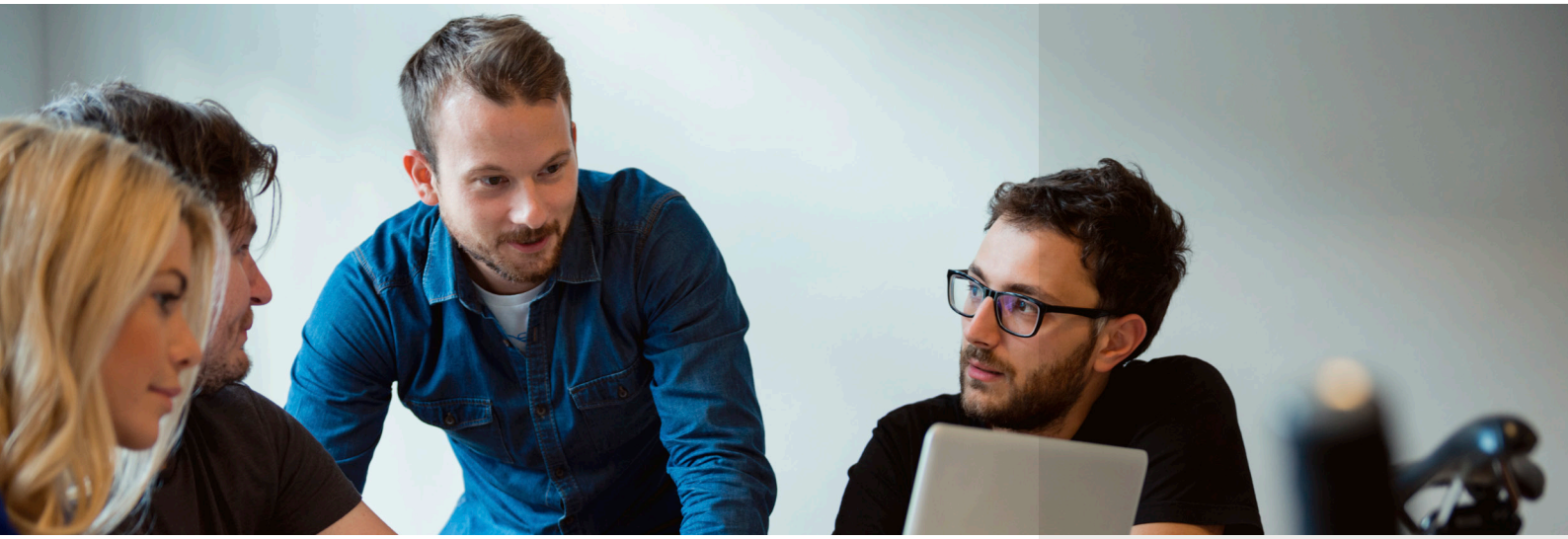
FORTINET

SOLUTION GUIDE

Maintaining Business Continuity Fighting Today's Advanced Attacks



Setting the Stage

The concept of today's advanced attacks, also known as Advanced Persistent Threats (APTs), has become part of the IT community's every day vocabulary and mindset. Driven by the news of yet another data breach, APT's have acquired a mythical meaning but are largely misunderstood. More importantly, it has been assumed that every data breach was an APT even if post-event forensics showed that the initial network infiltration was due to human error or poor network design.

Fanned by the technical press and vendor marketing, end users have been lead to believe that a single technology could solve all of the problems and give them complete protection against an APT. But whether an attack fits the profile of an APT or is just a determined hacker with a new piece of malware, what's most important is the understanding that a network is not a single, homogeneous entity. Today's networks are comprised of multiple technologies dispersed across a number of different sites and both of these; technology and location, as well as the human factor are potential weak links in the network's defensive capability. Only by understanding the requirements and challenges in each of these can a comprehensive defensive scheme be put in place.

Prevent, Detect, Mitigate

To understand how to protect the network, and ultimately the information sought out by cybercriminals, it's necessary to understand the hacker's mindset. Accessing the targeted network may be the result of a sophisticated attack strategy or of winning at the numbers game – throw enough malware at enough networks and eventually an entry point will be found. Stopping these attacks from successfully breaching your network requires a defense that is as sophisticated as the attack itself. Gartner first proposed a multi-layered approach to advanced threat defense that includes both analysis and forensics as early as August, 2013. This concept has continued to evolve but is still the fundamental basis of a comprehensive defensive strategy.

Since the first step in any attack is to infiltrate the network, the initial focus should be on stopping whatever malware there is from entering the network. This is the role of Prevent - thwarting the attempt to breach the network's defenses. The range of technologies and products designed to prevent attacks is wide and mature, with each potential attack vector benefitting from technology specifically designed for it. Network firewalls, web application firewalls, message security gateways and endpoint protection platforms are all useful tools in a prevention strategy.

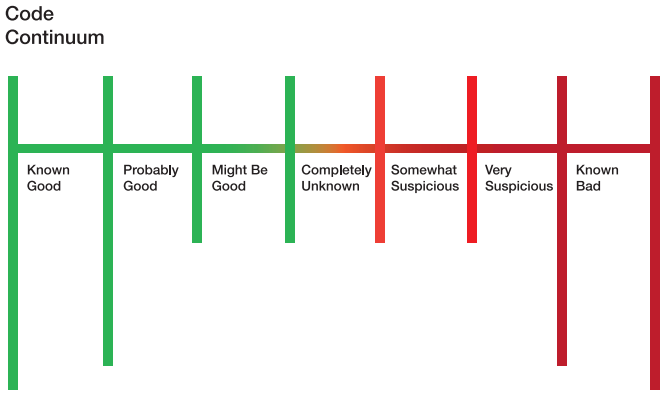


FIGURE 1: THE KNOWN AND THE UNKNOWN

Unfortunately this is where too many networks stop. While necessary, all of the aforementioned technologies are designed to counter threats that are already known (or at least highly suspected) and for which a defense has been developed. Stopping known threats certainly addresses a large percentage of the threat landscape. However, the exponential increase in the volume and variety of malware requires that prevention technologies be complemented with additional, specific technologies that deal with the "unknown" threats and their resulting network breaches. This is the role of Detection.

The underlying premise of detection is that regardless of how robust the prevention capabilities of the network are, eventually the network will be breached. Detection technologies are designed to identify when a breach has happened, ideally before any damage has been done or any data has been ex-filtrated from the network. Some of the detection technologies are extensions of the technologies used for prevention such as client reputation and network behavior analysis. These predictive technologies are designed to establish baseline behaviors for network users and react once the user's behavior deviates from the baseline. Abnormal behavior can be an early warning indicator of malware in the network, such as bot malware, which responds to commands from its Command and Control (C&C) server. A further method to detect an active bot is by monitoring activity on known communication channels.

Another technology, sandboxing, has gained lot of traction to detect previously unknown threats. As a technology sandboxing is not new (threat labs have employed it for automated sample analysis for years), but what is new is the application of the sandboxing concept to a customer's network security. Applying the concept of a safe, controlled environment in which to launch suspicious software to determine whether it is malicious or not has given enterprises a powerful new tool in their detection capabilities. In fact, sandboxing is the key technology called out in Gartner's Advance Threat Defense architecture for Payload Analysis.

Potential malware found in the network - unknown malware since it was able to bypass the prevention technologies - can be "sandboxed" and prompted to execute itself. If the sandboxed sample does turn out to be malicious, the third component of Mitigate now comes into play.

Mitigation is all about reacting to the threat, understanding the extent of it, and containment and corrective actions. Comprehensive network security management and analysis, Security Information and Event Management (SIEM) systems, human resources such as Professional Services and continuous Threat Intelligence and Prevention updates are all part of a comprehensive mitigation strategy.

The Fortinet Solution

Fortinet's Advanced Threat Protection (ATP) solution uniquely encompasses all three of the key components described above – Prevent, Detect and Mitigate.

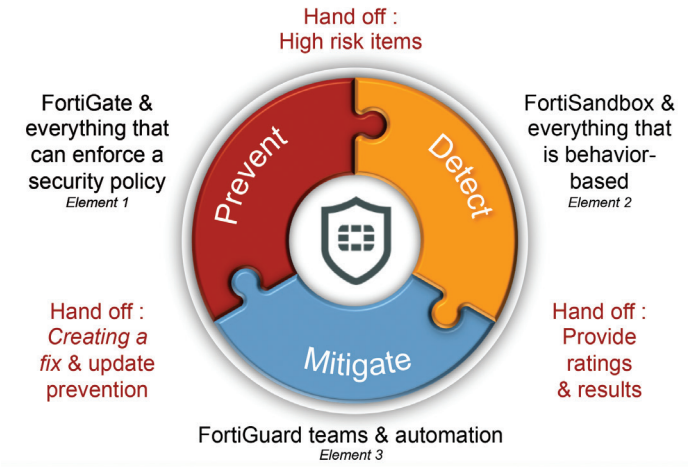


FIGURE 2: THE FORTINET ADVANCED THREAT PROTECTION FRAMEWORK

Keeping in mind that there are multiple, parallel attack vectors that the hacker or cybercriminal can use for their entry into a network, the focus for any ATP solution should be providing the maximum protection possible with all elements of the solution working collaboratively. This is not possible with a collection of individual point products. Only when the different elements of the solution interact will the three action areas – Prevent, Detect and Mitigate– be effective. This is the essence of the Fortinet ATP solution.

Prevent: Protecting Network Access and Beyond

A successful prevention capability relies on multiple technologies working together to reduce the attack surface and block threats from entering the network. FortiGate - Fortinet's network security appliance - goes beyond just being the industry's fastest firewall.

Accelerated by high performance ASIC technology integrated into each unit, FortiGate's multi-service functionality has been, and continues to be its key differentiator in the marketplace. Building from its full function firewall capability, additional higher-level features can be turned on through simple and cost-effective licensing. Depending upon customer requirements, services such as Intrusion Prevention (IPS), Application Control, URL filtering, Antivirus (AV) and end point control can be activated and run simultaneously for effective perimeter protection.

But access to the network via the WAN or Internet is only one possible attack vector. Two other popular vectors are public facing web sites and email servers. These systems need specialized protection. Fortinet meets this challenge with the FortiWeb Web Application Firewall (WAF) and FortiMail Secure Mail Gateway.

FortiWeb is a fully featured WAF and follows the recommendation of the Open Web Application Security Project (OWASP) top 10 most critical web application security risks.

FIGURE 3: OPEN WEB APPLICATION SECURITY PROJECT TOP 10 CRITICAL WEB APPLICATION SECURITY RISKS

Although FortiGate has a URL filtering capability, firewalls are designed to work primarily at the network level and can leave websites and their applications exposed to threats such as SQL injection, Cross Site Scripting (XSS) and remote code execution. FortiWeb provides protection at the application layer and is designed to address the specific needs of today's web-based applications.

The third Prevent element of Fortinet's ATP solution is FortiMail. FortiMail sits between the network and your organization's email server, scanning emails before they reach the server and get delivered to the end user. Like the relationship between FortiGate and FortiWeb, FortiMail complements FortiGate with a more advanced anti-spam capability and its own antivirus and URL filtering to detect known malicious files and URLs embedded in phishing emails. It provides real time inspection and blocking to stop email threats with as little resource impact as possible, often at the connection level. By removing the need for mail queuing if the destination mail server is available, it can deliver message protection for over 28 Million messages per hour in a single appliance.

Because these three systems - FortiGate, FortiWeb and FortiMail - can be deployed as standalone solutions, each one has a full set of features to prevent malware from entering a network. When deployed together, their combined set of features create an interlocking prevention capability across all of the potential attack vectors. One specific common feature however can be thought of as the "glue" that brings everything together – the strong antivirus engine that is part of each of the three products and a key component of Fortinet's prevention capability.

Strong antivirus technology is indeed a vital part of an advanced threat defense. This is due to the fact that a large percentage of malware being used is already known (or variations of the known) and continues to be effective. It's effective because the target systems require periodic updates to correct vulnerabilities than can be exploited by a hacker or cybercriminal. However, some percentage of these systems will either not be updated due to end user indifference or cannot be updated for operational purposes, offering a very large and attractive attack surface. Fortinet's antivirus capability is systematically tested by external, independent organizations and is consistently rated as one of the industry's most effective antivirus solutions in the market.

Complementing the network-based antivirus capabilities is FortiClient, Fortinet's desktop client software powered by the same antivirus engine. By extending Fortinet's strong antivirus capability throughout the network and down to the desktop, the entire network is further protected by this strong prevention capability.

Another aspect of preventing threats from entering the network is user authentication. With the increased use of email phishing to fraudulently obtain login credentials to gain initial entry into the network, the use of two-factor authentication adds an additional level of security to identify legitimate users. FortiAuthenticator and FortiToken along with FortiGate bring strong, two factor authentication capabilities to the network, either as a standalone system or working in conjunction with whatever authentication technology is already deployed. Combining "who you are" with "what you know" can eliminate holes in your user access and identity strategy. Once a user is correctly authenticated and identified, the endpoint control and access policy capabilities of FortiGate can ensure and control that the right level of access is granted to any user or device.

Detect: Eliminating the "Oops" Factor

When an intrusion happens, aside from human error or poor network design, unknown malware will be the most likely cause - malware that the prevention technologies were unable to stop because they were not able to recognize it as being malicious (polymorphism, compression, encryption and password protection are all reasons malware may remain undetected). This is why a second layer of defense is necessary, to deal with the unknown or undetected. As previously mentioned, there are a number a technologies and techniques that should be used for detection including the use of a sandbox.

A sandbox is designed to discover malware that has evaded whatever prevention technologies are present in the network. Ideally, a sandbox would detect 100% of malware within seconds of the intrusion. In the real world however, while 100% breach detection rates are achievable, the amount of time to detect an intrusion – Time to Detect – varies greatly between vendors.

A key differentiating factor between different products is in the relationship between detection and prevention. If the sandbox is designed solely on the principle of detection then every file that passes by the sandbox must be tested. The problem with this methodology is that it takes time, time that the malware can exploit.

To minimize Time to Detect, a sandbox should incorporate some sort of a pre-filtering function to reduce the amount of files that need to be sandboxed. By carrying over part of prevention into detection improves the networks ability to detect and respond to an intrusion.

FortiSandbox is a full featured, multi-layer sandbox that leverages two pre-filtering functions; a strong antivirus capability and cloud access to threat intelligence maintained by FortiGuard, Fortinet's threat research, intelligence and research arm. If not eliminated by these two, separate processes, the sample is then passed onto a full virtual sandbox including code emulation to determine if it is malicious or not. If the sample proves to be malicious, FortiSandbox will upload data about the malware to FortiGuard Labs, which will analyze and ultimately push an update to Fortinet products worldwide.

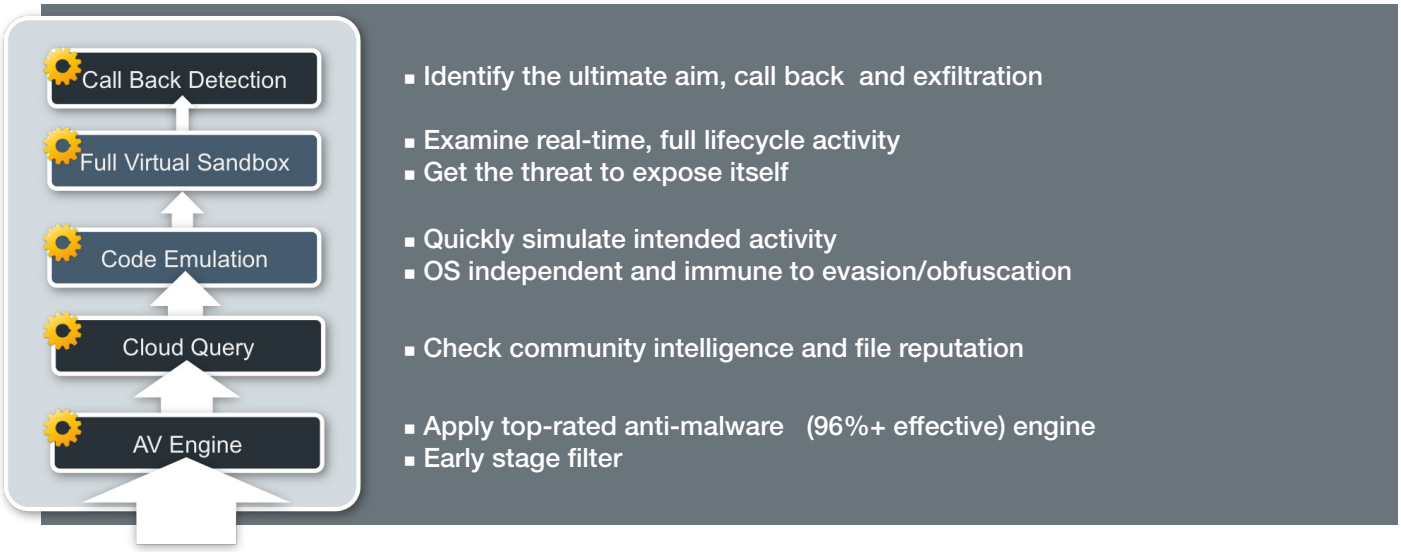


FIGURE 4: FORTISANDBOX THREAT DETECTION TECHNIQUES

Because a sandbox emulates a typical desktop environment, both an operating system such as Windows XP or Windows 7 and applications such as Microsoft Office must be part of the sandbox. Each FortiSandbox is supplied with Genuine Windows and Office licenses so procurement and legal departments do not have to worry about license compliance.

FortiSandbox supports a wide range of protocols and file types including Microsoft Office files, PDF, compressed files (.zip) and even files in shared network locations.

But FortiSandbox is not a standalone device in the Fortinet ATP solution. The different elements of the solution – FortiGate, FortiMail, FortiWeb and FortiSandbox are designed to work collaboratively to provide an integrated solution. For example, if the antivirus engine in FortiMail detects a suspicious file attached to an email, it will hold the email and forward the file to FortiSandbox for analysis. Based on the response from FortiSandbox, FortiMail will either delete the email or forward it to the mail server for delivery. This interaction between the two functions ensures the highest possible efficacy against both known and unknown threats.

Mitigate: Completing the Circle

The enterprise network is constantly under attack from different sources scattered around the world. Some of these attempts will be blocked from entering the network by the different prevention technologies that have been deployed. Those that are able to penetrate the first layer of defense will be subjected to the network's detection technologies including sandboxing. Once FortiSandbox has confirmed that malware has entered the network, a number of different actions need to be taken. The IT security manager needs to evaluate the threat and move to control the damage, quarantine the infected system(s) and ensure the safety of network resources and the company's data. At the same time, the malware used in the breach needs to be fully analyzed and network security systems updated so that a previously unknown threat can become known.

Ensuring that this feedback loop exists between Detect and Prevent is the role of Mitigate in the Fortinet ATP solution. Leveraging the resources and expertise of Fortinet's FortiGuard Labs, detected malware will be submitted by FortiSandbox to FortiGuard Labs for an in-depth analysis. The knowledge gained from this incident will subsequently be fed back to the network, as well as to other Fortinet networks, in the form of an update. FortiGuard Labs and Services are a critical component of mitigation as well as of the overall solution, ensuring that the solution's security efficacy is maintained throughout its lifecycle.

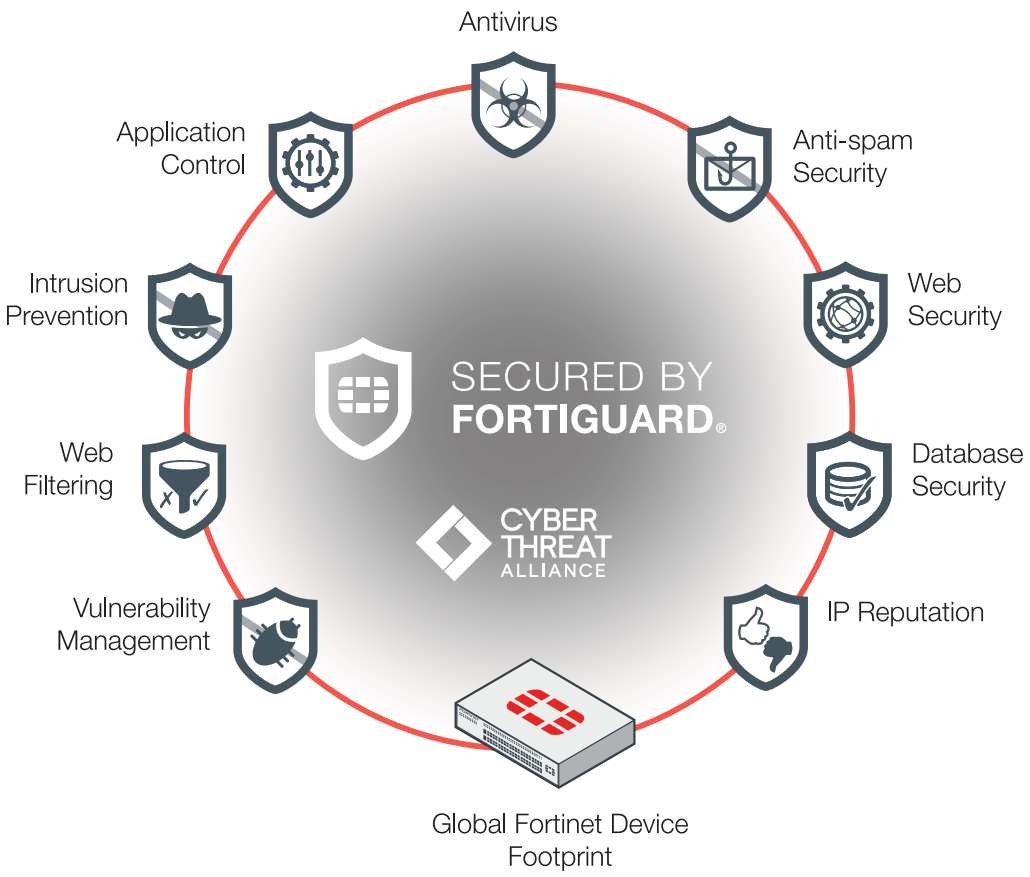
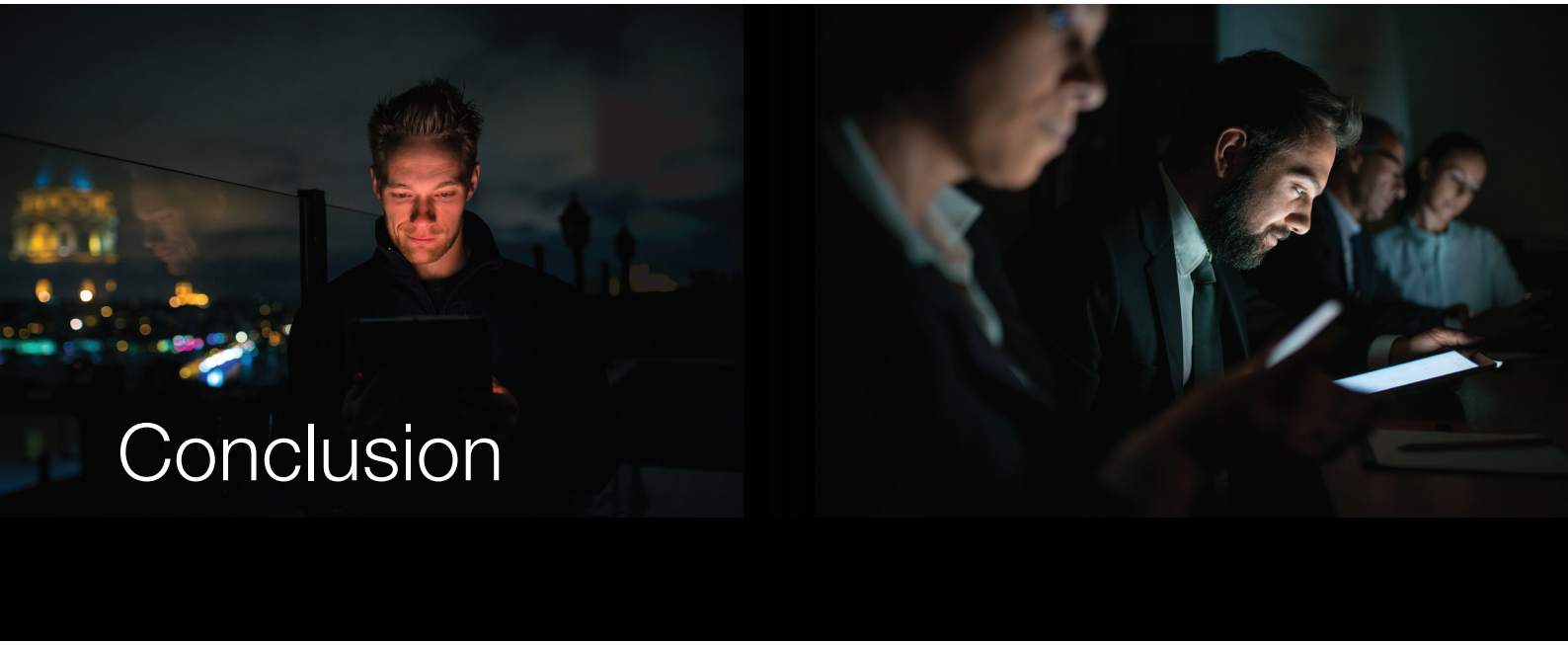


FIGURE 5: THE THREAT PROTECTION SERVICES OFFERED BY FORTIGUARD

FortiGuard Labs is a global organization at the forefront of threat research, Zero Day Threat discovery and threat intelligence. As part of the Cyber Threat Alliance and other related initiatives, Fortinet also shares threat intelligence with a larger body of researchers, further extending the reach of their work and of organization-generated threat intelligence discovered under this framework.



Conclusion

Current and ongoing events highlight the scope of the Internet threats that today's networks face on a daily basis. The hacker and cybercriminal community is talented, committed and determined to exploit any weakness in an organization's network. Because that weakness could be anywhere, the network's defensive strategy has to be a sophisticated as the attacks themselves.

Fortinet's Advanced Threat Protection solution is designed to provide the highest levels of protection against today's sophisticated attacks. Through the coordinated actions of Prevention, Detection and Mitigation, the Fortinet solution provides constant protection against both today's known threats and tomorrow's unknown.

For more information about Fortinet and their ecosystem of Advanced Threat Protection products, visit www.fortinet.com/solutions/advanced-threat-protection.html

FORTINET®

www.fortinet.com

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480