

Building Natural Active Immunity against Advanced Threats

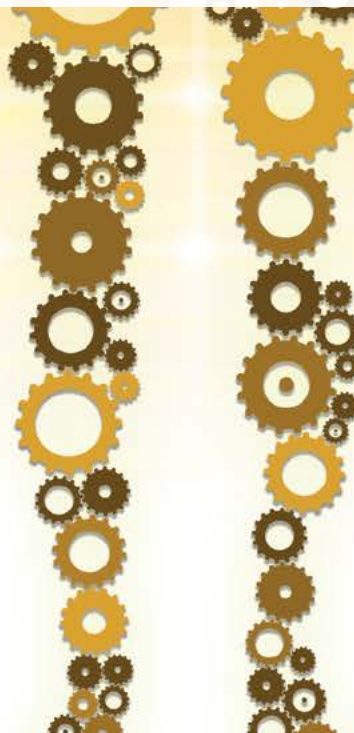




Table of Contents

Introduction	2
Preventing Known Threats	3
Detecting Unknown Threats	3
Mitigating the impact of Unknown Threats	4
The Fortinet Solution	4
Prevent	5
Detect	5
Mitigate	6
Conclusion	7

Introduction

In the late 1980s and early 1990s, when the first computer viruses were appearing in the wild and a nascent ‘anti-virus’ software industry was trying to scare us into buying their products, analogies to the biological immune system were not uncommon.

But as threats became ever more complex, and the technologies required to counter them ever more sophisticated, a new lexicon emerged that was as fragmented as the various point solutions slowly rising to the challenge of securing each part of our corporate networks.

Basic firewalls and antivirus scanning software were soon joined by gateway products that would scan incoming file transfers and email security solutions that would scan for malicious attachments. These defenses in turn acquired new capabilities such as URL filtering, application control, anti-spam and anti-phishing and new classes of product emerged to secure specific assets such as web and database servers. And with each new technology came new vocabulary.

Of the latest industry terms currently in circulation, one of the most hyped and yet least understood is Advanced Persistent Threat (APT), which broadly refers to the risk of protracted, unauthorized access to a network for the primary purpose of stealing valuable information.

One reason for the confusion surrounding APTs is that they often combine

Did You Know*

- The top three industries affected by cyber attacks: Public Sector, Information Technology, and Financial Services.
- In 60% of cases, attackers are able to compromise an organization within minutes
- 75% of attacks spread from Victim 0 to Victim 1 within one day (24 hours)
- 23% of recipients now open phishing messages and 11% click on attachments
- Nearly 50% open e-mails and click on phishing links within the first hour after receipt.
- “One of the most effective ways you can minimize the phishing threat is through awareness and training.” *Lance Spitzner, Training Director, SANS Securing The Human*
- There were many changes in the threat landscape in the last 12 months but just nine patterns still covered the vast majority of incidents (96%).
- Larger breaches tend to be a multi-step attack with some secondary system being breached before attacking the POS system.

* Verizon 2015 DBIR

multiple attack vectors and exploit multiple vulnerabilities, both technical and human, within an organization. This makes them hard to categorize in traditional network security terms, since they traverse the technological silos on which we have previously focused our network security attention. And of course this is the very same property that makes them so hard to detect and eradicate within the network itself.

In the face of such threats, the traditional approach of bolting together the best available point solutions from independent security vendors is like trying to police a city with multiple specialized units – each highly skilled within their own narrow domains but with no communication or coordination between them. Isolated security breaches may be dealt with effectively, but any sustained coordinated attack is likely to slip through the cracks because no common security intelligence is being applied across the system as a whole.

Instead, what are needed are multiple elements with a common ability to collaborate intelligently as one, and it is this philosophy that underpins Fortinet's Advanced Threat Protection solution.

Preventing Known Threats

In the same way that our immune systems comprise many separate layers of defence working together to fight unwanted intrusions, the concept of multi-layered protection is now a cornerstone of modern network security.

A useful analogy drawn between the immune system and computer anti-virus software is the process of vaccination against known pathogens, referred to as 'artificially acquired active immunity'. Here, the pathogen / computer virus is first detected and analyzed by external parties who then create a vaccine / antivirus signature that is reintroduced into the system. This then enables the system to recognize and eradicate this specific pathogen / computer virus on all subsequent encounters.

Code Continuum

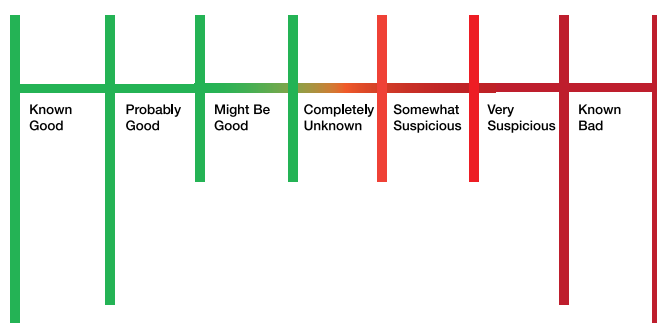


FIGURE 1 – Known vs Unknown

Of course the mechanisms are very different and in the case of computer network intrusion, the 'signature' may also refer to a specific pattern of suspicious network behavior rather than a snippet of malicious code, but the net effect is the same – successful prevention of known threats.

Detecting Unknown Threats

For both biological organisms and corporate networks, intrusions from previously un-encountered threats are sadly inevitable, and the resulting disruption depends on how fast and effectively they can be detected, contained, and eradicated.

Just as our immune system is constantly on the lookout for intruders, corporate networks must remain vigilant of any unusual behavior or suspicious code. To do this, they must rely on a collaborative combination of technologies including behavioral analysis and sandboxing.

By constantly comparing the activity on a network with 'normal' baseline parameters, it is possible to detect the early signs of most network intrusions. Combined with a detailed knowledge of how certain threats progress, such as the communications chain established in the command and control of an active botnet, this can result in accurate and rapid detection for the majority of unknown threats.

Detection of previously un-encountered malicious code is a problem best tackled in two steps. First, although the malicious code may be new in its current form, it may still contain code routines that can be recognized through deep-inspection proactive signature detection technology. However, for detection of genuinely new threats (sometimes referred to as zero-day threats), the best current solution is a breed of network security device known as a sandbox. Used for many years by threat researchers, it is only comparatively recently that sandbox technology has become a realistic option for corporate network security.

The basic idea is to provide a safely isolated environment in which to test any suspicious files entering the network. Such files can be prompted to execute within the virtual environment of the sandbox without risk to the primary system. Any resulting activity can then be monitored, revealing whether the file is benign or malicious.

The second major challenge is not to let the sandbox be fooled by advanced evasion techniques such as logic bombs,

rootkits or bootkits, to name but a few. Aware of the growing usage of sandbox technology within corporate networks, cybercriminals have developed an increasingly sophisticated range of techniques for evading detection, most of which take advantage of the fact that conditions within the sandbox are not quite identical to those of the production network. With this in mind, advanced malware can be engineered to only activate within the production network, thereby evading detection by the sandbox. The only way to counter such techniques is through advanced code emulation analysis where malicious operating instructions can be recognized, even before their code is run.

Mitigating the impact of Unknown Threats

Once an unwanted intrusion of an unknown type has been detected, there are two key things that need to happen:

- Containment

To limit the potential damage of any intrusion, it is paramount that it first be contained, reducing its sphere of influence to as small an area as possible. As in biology, containment of network attacks can involve both inherent, automatic measures, as well as manual intervention such as the quarantine of infected systems by the security administrator.

- Analysis and Memory – The transition from unknown to known

Once contained, the threat must be analyzed to determine its potential impact, risk level, and how it can be recognized by the other components of the network. This information then needs to be spread as fast as possible, both to the administrator and to all other components of the security system, to better inform their combined responses.

Finally, this unknown threat needs to be ‘remembered’ for all future encounters. Our immune system has a natural, automatic capability for building immunological memory known as ‘naturally acquired active immunity’, but until recently, network security had no real equivalent to this.

Traditionally, the analysis of malicious code and the subsequent creation of a corresponding signature has always been an external process involving human intervention. This inevitably meant some significant time delay between the infection and its mitigation / eradication. So while such intervention can reasonably be termed active immunity, it is really ‘artificial’ rather than ‘naturally acquired’ active immunity.

To endow a network with naturally acquired active immunity against advanced threats requires a level of automation and collaboration between its component security systems that until recently had not existed.

The Fortinet Solution

The first part of Fortinet’s unique advantage lies with its core security software that underpins the product range, unifying its multi-layered security response, and providing the integration, collaboration and automation necessary to combat today’s most advanced threats.

The second part is FortiGuard, Fortinet’s semi-automated global threat research network, providing worldwide zero-day threat discovery and intelligence around the clock. As part of the Cyber Threat Alliance and other related initiatives, Fortinet also shares its threat intelligence with a larger body of researchers, further extending the reach as well as the overall quality of threat intelligence.

In terms of coverage, Fortinet provides industry validated protection (e.g. certification by NSS Labs) for all key aspects of the network including:

- The Wide Area Network/Internet/Cloud, via FortiGate
- The Email Server, via FortiMail
- The Web server, via FortiWeb Web Application Firewall (WAF)



FIGURE 2 – ATP Solution Elements

- Network sandbox, via FortiSandbox
- The End Points, via FortiClient

Working together, these products combine to form Fortinet’s Advanced Threat Protection Solution, an intelligent, collaborative security framework that integrates all three of the critical tasks outlined earlier:

- Preventing known threats from entering the network.
- Detecting unknown threats, should they succeed in breaching network defenses.
- Mitigating the impact of any breaches that do occur and ensuring that any future encounters are prevented from initial entry.

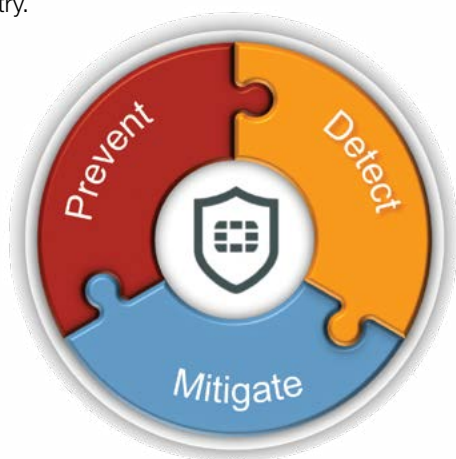


FIGURE 3 – The Fortinet Advanced Threat Protection Framework

Prevent

The first step in prevention is identity control, ensuring that only properly validated users and devices are granted access to the network. The integration and management of this control is handled by FortiAuthenticator and FortiToken.

Next in line are Fortinet’s unified prevention technologies include antivirus, anti-phishing, URL filtering, intrusion prevention, application control and endpoint control. Of these, the antivirus engine, common to all components of the Advanced Threat Protection Solution, is arguably one of the most critical.

Traditional signature detection, being reactive, uses signatures that are essentially fingerprints of known malware. This means that while exact copies of such code will generally be caught, the myriad variants, which have been mutated or obfuscated in various ways, may evade detection.

Fortinet’s patented Compact Pattern Recognition Language (CPRL) is a deep-inspection proactive signature detection technology that goes far beyond the limits of traditional signature matching. The result is that a single CPRL signature

may be able to catch 50,000 or more new variants, and since such variants account for the majority of current active malware, this greatly enhances the efficacy of Fortinet’s prevention capabilities.

With CPRL common to all solution components, the majority of new threats can be immediately stopped in their tracks, irrespective of their chosen attack vector. So whether the attempted access is via email, web browsing, file transfer, or even an infected USB drive, they will be recognized as known threats and duly prevented from entering the network.

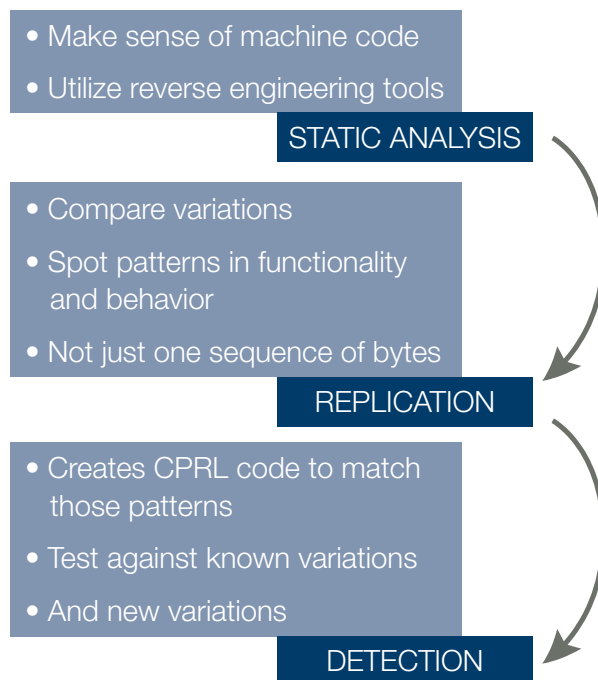


FIGURE 4 – CPRL

Detect

To limit the damage from new threats for which no effective antivirus or intrusion prevention signatures currently exist, the system must remain vigilant of any unusual behavior or suspicious code – a key component of the multi-layered security within FortiGate and FortiSandbox.

FortiSandbox is a full featured, multi-layer sandbox that leverages two pre-filtering functions; a strong antivirus capability, courtesy of CPRL, and cloud access to threat intelligence maintained by FortiGuard Labs. 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 is deemed malicious, FortiSandbox will pass a temporary signature to the other components of Fortinet’s Advanced Protection System, while in parallel uploading full details of the malware to FortiGuard Labs for further analysis and global distribution to Fortinet products worldwide.

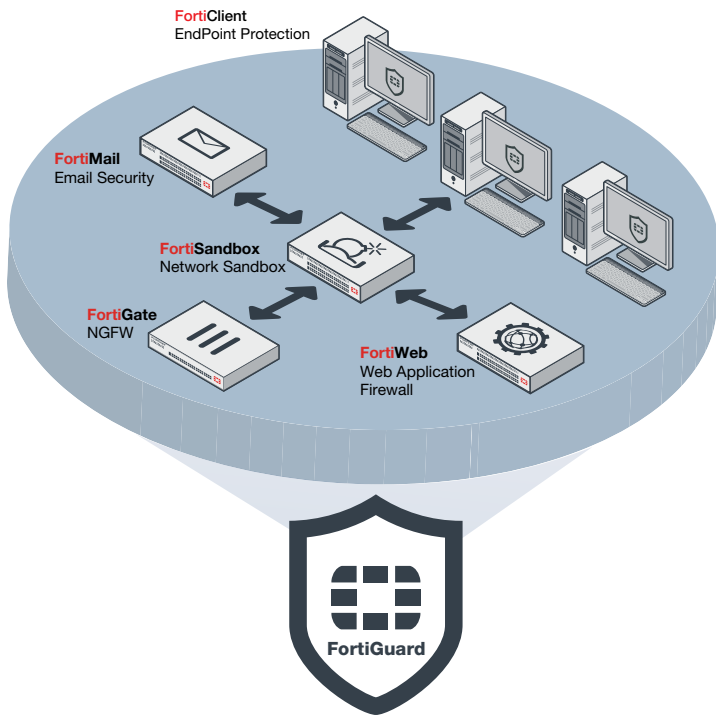


FIGURE 5 – ATP Solution Elements in action

Mitigate

Once FortiSandbox has confirmed the presence of malware in the network, the three processes of containment, analysis and memory come into play:

- Containment

Before considering the various active steps that can be triggered to limit the spread of an attack, it is worth considering the role of network segmentation. With the

traditional notion of ‘perimeter’ all but consigned to history with the introduction of WiFi and cloud technologies, an increasing number of organizations are bringing firewalls inside the corporate network to create secure segmentation of their critical resources.

Deployed inside of the network FortiGate provides both functional and physical segmentation, taking advantage of a wide selection of high speed LAN interfaces and hardware acceleration provided by its custom ASIC design.

Using the granular security policies available with FortiOS, segmentation can be enforced based on criteria such as user identity, application, location, and device type. In this way, the lateral movement of any malicious attack can easily be restricted to the segment of the initial breach.

In terms of active containment, the IT security manager is immediately alerted so that the threat can be evaluated and the most appropriate action taken. This will usually involve quarantine of known infected hosts and possibly further isolation of other mission critical systems.

- Analysis and Memory

At the same time, the malware used in the breach needs to be fully analyzed and network security systems updated so that this 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 and necessarily involves a combination of automation and human intervention.

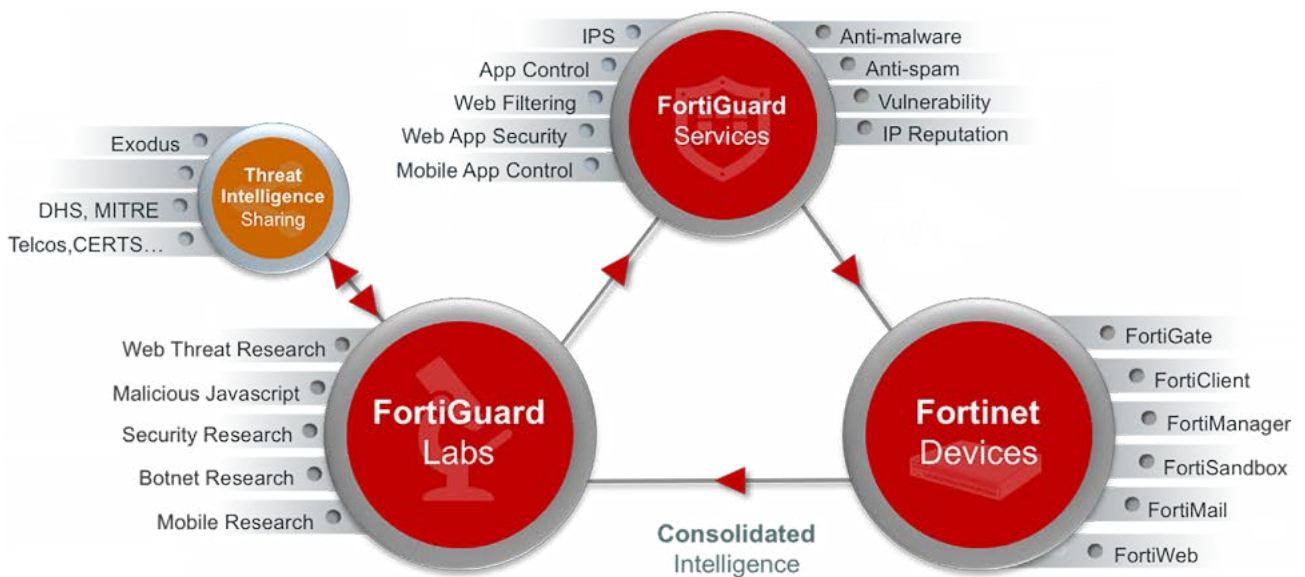
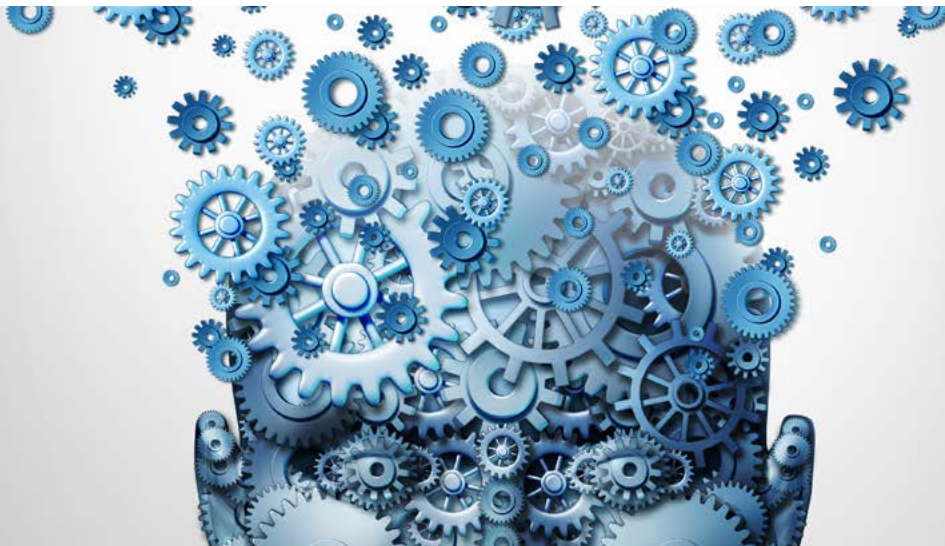


FIGURE 6 – FortiGuard



Leveraging the resources and expertise of FortiGuard, 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 this and 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, providing a threat response capability that evolves throughout the solution's lifecycle.

Conclusion

In the same way that medicine may never be able to fully inoculate us against 100% of all infections, the arms race between cybercriminals and those tasked with protecting their organizations' most valuable data assets will likely never end. As the stakes increase and the technology available to each side becomes ever more sophisticated, IT Security managers need all the help they can get.

But as with any arms race, there are occasional unilateral advances which offer an advantage to one side over the other. Fortinet's Advanced Threat Protection solution, with its unique combination of collaborating, semi-automated, multi-layer security systems represents just such an advance.

Through the coordinated actions of Prevention, Detection and Mitigation, the Fortinet solution provides natural active immunity against the most advanced, persistent threats of today and those of the foreseeable future.



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
905 rue Albert Einstein
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0500

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