EBOOK

IT LEADER'S GUIDE TO ENTERPRISE SECURITY IN A DIGITAL WORLD

WEI

FORTINET

TABLE OF CONTENTS

01 INTRODUCTION

02 NETWORK SECURITY

03 MICRO-SEGMENTATION

04 SECURITY PROFILES

05 SD-WAN

06 NETWORK ACCESS CONTROL

07 IDENTITY & ACCESS MANAGEMENT

08 MULTIPLE FIREWALL FORMS

09 VIRTUALIZED NGFW

10 DATA CENTER FIREWALLS

11 CLOUD WORKLOAD PROTECTION

12 WEB APPLICATION FIREWALLS

13 REMOTE WORK SECURITY

14 ENDPOINT SECURITY

15 VISIBILITY AND MONITORING

WEI

FORTINET

01

INTRODUCTION

01 Introduction

In the past 15 years we have witnessed perpetual technological changes within the enterprise such as virtualization, cloud computing and mobile Wi-Fi technologies. Now compound technology changes with other climatic revolutions such as business outsourcing, digital transformation initiatives and remote work strategies. **Despite the enormity of these changes, one paramount necessity remains constant—the need to protect the usability and integrity of your network and the data that resides within it.** No matter how many renditions of "the new normal" we find ourselves in, network security remains a paramount concern that is never antiquated.

In this new digital age, enterprise companies reside on a delicate precipice. A data breach can permanently damage a brand's image, a ransomware attack can bring elongated business interruptions, and a growing chorus of regulatory compliances (HIPAA, PCI, GDPR and CPPA) can bring forth punishing fines and legal struggles. Some key insights provided by the annual 2020 Data Breach Investigations Report show that little has changed when it comes to threat actors:

- **70 percent of breaches were carried out by external actors**
- **Organized criminal organizations were behind 55 percent of all breaches**
- **45 percent of breaches were implemented by traditional hacking[1]**

A recent survey by VMware in July 2020 showed a disturbing pattern. As remote work strategies expanded, so did the frequency of cyberattacks as 88 percent of all North American respondents reported an increase in overall cyberattacks as a result of employees working from home. The surge in attacks is not limited to those working from home, however.

92 percent of respondents said that attack volumes have increased in the last 12 months and 84 percent reported that attacks are growing more sophisticated.[2]

The inability to curb this wave of cyber threats is certainly not due to a lack of trying. According to Gartner, the world will spend a total of $3.9 trillion in 2020, a 3.4 percent increase over the year prior.[3] The same VMware survey reported 95 percent of respondents planning to increase cyber defense spending next year. The world is not afraid to spend money to protect their enterprises.

In the coming pages, our subject matter experts at WEI will outline a basic road map to better educate your company about what tools are available today that can best protect your enterprise, without breaking the bank.

02

NETWORK SECURITY

WEI

FORTINET

02 Network Security

There is a misconception today that a company's dependence on a network perimeter diminishes as it pushes its digital transformation efforts. The truth is that the perimeter still matters, it's just that there is no longer a single perimeter. **Today's enterprises require multiple perimeters and each of them plays a critical role in securing your network.** This means that the concept of a network firewall that creates a secure boundary between one's private network and an untrusted outside world must be expanded. These multiple perimeters require what we refer today as the Next-Generation Firewall (NGFW).

According to a 2015 survey, 91 percent of security practitioners stated that firewalls were as critical or more critical than ever.[4] This crucial reliance on firewalls will only continue. The network security firewall market is expected to grow at a compound annual growth rate of 13.1 percent from 2019 to 2025, reaching a combined expenditure of $15.8 billion.[5] Today's firewall does far more than simply restrict ingress and egress connections in between perimeters. According to Gartner, NGFWs are "deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bring intelligence from outside the firewall."[6]

Today's NGFW goes far beyond the original concept of what a firewall is. **While many are still purpose-built physical appliances, they also come in other forms including virtual appliances, embedded firewall modules and IaaS platform controls.** Security vendors such as Fortinet, a recognized leader in Gartner's Magic Quadrant for Network Firewalls, consolidates an entire suite of security tools including intrusion prevention system (IPS), antivirus, web filtering, secure socket layer (SSL) inspection, application filtering, DDoS prevention and automated threat protection into a single platform. These security-driven solutions are highly scalable and are programmed to communicate and share threat intelligence within their own proprietary suite of components, as well as third party solutions within multi-vendor environments.

While security is paramount, ensuring that networks keep pace with the speed of business is just as important. Even small business firewalls such as the FortiGate 60-F can provide realistic throughput of 1 GB for an office of up to 25 users. Firewall vendors offer solutions of all levels of performance up to 100 Gbps+ NGFW appliances such as the FortiGate 6000F. Many of these devices incorporate AI-driven intelligence and machine learning in order to address the ever-evolving threat climates of today, as well as the unknown threats of tomorrow.

03

MICRO-SEGMENTATION

WEI

FORTINET

03 Micro-segmentation

FEATURED SOLUTION BRIEF
LEARN HOW MICRO-SEGMENTATION PROTECTS YOUR NETWORK WITHOUT SACRIFICING PERFORMANCE.

A ship's hull is segregated into multiple compartments in order to prevent the ship from sinking in the event of a leak. Health officials recommend social distancing in order to diminish the spread of a virus. In similar fashion, network security architects recommend a segmentation approach when designing your network, providing distancing between network segments. With the increased utilization of BYOD strategies and the proliferation IoT devices, the open flat networks of yesteryear provide petri dish like environments for rapid spreads of malware attacks. These legacy network designs also allow hackers to roam inhibited once they gain entrance through a vulnerable area of the network.

Traditional models of segmentation allocated a DMZ area for web services but little more. This means that any threats targeting east-west or lateral traffic can remain unscathed by simply bypassing perimeter-based security tools. Today's network segmentation, also known as network isolation, provides lateral security controls that help you limit maneuverability of an attacker or invading malware. While network admins have utilized switch VLANs to segment wireless from wired or guests from internal users, the infusion of a firewall to provide segmentation of your network into chunks is far superior. **Zero-trust security policies, traffic analyzation and filtering can be applied to inter-VLAN traffic, ensuring that east-west traffic is secured in the same manner as north-south traffic and that security incidents are contained.**

Micro-segmentation expands this concept even further and is based on the premise that networks should be considered untrusted today. Gartner describes micro-segmentation as the future of modern data center and cloud security. Micro-segmentation takes advantage of the software defined paradigm being adopted by enterprises today by virtualizing data center components into trust groups of related devices. These virtual VLANs can then be assigned different levels of protection through unique granular security policies. This granular approach can even be applied to individual workloads that protect them throughout their journey, whether it be on-prem or in the cloud. **This workload-centric approach is ideal for hybrid networks as well as software defined environments that dynamically respond to traffic loads. This means that workloads can be protected even when traversing third-party networks.** Once again, there is no "one perimeter" using this approach. Instead, your enterprise is comprised of multitudes of micro-perimeters that automatically pigeonhole attackers and malware strains alike in rapid fashion.

04

SECURITY PROFILES

WEI

FORTINET

04 Security Profiles

Your workloads contain many types of traffic and vulnerabilities, thus exposing them to a multitude of attacks threats. Different traffic categories require different security tools, and that is where security profiles come into play. A security profile is a group of options and filters that can be applied to one or more firewall policies. These options provide necessary instructions to the firewall unit for regulating what traffic is allowed through a connection. While many of these same types of profiles can be found in any one of the leading firewall solutions, we will examine some of the available security profiles included in the FortiGate NGFW suite of firewall products. These security profiles come with preconfigured default options. Some are geared towards wired or wireless traffic while others provide varying levels of restrictiveness. Most allow you to modify and create your own sets of custom profiles.

- **Antivirus profiles** can be used to scrub traffic of malicious code including Trojan horses, viruses, worms, adware, backdoor exploits, spyware and other types of malware. These filters check for attributes and signatures associated with malware and removes them.
- **IPS profiles** examine incoming traffic for activity or behavior abnormalities that are consistent with network attacks. Once detected, traffic can be monitored or dropped.
- **VoIP profiles** give you control over SIP and SCCP traffic. These profiles can verify and inspect SIP message syntax as well as restrict particular SIP requests.
- **Application Control** allows you to manage what applications are allowed to traverse your network, even those that utilize non standard ports. You can restrict different application category types such as proxy servers and P2P.
- **DNS Web Filtering** can block known malware, spyware and phishing sites as well as content that goes against your company's internet use policies.
- **Botnet and Command & Control Filtering** allows you to block known botnet coalitions across the globe. These botnets are often used in denial-of-service and credential stuffing attacks. Traffic directed to or from known botnets is simply deleted.
- **Data Leak Prevention** helps ensure that sensitive information such as credit card and social security numbers aren't shared within communicative mediums such as email, cloud shares or instant messaging.
- **Deep level SSL inspection** allows you to decrypt SSL traffic. While malicious code could be embedded in HTTPS traffic, that is no longer the case as a security device can now receive, open and review all SSL traffic on behalf of the client and manage the traffic accordingly.

05

SD-WAN

WEI

FORTINET

05 SD-WAN

34% OF IT DECISION MAKERS PLAN TO MAKE NEW INVESTMENTS IN SD-WAN TECHNOLOGY BY THE END OF 2020.[18]

Remember how easy it was to define a WAN at one time? Not anymore. The corporate WAN is now a complex mesh that is complicated by wireless, cloud and IoT. One of the driving reasons for companies pursuing digital transformations is to make their branch locations cloud ready for cloud and SaaS applications and fully leverage wireless mobility. Unfortunately, legacy architectures that backhaul all traffic to the data center greatly hampers performance.

That is why companies are implementing SD-WAN technology to enhance user performance regardless of location. **SD-WAN unifies multiple physical WAN links into a single logical network and then prioritizes traffic based on application and workload types. It does this through intelligence based routing in which an application or workload is instantly identified and routed to its destination using the most efficient path possible.** Shortcutting cloud traffic can also shortcut security measures, however. Whether it is to increase the response times of cloud based applications for branch users, or accommodate IoT sensors that need to send enormous volumes of data to cloud based data centers, direct internet access vastly increases the exposure of your enterprises to attack threats.

The conundrum for IT leaders today is how to offer business application steering performance at the elastic edge and still secure it. Maximized performance and functionality is of little use unless accompanied by maximum security. **SD-WAN performance without security is not a viable solution, which is why 72 percent of executives surveyed in a recent Gartner report stated that securing their SD-WAN deployment was a top concern.[7]**

Secure SD-WAN completes the package. This involves placing either virtual or appliance-based SD-WAN NGFWs at the branch perimeters that can work in conjunction with the data center. This interaction means that network security and WLAN control can now be managed and enforced in a single motion through a single pane of glass. Secure SD-WAN solutions provide visibility and analytics into your network traffic. A good example is Fortinet, which classifies over 5,000 applications, giving its products the ability to instantly identify nearly any application you run within your enterprise. You can then add any of the security profiles covered earlier so branch egress/ingress traffic is analyzed through multiple security measures in a single pass. **With Secure SD-WAN, network latency and cyber threats are minimized at the same time within a single solution set, thus reducing TCO as well.**

06

NETWORK ACCESS CONTROL

06 Network Access Control

FEATURED WHITE PAPER

LEARN WHY NETWORK ACCESS CONTROL IS ESSENTIAL FOR THE MOBILE ENTERPRISE IN THIS WHITE PAPER.

Security is driven by the need to know. We've discussed the need to know what is embedded within your network traffic traversing your networks in all directions. But gaining application visibility is not enough. You also need to know what is attached to your network because the proliferation of devices on your network expands both the attack surface of your network as well as its exposure to threats. **Network and security admins need to not only know every device and user that accesses their networks, but have full control over the entire network access process.**

The stark reality is that a single, seamlessly harmless device can become a hazardous threat to your network and can singlehandedly bring it down. According to Verizon's 2019 Data Breach Investigations Report, the time it takes for an attack today to compromise a device can be measured in minutes. Unfortunately, the time to discovery can typically be measured in months.[8] As a result, it should be no surprise that the average time required to identify a data breach is 197 days according to a Ponemon Institute study in 2019.[9]

Today's Network Access Control (NAC) solutions are built to add control and peace of mind for enterprises that grapple with BYOD and IoT environments. The aim of a modern NAC solution is centered on visibility, control, and automated response. Visibility must include agentless scanning in order to identify and perform analytics for any BYOD or wireless device. It means not only knowing what is connecting to your network, but when. Control means not only regulating what devices are allowed into your network but enforcing micro-segmentation so that devices can be contained within narrow segments. Automated response means having the ability to quarantine compromised devices in real time. All of these complex security measures need to perform invisibly behind an automated onboarding process that is simplified for large numbers of users and guests.

One of the leading NAC solutions today is FortiNAC, which provides the same level of network access control for both wired and wireless and utilizes up to 17 different profiling methods to determine the identity of a device. **The FortiNAC solution enables effective scaling to multi-site locations and supports millions of devices.** Regardless of which vendor you choose to partner with, a NAC solution can not only reduce your company's exposure to attacks, but your fear of the unknown.

07

IDENTITY & ACCESS MANAGEMENT

WEI

FORTINET

07 Identity & Access Management

Identify and access management is the very essence of what privacy and security is all about. Whether you are guarding access to a corporate headquarters, a school building or an enterprise network, identifying those who wish to gain access is a fundamental security requisite. While the traditional username and password combination proved worthy enough a decade ago, password-only authentication is completely vulnerable today thanks to the simplistic nature of credential stuffing attacks. Hackers now make use of vast lists of stolen username credentials obtained through data breaches and unleash botnet armies to make use of them. These lists are bought, sold and traded in a variety of dark web storefronts. **In 2018, there were nearly 30 billion documented attempts to access someone else's login account using stolen credentials. On average there are 115 million attempts using stolen credentials every day.**[10]

In order to protect the integrity of the network access process, you must append password authentication with a second factor. Companies such as Fortinet are creating multifactor authentication solutions that can transparently identify network users using identity-driven policies. These Identity & Access Management product suites provide Single Sign On capabilities, seamless two-factor/one-time password authentication, and certificate management for wireless and VPN deployments. This includes not only cloud or remote access, but internal network logins as well.

Available solutions such as the FortiAuthenticator integrates with Active Directory or third-party LDAP systems. Companies can choose a primary authentication method depending on their environment such as Active Directory Polling or an SSO mobility agent. For guests or non-domain environments, an authentication portal can be used. A token is then utilized as the secondary method. For mobile users that consistently have access to a smartphone, a mobile token app may prove optimum. An example is FortiToken Mobile that is built for iOS and Android phones and requires no additional hardware. Users can feel comfortable installing it on their personal devices as it cannot make any changes to the phone itself nor capture any type of activity. Another option is the FortiToken 200, a small device the size of a credit card that can generate and display a secure one-time password every 60 seconds to further verify user identity. **Whatever form you prefer, a second layer of authentication can provide an additional layer of confirmation necessary to reduce cyberattack probability and meet government and business regulatory obligations.**

08

MULTIPLE FIREWALL FORMS

WEI

FORTINET

08 Multiple Firewall Forms

When one thinks of a network perimeter firewall, a traditional appliance comes to mind. Hardware firewalls remain an ideal choice in many circumstances. These security enforcement appliances reside between the LAN and the Internet and serve as a hard barrier. All inter-perimeter traffic must be analyzed and scrubbed in order to complete pass through. Due to its placement, all ability to communicate with the other side of the perimeter and transmit data can potentially come to an abrupt halt. This makes it a highly effective gauntlet.

Hardware based firewalls are not a fit for every circumstance however, especially within highly scalable and dynamic networks. Some of the basic shortcomings include the following:

- **They take up valuable space in the data center**
- **They require extensive wiring**
- **The initial setup and configuration is quite extensive**
- **They require forklift upgrades for each product cycle**
- **Supporting them can be expensive**

Network firewalls are now following the same evolutionary trajectory of servers that at one time were exclusively hardware as well. Firewalls today come in a variety of forms and some are built for specific circumstances.

BY THE END OF 2020:

44% of IT decision makers plan to **UPGRADE** their existing Firewall solution

36% of IT decision makers plan to make **NEW** investments in a Firewall solutions

WEI

FORTINET


09
VIRTUALIZED NGFW
WEI
FORTINET

09 Virtualized NGFW

Think of all the many benefits of software defining the compute, networking and storage components of your infrastructure. Now apply them to firewalls. Virtualization means mobility, scalability and agility. These inherent qualities pay big time benefits when it comes to cybersecurity. **The ability to deploy a virtualized NFGW anywhere in quick fashion is significant, as well as the ability to adapt and scale to dynamic network environments that respond to fluctuating workloads.** Software based firewalls are nimble, easy to install and have a lower TCO in most cases. Time savings here is key, as you can download a virtual appliance straight from the vendor and begin operating.

As organizations continue to push computing power back to the edge of their network, the complexity and cost of deploying physical firewalls to every perimeter is prohibitive. Virtualized firewalls can be widely dispersed throughout your network, yet centrally managed using a single pane of glass. These virtualized units can communicate with one another, eliminating the decentralized weakness of legacy network architectures that attackers love to take advantage of. The nature of virtualized NGFW makes segmentation easier. For enterprise companies, it means that each business unit can have their own firewall instance that won't interfere with the traffic or policies of another instance on the same firewall.

VIRTUALIZED FIREWALLS CAN BE WIDELY DISPERSED THROUGHOUT YOUR NETWORK, YET CENTRALLY MANAGED USING A SINGLE PANE OF GLASS.

10

DATA CENTER FIREWALLS

WEI

FORTINET

10 Data Center Firewalls

In the modern enterprise, security and performance are not exclusive. While your users appreciate enhanced security, they detest latency. Performance cannot be sacrificed for security. That's why the selective process of choosing a best of breed appliance for your data center firewall is vital to your enterprise. Once you find a NGFW solution that offers the security services you need, it is time to talk throughput. This usually means a physical firewall. Companies such as Fortinet now offer solutions that host 10, 40 and 100 GE interfaces that can offer throughput ranging from 50 Gbps to over 1 Tbps. Speed and performance isn't limited to throughput. It's also about having the processing power to decrypt encrypted SSL traffic for thousands and thousands of end user devices simultaneously.

Today's data center firewalls not only have to be aware of security, they have to be aware of virtual environments and be able to adapt to their rapidly changing ecospheres.

It must also be as agile as the data centers they protect with the ability to orchestrate the rapid movement of data within hybrid environments that can encompass multiple data centers, cloud infrastructures and remote edges.

DID YOU KNOW?

FORTINET HAS BEEN RECOGNIZED 10 TIMES AS A LEADER IN THE GARTNER MAGIC QUADRANT FOR NETWORK FIREWALLS.[19]

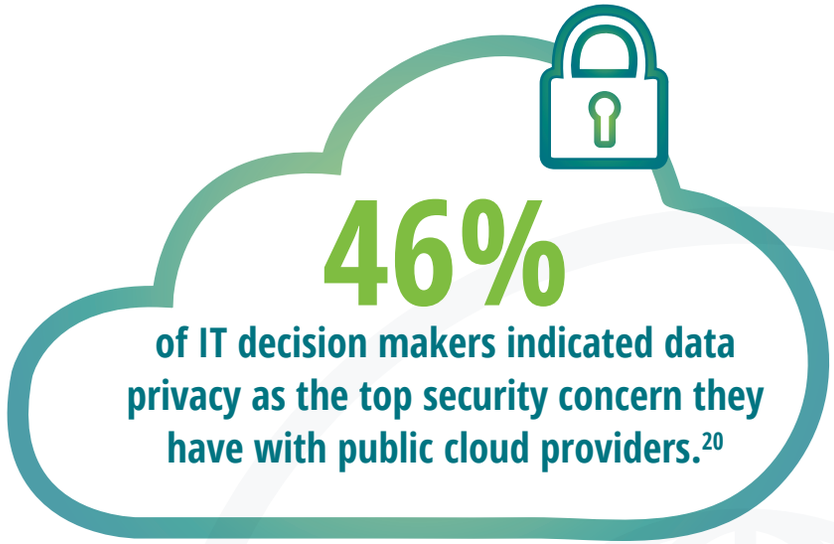
11

CLOUD WORKLOAD PROTECTION

11 Cloud Workload Protection

You cannot have a conversation about network security without discussing the cloud! That's because SaaS applications and users store data and files outside the organization, especially with the growth of remote workforces. This creates a loss of visibility and control for internal IT. Traditional security appliances are ineffective in protecting off premise resources. **While some cloud vendors offer integrated security tools, they are unique to each cloud vendor, averting consistency.**

Due to the rapid expansion of cloud attack surfaces, hackers are regularly targeting cloud infrastructures and SaaS applications, taking advantage of misconfigurations which is a common problem in the cloud. On top of all of this, regulatory compliance still applies to your business regardless of where sensitive data is hosted. In response, leading security vendors are creating solutions designed to secure cloud workloads throughout their entire journey. Fortinet's own FortiCWP hooks into APIs provided by cloud vendors including AWS, Azure and Google Cloud Platform to monitor and track all security components. This and solutions like it offer centralized dashboards and visibility, event tracking, on-demand scanning, traffic flow logs, advanced threat detection and much more. **Whether you host most of your resources in the cloud, or only your DevOps environment, cloud workload protection is a requirement in today's cloud-ready enterprises.**



12

WEB APPLICATION FIREWALLS

WEI

FORTINET

12 Web Application Firewalls

20,000 times a day. That is how often the average web application was attacked in January and February of 2020.[11] That's an extremely worrisome statistic because many companies completely rely on their web applications to perform seamlessly. For many companies, web applications are the primary means of interacting with their customers and conducting commerce. This makes web applications a treasure trove of high value data for hackers, which is why they are so heavily targeted. Because they reside on internet facing hosts it makes them easy prey for attacks. **This degree of open vulnerability compounded with the reliance of these value generating applications calls for an extra layer of security.** That extra layer today is in the form of Web Application Firewalls (WAFs).

Some of the capabilities of modern WAFs today include the following:

- **Scan application traffic for multiple threat types**
- **Enforce traffic shaping of non-priority traffic**
- **Secure and restrict who can connect**
- **Granular control of applications through rapid policy deployment**
- **Protect against automated attacks by bots**
- **Behavioral analytics to detect potential threats**

The motherload for a hacker is the backend database. The compromise of personal identifiable information (PII) can bring about costly remediation, litigation and bad press. A well-executed DDoS attack can suppress all legitimate traffic and completely disrupt your business.

As discussed, WAFs are available in multiple formats including the traditional hardware appliance as well as virtualized deployments designed for designated cloud providers. **Because your web applications are mission critical, a WAF should be an integral part of an effective multi-layer security strategy.**

13

REMOTE WORK SECURITY

13 Remote Work Security

Remember when VPN was boring. It was allocated to just a few select mobile users and support personnel. Now it is an essential part of your enterprise. The VPN market is expected to reach $54 billion by 2024.[12] In fact, the U.S. saw a 41 percent increase in VPN usage alone in a single week in 2020.[13] While much of the recent spotlight on VPN has been due to the surge in remote work strategies, VPN had already witnessed significant growth over the years due to the increased reliance on cloud computing and hybrid networks.

Site-to-site VPN tunneling is nothing new. An organization that resides in a campus environment or has one or more remote offices must have the ability to encrypt its WAN connections in order to secure the movement of data, applications and services. This requires the use of static or on-demand VPN tunnels. The cloud is no different. If you host servers in the cloud, you need a permanent VPN connection to create an encrypted pipeline between your on-premises network and the cloud. This means setting up an IPSec tunnel using your existing firewall or a dedicated VPN appliance. Like Fortinet, most leading firewall solutions offer a number of VPN options. Each site does not have to use the identical proprietary equipment. **A FortiGate firewall will connect to a Cisco unit for example and provides multiple templates depending on the type of environment to make configuration a snap.** You can then assign policies and security profiles to completely secure the connection and scrub traffic of malware and other malicious threats.

You can also setup VPN access for remote users as well. There are two ways to accomplish this. The first involves deploying a VPN proprietary client to designated users. **An example is FortiClient, which serves as a free VPN client, giving you the ability to allow users to VPN from anywhere or restrict access from assigned devices.** You can also provide an SSL VPN portal to allow users to easily connect through a web browser using a designated URL. Remote VPN connections are about more than encrypting traffic, however. You can create policies to control where users can navigate once connected. **You can then apply security profiles to eradicate malware and other malicious code originating from the remote work locations.** This is especially important in the case of home base employees who have consumer grade security devices at best to protect their home networks.

14

ENDPOINT SECURITY

WEI

FORTINET

14 Endpoint Security

There is nothing generic today about endpoint security. Endpoint security should not be equated to simply antivirus software. Consider the following statistics concerning the recent state of endpoint security:

- **At least 30 percent of malware today is zero-day malware[14]**
- **Nearly 40 percent of users that utilize two or more traditional antivirus solutions running simultaneously on their endpoints experienced a malware attack last year[15]**
- **Nearly 66 percent of enterprises have been compromised in the past 12 months by attacks that originated at endpoints at a cost of $440 per endpoint[16]**

Endpoints are the most vulnerable nodes in your enterprise. This includes the cloud. Protecting thousands of these devices is challenging at best in an age when zero-day and fileless attacks are able to easily evade traditional signature protection and whitelisting techniques. Just as you need a NGFW, you need a next generation endpoint security solution as well that is built to combat the most modern of threats.

FortiClient is an example of today's next generation cyber hygiene enforcers. It is a robust advanced endpoint protection solution that detects and combats multiple threat types including malware, exploits and malicious scripts. It does this through advanced vulnerability scanning and correlated threat intelligence. FortiClient received the coveted NSS Labs' "Recommended" rating for the third straight year along with low TCO.[17] The involved test highlights were as follows:

- **100 percent block rate on exploits**
- **100 percent block rate for web-borne malware**
- **100 percent detection rate for evasions**
- **Zero false positives**

FortiClient is just one component of the Fortinet Security Fabric. The fabric incorporates all of the company's deployed security point products so that they work together. FortiClient shares endpoint telemetry intelligence with other deployed devices in your network running the FortiOS including FortiAnalyzer, FortiSandbox and FortiGate. **By leveraging telemetry intelligence, the Fortinet Security Fabric can identify Indicators of Compromise (IoC) and deal with them in automated fashion. It also allows you to centrally monitor and manage their endpoint fleets regardless of the size of your enterprise.** By giving admins deep level visibility into their networks in real time, they can properly investigate and remotely quarantine compromised endpoints before they can attack the network.

15

VISIBILITY AND MONITORING

WEI

FORTINET

15 Visibility and Monitoring

Visibility is a critical necessity to secure something. Regardless of what you are trying to protect, having eyes on the ground is critical to understand the threat level you are up against. *If you don't know what is lurking in your network, how can you protect it?* You need to be able to identify a threat while in its infancy. Too often, discovery takes place when the network is under full-scale attack.

That's why it is so important to have a system that gives your security teams the ability to easily manage the incident lifecycle. Many of the leading IT security vendors today provide a visibility, monitoring and management solution to support security efforts and get advanced notice of threats and suspicious behavior before they can do irrevocable damage to your enterprise. A good example is Fortinet's FortiAnalyzer. FortiAnalyzer provides complete visibility into your network as well as incident response capabilities. It provides security fabric analytics and automation in order to detect compromised endpoints so you can respond to attacks quickly. Through a single pane of glass, security teams can view real-time log and threat data in the form of actionable views, notifications and reports. **Its reporting features include hundreds of pre-built reports and templates that are regulation specific so you can use them for compliance reporting and documentation.**

FortiAnalyzer retrieves its information through multiple sources. These include individual FortiClient deployments or the Enterprise Management Server that manages large scale deployments of FortiClient. It also communicates directly with your FortiGate firewall. One of the features of FortiAnalyzer is FortiView, a comprehensive monitoring system that gives you both real-time and historical data and insight into the activity discovered by firewall.

With FortiView you can instantly view information such as:

- **Your top 10 threats**
- **Top 10 traffic sources and destinations**
- **Top internal and cloud applications**
- **Top policy utilizations**
- **Listing of VPN connections**
- **List of compromised hosts**

Much of this information is shown in animated charts that you can digest quickly. FortiView can also communicate with FortiSandbox or Fortinet access points to provide telemetry insights into your wireless traffic. Regardless of which vendor you choose, a security monitoring and management system takes the mystery out of threat detection.

WHY WEI?

Why WEI?

WEI has the expertise and experience to help deploy and manage your enterprise security solutions. We offer a variety of assessments based on your security needs. Contact us today.

We mentioned earlier that the perimeter matters as much today as it ever did. It also matters which IT security company you choose to partner with. At WEI, ensuring the security of our customers from digital threats matters a lot to us. We have vast experience in configuring and implementing solutions for organizations of all sizes from a multitude of industries including retail, healthcare, finance and higher education. **Whether your digital footprint resides in a single site, multiple branches, multiple countries or up in the cloud, our solution experts have experience working within all types of hybrid IT enterprise architectures.** We specialize in work from home scenarios as well. At WEI, we've seen more than a thing or two. We have practically seen it all, and it is that kind of experience we bring to our customers. It is the depth and broadness of our experience and our life-long commitment to your business success that sets us apart from many VARs today.

WE CREATE CUSTOMIZED SECURITY SOLUTIONS

From a legal perspective, organizations are not expected to protect their digital infrastructures from every possible threat. They are however required to perform their "Duty of Care." This equates to the measures that a reasonable party in that circumstance would have implemented. What this means is that a cybersecurity solution strategy must align with the goals and objectives of your business as well as its budgetary constraints. Just as no two organizations have the same needs, no two have the same threat challenges either. **At WEI, we tailor custom solutions and processes to best suit your unique business.** Our WEI pre-sales engineers collaborate with you from the beginning to properly align your goals and individual needs to the best-fitting security technology.

WE TEST AND REHEARSE OUR SOLUTION DEPLOYMENTS

WEI has invested in the creation of several different labs within our own headquarters to test solutions of all types, including cybersecurity. You can even see them for yourself if you visit us. **Our solutions are created by experienced engineering perspectives and are based on best practices throughout. Creating and testing our solutions in-house in an environment that replicates yours gives us the confidence and ability to implement these solutions at scale, nationwide.** All of this not only ensures that our solutions work as expected, but that deployments operate smoothly and within planned deadlines and expectations. Let WEI create a customized solution to secure your digital assets regardless of what challenges lie ahead tomorrow.

WEI

FORTINET

About

ABOUT WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care.
Because we go further.

At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further. And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 30 years.

ABOUT FORTINET

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks number one in the most security appliances shipped worldwide and more than 450,000 customers trust Fortinet to protect their businesses.

www.fortinet.com

SOURCES

1. https://enterprise.verizon.com/resources/reports/dbir/
2. https://ir.vmware.com/websites/vmware/English/2120/us-press-release.html?airportNewsID=85da6289-ab5e-40e2-86f7-d2b731b0dc93
3. https://securityboulevard.com/2020/05/the-definitive-cyber-security-statistics-guide-for-2020/
4. https://www.darkreading.com/perimeter/like-it-or-not-firewalls-still-front-and-center/d/d-id/1324866
5. https://www.globenewswire.com/news-release/2020/01/17/1972020/0/en/Global-Network-Security-Firewall-Market-Study-2019-2025-A-15-8-Billion-Opportunity-by-2025-Lucrative-Opportunities-in-Next-Generation-Firewalls.html
6. https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfws#:~:text=Next%2Dgeneration%20firewalls%20(NGFWs)%20are%20deep%2Dpacket%20inspection,intelligence%20from%20outside%20the%20firewall.
7. https://www.fortinet.com/blog/business-and-technology/our-customers-emphasize-the-value-of-fortigate-secure-sd-wan-in-
8. https://threatpost.com/verizon-dbir-espionage-c-suite-cloud/144486/
9. https://www.secureworldexpo.com/industry-news/9-years-incident-to-breach-discovery-time#:~:text=The%20latest%20study%20by%20the,is%20identified%20is%2069%20days.
10. https://www.darkreading.com/threat-intelligence/credential-stuffing-attacks-behind-30-billion-login-attempts-in-2018/d/d-id/1334371#:~:text=Credential%20stuffing%20%E2%80%94%20where%20attackers%20use,according%20to%20its%20new%20report.
11. https://techbeacon.com/security/30-app-sec-stats-matter#:~:text=20%2C000%3A%20Number%20of%20times%20the,not%20reach%20a%20targeted%20vulnerability.
12. https://www.marketwatch.com/press-release/virtual-private-network-vpn-market-comprehensive-analysis-growth-forecast-from-2020-to-2026-2020-06-02?tesla=y
13. https://www.networkworld.com/article/3542032/global-vpn-use-exploded-in-march.html
14. https://www.csoonline.com/article/3187422/report-30-of-malware-is-zero-day-missed-by-legacy-antivirus.html
15. https://www.darkreading.com/endpoint/doubling-up-on-av-fails-to-protect-40--of-users-from-malware-attacks/d/d-id/1330229
16. https://www.zdnet.com/article/zero-days-fileless-attacks-are-now-the-most-dangerous-threats-to-the-enterprise/
17. https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2019/fortinet-s-forticlient-blocks-100-percent-malware-in-nss-lab
18. IDG Research commissioned by WEI, January 2019.
19. "Gartner recognized Fortinet a Leader in the 2019 Magic Quadrant for Network Firewalls." https://www.fortinet.com/solutions/gartner-network-firewalls
20. IDG Research commissioned by WEI, February 2016.