FORTINET

ASD'S CYBER MITIGATION STRATEGIES

Addressing the ASD 2017 recommendations with Fortinet

WHITE PAPER

ASD'S CYBER MITIGATION STRATEGIES

Addressing the ASD 2017 recommendations with Fortinet

INTRODUCTION

The Australian Signals Directorate (ASD) updated its "Strategies to Mitigate Cyber Security Incidents" in February 2017. These strategies provide guidance to address targeted cyber intrusions caused by various threats. Of these, "the essential eight" has created a new cyber security baseline for all organisations and is reflective of the current evolving threat landscape.

Initially published in 2010, ASD's guidance described 35 strategies to mitigate one key threat - targeted cyber-attacks. The latest publication includes 37 mitigating strategies, which better recognise the threats that organisations currently face and typically caused by:

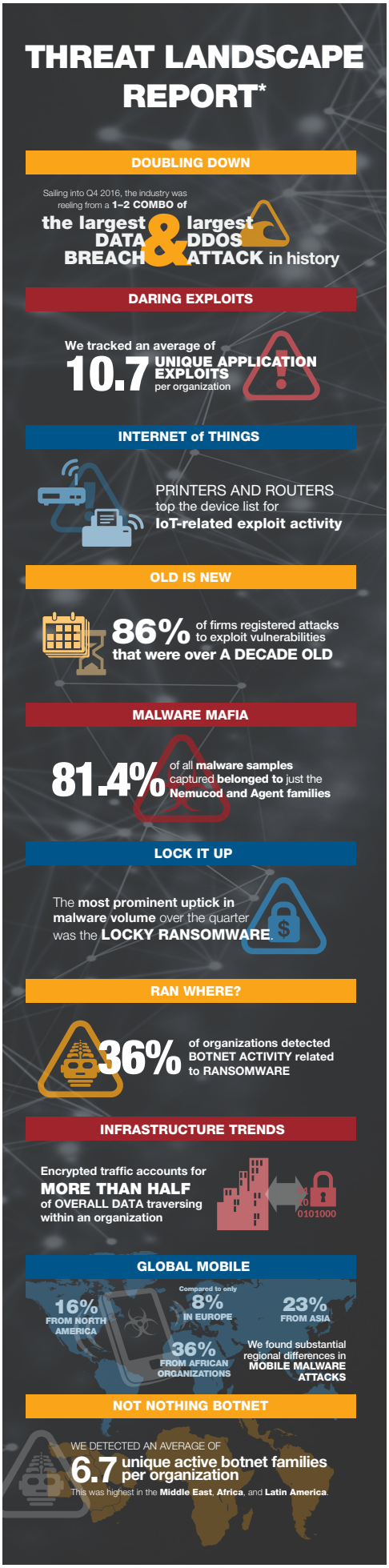
- targeted cyber intrusions (e.g. executed by advanced persistent threats such as foreign intelligence services) and other external adversaries who steal data
- ransomware denying access to data for monetary gain, and external adversaries who destroy data and prevent computers/networks from functioning
- malicious insiders who steal data such as customer details or intellectual property
- malicious insiders who destroy data and prevent computers/networks from functioning
- "business email compromise"
- threats to industrial control systems.

This document outlines the Fortinet solutions that will enable security professionals to address these threats. Fortinet's mission is to deliver industry leading network and content security, and secure access products that share intelligence and work together to form a cooperative security fabric. Our unique security fabric combines Security Processors, an intuitive operating system, and applied threat intelligence to give you proven security, exceptional performance, and better visibility and control - while providing easier administration.

THE ESSENTIAL 8: ASD'S STRATEGIES TO MITIGATE CYBER SECURITY INCIDENTS

The Australian Signals Directorate's (ASD) 'Essential 8' strategies to mitigate cyber security incidents represent a set of cyber security best practices that, when implemented successfully, will provide goverment agencies with a baseline cyber security posture.

The Essential 8 expand upon the 'Top 4' mitigation strategies, part of the government's Protective Security Policy Framework, which have been mandatory for federal agencies since 2014. ASD has stated that implementing the Top 4 mitigation strategies will assist in preventing over 85% of unauthorised intrusions.



* Data pulled from FortiGuard Labs Q4 2016

THE ESSENTIAL 8 AND FORTINET

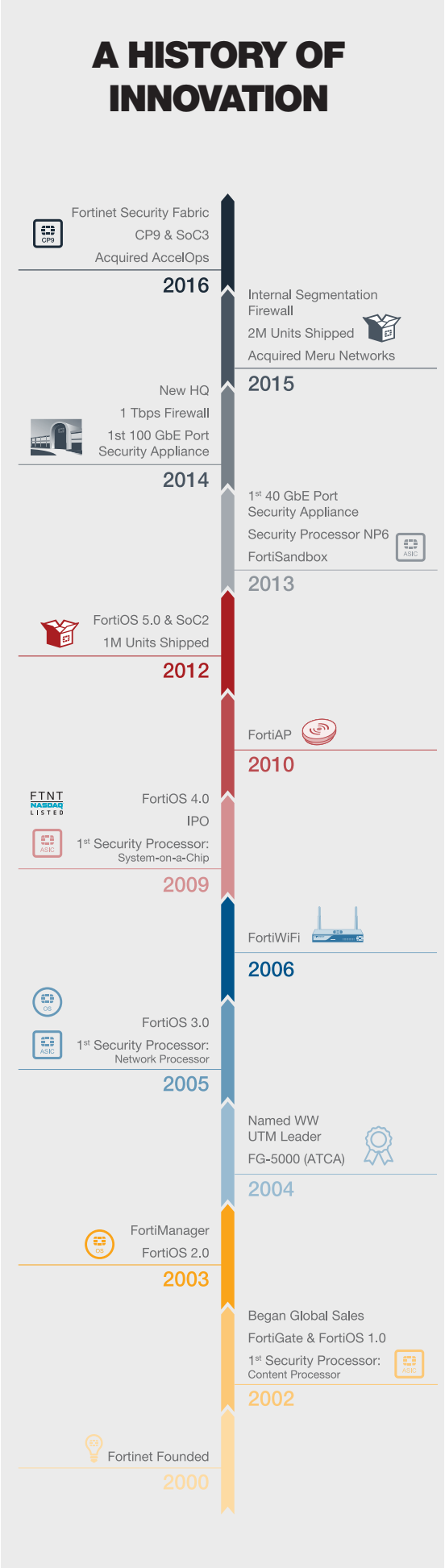
Fortinet's security fabric is ideally situated to support almost all of the 37 mitigation strategies. With the FortiGate next generation firewall, the FortiOS secure operating system, and realtime updates from the FortiGuard threat intelligence service, agencies can ensure compliance and, indeed, automate many of these strategies. Ancillary solutions, including FortiSandbox, FortiAuthenticator, and FortiAnalyzer, not only add critical additional features, but are able to scale up to the largest workloads.

The advantage of Fortinet's Security Fabric is that all components are tightly integrated. This enables a synchronised, multi-level approach that provides comprehensive protection. If adversaries compromise one layer of the defensive measures, they'll be stopped before they can go further. Integration by design also provides visibility across every device in a distributed network, manage most of the day-to-day activities from a centralised dashboard, monitor traffic and application usage, and take quick action if any anomalous activity is detected. This is especially critical for advanced threat protection.

The Essential 8 strategies go a long way toward protecting your agency from security breaches and potentially damaging malware for a comparatively modest financial investment. While implementing these strategies will entail an investment of staff time and possible hardware and software upgrades, the costs involved will be considerably lower than cleaning up in the wake of a compromise.

CORPORATE OVERVIEW

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organisations 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 #1 in the most security appliances shipped worldwide and more than 290,000 customers trust Fortinet to protect their businesses. More than 300,000 customers worldwide, including the majority of the Global Fortune 100, rely on Fortinet for protection. Every Fortune 10 Carrier relies on Fortinet's high performance solutions to secure their mission critical networks, as do 9 of the top 10 retail and commercial banks and 70% of the top aerospace and defence agencies.



ASD STRATEGIES TO MITIGATE CYBER SECURITY INCIDENTS

ASD Relative Security Effectiveness Rating	Mitigation Strategy	ASD Potential User Resistance	Fortinet Upfront & Ongoing Cost	Fortinet Solution
Mitigation Strategies to Prevent Malware Delivery and Execution				
Essential	Application whitelisting of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.	Medium	Low	FortiGate Application Control FortiGuard
Essential	Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.	Low	Low	FortiGate IPS FortiSandbox FortiGuard
Essential	Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.	Medium	Low	FortiGate Application Control FortiGuard
Essential	User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.	Medium	Low	FortiGate Application Control FortiGuard
Excellent	Automated dynamic analysis of email and web content run in a sandbox, blocked if suspicious behaviour is identified e.g. network traffic, new or modified files, or other system configuration changes.	Low	Low	FortiSandbox
Excellent	Email content filtering. Whitelist allowed attachment types (including in archives and nested archives). Analyse/sanitise hyperlinks, PDF and Microsoft Office attachments. Quarantine Microsoft Office macros.	Medium	Low	FortiMail FortiSandbox FortiGuard
Excellent	Web content filtering. Whitelist allowed types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks and free domains.	Medium	Low	FortiGate Web Filtering & AV FortiCache Web Filtering & AV FortiSandbox FortiGuard
Excellent	Deny corporate computers direct Internet connectivity. Use a gateway firewall to require use of a split DNS server, an email server, and an authenticated web proxy server for outbound web connections.	Medium	Low	FortiGate FortiGate Web Filtering & AV
Excellent	Operating system generic exploit mitigation e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Low	N/A	N/A
Very good	Server application hardening especially Internet-accessible web applications (sanitise input and use TLS not SSL) and databases, as well as applications that access important (sensitive or high-availability) data.	Low	Low	FortiDB FortiWeb FortiGuard
Very good	Operating system hardening (including for network devices) based on a Standard Operating Environment, disabling unneeded functionality e.g. RDP, AutoRun, LanMan, SMB/NetBIOS, LLMNR and WPAD.	Medium	N/A	N/A
Very good	Antivirus software using heuristics and reputation ratings to check a file's prevalence and digital signature prior to execution. Use antivirus software from different vendors for gateways versus computers.	Low	Low	FortiGate AV & App control FortiMail FortiClient FortiGuard
Very good	Control removable storage media and connected devices. Block unapproved CD/DVD/USB storage media. Block connectivity with unapproved smartphones, tablets and Bluetooth/Wi-Fi/3G/4G devices.	High	N/A	N/A
Very good	Block spoofed emails. Use Sender Policy Framework (SPF) or Sender ID to check incoming emails. Use 'hard fail' SPF TXT and DMARC DNS records to mitigate emails that spoof the organisation's domain.	Low	Low	FortiMAIL
Good	User education. Avoid phishing emails (e.g. with links to login to fake websites), weak passphrases, passphrase reuse, as well as unapproved: removable storage media, connected devices and cloud services.	Medium	Low	FortiMail FortiSandbox
Limited	Antivirus software with up-to-date signatures to identify malware, from a vendor that rapidly adds signatures for new malware. Use antivirus software from different vendors for gateways versus computers.	Low	Low	FortiClient FortiGuard
Limited	TLS encryption between email servers to help prevent legitimate emails being intercepted and subsequently leveraged for social engineering. Perform content scanning after email traffic is decrypted.	Low	Low	FortiMail FortiSandbox FortiGuard
Mitigation Strategies to limit the extent of cyber security incidents				
Essential	Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.	Medium	Low	FortiGate FortiAuthenticator \FortiClient with Fortinet Single Sign On (FSSO)

Essential	Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.	Low	Low	FortiSIEM
Essential	Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.	Medium	Low	FortiToken FortiAuthenticator FortiGate (SMS, Email) FortiSIEM
Excellent	Disable local administrator accounts or assign passphrases that are random and unique for each computer's local administrator account to prevent propagation using shared local administrator credentials.	Low	N/A	N/A
Excellent	Network segmentation. Deny network traffic between computers unless required. Constrain devices with low assurance e.g. BYOD and IoT. Restrict access to network drives and data repositories based on user duties.	Low	Low	FortiGate FortiGate WLAN / AP
Excellent	Protect authentication credentials. Remove CPassword values (MS14-025). Configure WDigest (KB2871997). Use Credential Guard. Change default passphrases. Require long complex passphrases.	Medium	Low	FortiGate FortiCache
Very good	Non-persistent virtualised sandboxed environment, denying access to important (sensitive or high-availability) data, for risky activities e.g. web browsing, and viewing untrusted Microsoft Office and PDF files.	Medium	Low	FortiGuard FortiCloud FortiCloud Sandbox
Very good	Software-based application firewall, blocking incoming network traffic that is malicious/unauthorised, and denying network traffic by default e.g. unneeded/unauthorised RDP and SMB/NetBIOS traffic.	Low	Low	FortiGate Application Control & Security Fabric FortiClient FortiGuard
Very good	Software-based application firewall, blocking outgoing network traffic that is not generated by approved/trusted programs, and denying network traffic by default.	Medium	Low	FortiGate Application Control FortiClient FortiGuard
Very good	Outbound web and email data loss prevention. Block unapproved cloud computing services. Log recipient, size and frequency of outbound emails. Block and log emails with sensitive words or data patterns.	Medium	Low	FortiGate FortiMail
Mitigation strategies to dectect cyber security incidents and respond				
Excellent	Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access and network activity.	Good	Low	FortiSIEM FortiSandbox FortiAnalyser
Very good	Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence.	Good	Low	FortiSIEM Windows Agent FortiGuard FortiGate IPS
Very good	Endpoint detection and response software on all computers to centrally log system behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry-level option.	Good	Low	FortiSIEM Windows Agent FortiClient
Very good	Hunt to discover incidents based on knowledge of adversary tradecraft. Leverage threat intelligence consisting of analysed threat data with context enabling mitigating action, not just indicators of compromise.	Good	Low	FortiSIEM FortiGuard
Limited	Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Average	Low	FortiGate IDS & IPS
Limited	Capture network traffic to and from corporate computers storing important data or considered as critical assets, and network traffic traversing the network perimeter, to perform incident detection and analysis.	Average	Low	FortiSIEM FortiGate
Mitigation strategies to recover data and system availability				
Essential	Daily backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.	Low	N/A	N/A
Very good	Business continuity and disaster recovery plans which are tested, documented and printed in hardcopy with a softcopy stored offline. Focus on the highest priority systems and data to recover.	Low	N/A	N/A
Very good	System recovery capabilities e.g. virtualisation with snapshot backups, remotely installing operating systems and applications on computers, approved enterprise mobility, and onsite vendor support contracts.	Low	Low	FortiManager
Mitigation strategy specific to preventing malicious insiders				
Very good	Personnel management e.g. ongoing vetting especially for users with privileged access, immediately disable all accounts of departing users, and remind users of their security obligations and penalties.	High	Low	FortiSIEM

FORTINET CERTIFICATIONS FOR GOVERNMENT

Fortinet is committed to Government certification requirements including Network Device Protection Profile (NDPP), Collaborative Protection Profile (cPP), ASD Crypto Evaluation (ACE), Common Criteria EAL2 and EAL4+, FIPS 140-2, Department of Defence (DoD) APL as well as other important certifications for IPv6 or ISO 9001. Fortinet invests heavily in meeting independent testing standards. The quality of our security functionality is certified by independent organisations such as ICSA Labs, NSS Labs and Virus Bulletin 100.

COMMON CRITERIA

Common Criteria evaluations involve formal rigorous analysis and testing to examine security aspects of a product or system. Extensive testing activities involve a comprehensive and formally repeatable process, confirming that the security product functions as claimed by the manufacturer. Security weaknesses and potential vulnerabilities are specifically examined during an evaluation. Fortinet products have received EAL2+ and EAL4+ certifications for FortiOS 4.3 through the Communications Security Establishment of Canada. In September 2016 FortiOS 5.2.7 achieved EAL4+ certification through the Swedish Certification Body for IT Security.

NETWORK DEVICES PROTECTION PROFILE (NDPP)

Fortinet has completed NDPP certification based on FortiOS 5.0.10 performed under the Communications Security Establishment of Canada. This certification was completed in April 2015 and is mutually recognised by ASD.

COLLABORATIVE PROTECTION PROFILE (CPP)

Fortinet has started a project with BAE Systems in Australia for the new cPP / NDPP certification based on FortiOS 5.4. At time of publication is due to be completed in Q3 2017. The cPP evaluation will include the following;

- Collaborative Protection Profile for Stateful Traffic Filter Firewalls (FWcPP), Version 1.0, 27 February 2015.
- Network Device collaborative Protection Profile (NDcPP) Extended Package - VPN Gateway, Version 2.0, 01 December 2015
- Collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS), Version 2.1, 28 January 2016.

To find out what platforms are supported go to **https://www.asd.gov.au/infosec/epl/index.php** and search for Fortinet.

ASD CRYPTO EVALUATION

In August 2013, Fortinet completed ASD's cryptographic evaluation allowing administrators to create a Virtual Private Network (VPN) between trusted networks over an untrusted network such as the Internet. During February 2017 ASD has commenced a new Cryptographic Evaluation on version 5.4 of FortiOS and this is due for completion in 2017.

OTHER GOVERNMENT CERTIFICATIONS FIPS 140-2

Fortinet products, including FortiGate, FortiAnalyzer, FortiMail and FortiClient have successfully passed FIPS 140-2 Level 1 and Level 2 evaluations. These standards focus on the security and cryptographic requirements to verify the secure design and implementation of cryptographic modules.

DEPARTMENT OF DEFENSE (DOD) APL

Unified Capabilities (UC) Approved Products List (APL) certified 18 FortiGate's for FW, VPN, IPS, IDS in August 20

INDEPENDENT CERTIFICATION

Fortinet has always been dedicated to validating the value and efficacy of our solutions through stringent third-party testing, validation and certification, adding to the company's growing list of technical credentials, which include recognition by NSS Labs, ICSA Labs, International Organization for Standardization (ISO), Department of Defense (DoD UC APL) and Federal Information Processing Standards (FIPS), among others.

Organisations today face significant challenges in battling the complicated and ever-changing cyber threat landscape and these challenges can be exacerbated by the confusing breadth of highly-marketed security solutions IT departments have to choose from in order to protect their critical assets. Fortinet have come to recognised that marketing hype is never enough to prove credibility of a security solution nor it is to be the reason for its adoption.

The Common Criteria certification extends our unrivalled certification portfolio, further showcasing our commitment to developing the best solutions on the market for helping organisations protect their most valuable assets.

■ RECOMMENDED ☐ NEUTRAL ■ CAUTION RETESTED & PASSED

Certification	Fortinet	Check Point	Cisco	Palo Alto	Juniper SRX	FireEye
NSS Labs Firewall NGFW	■	■	■ ☐	☐	☐	X
NSS Labs Data Center Firewall	■	X	X	X	X	X
NSS Labs Breach Detection System	■ ■	■	☐	■ ■	X	☐
NSS Labs WAF	■	X	X	X	X	X
NSS Labs Next Gen IPS		X	■	☐	X	X
NSS Labs Data Center IPS	■	X	X	■	■	X
BreakingPoint Resiliency Score	■	X	X	☐	X	X
ICSA Firewall	■	■	X	■	■	X
ICSA IPS	■	X	X	X	X	X
ICSA Antivirus	■	X	X	X	X	X
ICSA WAF	■	X	X	X	X	X
ICSA ATD	■	X	X	■	X	X
VB100 Virus	■	■	X	X	X	X
VBSpam	■	X	X	X	X	X
AV Comparative	■	X	X	X	X	X
Common Criteria	■	■	■	■	■	■
FIPS	■	■	■	■	■	■
UNH USGv6/IPv6	■	■	■	■	■	X

FORTIFYING SECURITY – THREAT INTELLIGENCE

LOCAL INTELLIGENCE

Fortinet Security Fabric sensors collect real-time threat information from both Fortinet and third-party security and network devices, correlate and analyse that data, and utilise advanced sandbox technologies to discover sophisticated and zero-day threats. The Fortinet Security Fabric then distributes that intelligence to every security device deployed across the distributed network, while simultaneously pushing that information out to Fortinet's global threat intelligence network.

GLOBAL INTELLIGENCE

The global intelligence element supporting Fortinet Security Fabric is delivered from FortiGuard Labs, a threat research and analysis agency consisting of more than 200 security researchers and analysts stationed around the world. These security researchers and analyst operate in an environment equipped with state of the art in-house developed tools and technology, combined with data collected from about three million sensors that is deployed around the world, to study, discover, and protect against new and evolving threats.

INFORMATION SHARING AND INDUSTRY PARTNERSHIPS

Cyber security is a shared responsibility. Public/private sector partnerships play a critical role in the global arms race against the increasing cyber-attacks. Security controls need to be able to digest automated threat intelligence and take action. The vast amount of threat intelligence that exists today and more coming tomorrow cannot be managed otherwise. Fortinet is actively directing the future of threat intelligence standards and protocols through its ongoing collaboration with global law enforcement, government and industry organisations. We partner with the world's largest technology providers and global organisations including NATO, CTA, Interpol, etc. to extend Fortinet's Security Fabric across a broad ecosystem so that our customers are protected now and into the future.

ADDRESSING THE SECURITY CHALLENGES

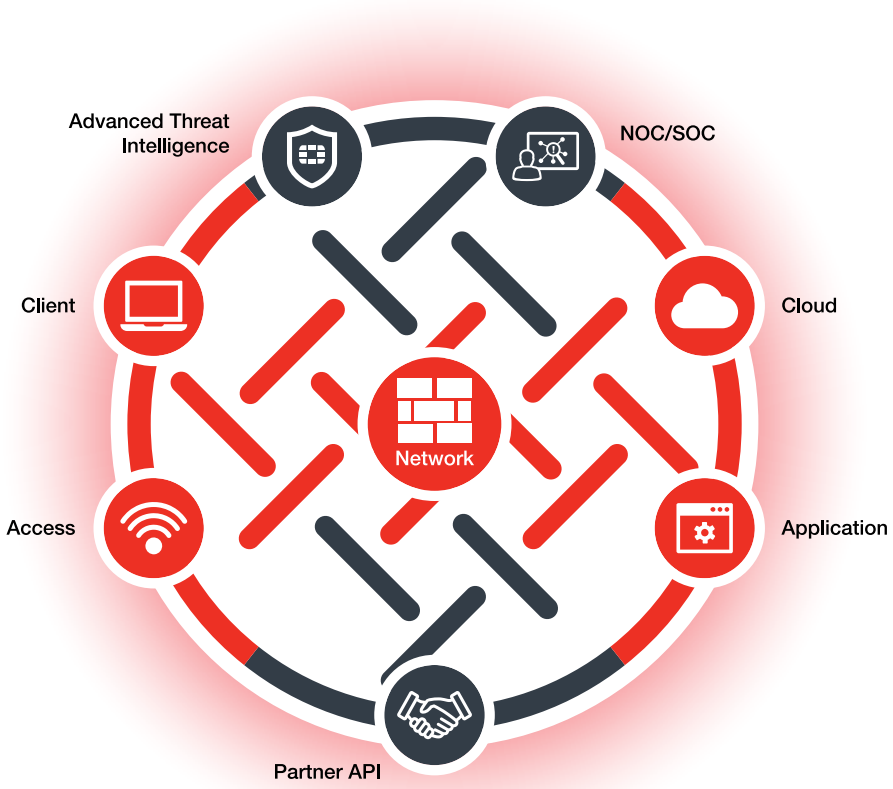
The adoption of a digital models are requiring networks to evolve rapidly, requiring applications, data, and services to flow faster across an increasingly diverse landscape of users, domains, and devices. As a result, today's networks and their related security are also increasingly borderless. IoT and cloud applications, services, and infrastructure now require organisations to worry about an attack surface that may not be visible to IT teams. The irony of this network evolution is that as we make applications, data, and services flow faster across an increasingly diverse landscape of users, devices, and domains, we are also compounding the complexity of securing this new environment against an ever-changing threat landscape.

Today, we face a huge volume of cyber threats along with highly sophisticated targeted attacks, made possible by the commercialisation of a whole ecosystem of cybercrime services and supply chain resources and services. In addition to securing themselves against these threats, organisations must also document and demonstrate the measures they are taking to meet evolving regulatory and compliance requirements. Because risk is accelerating, governing bodies all over the world are mandating risk management processes. Implementing these is an arduous task—compliance requires auditing, monitoring, and adherence—and the complexity of these processes is compounded as the network becomes more and more distributed.

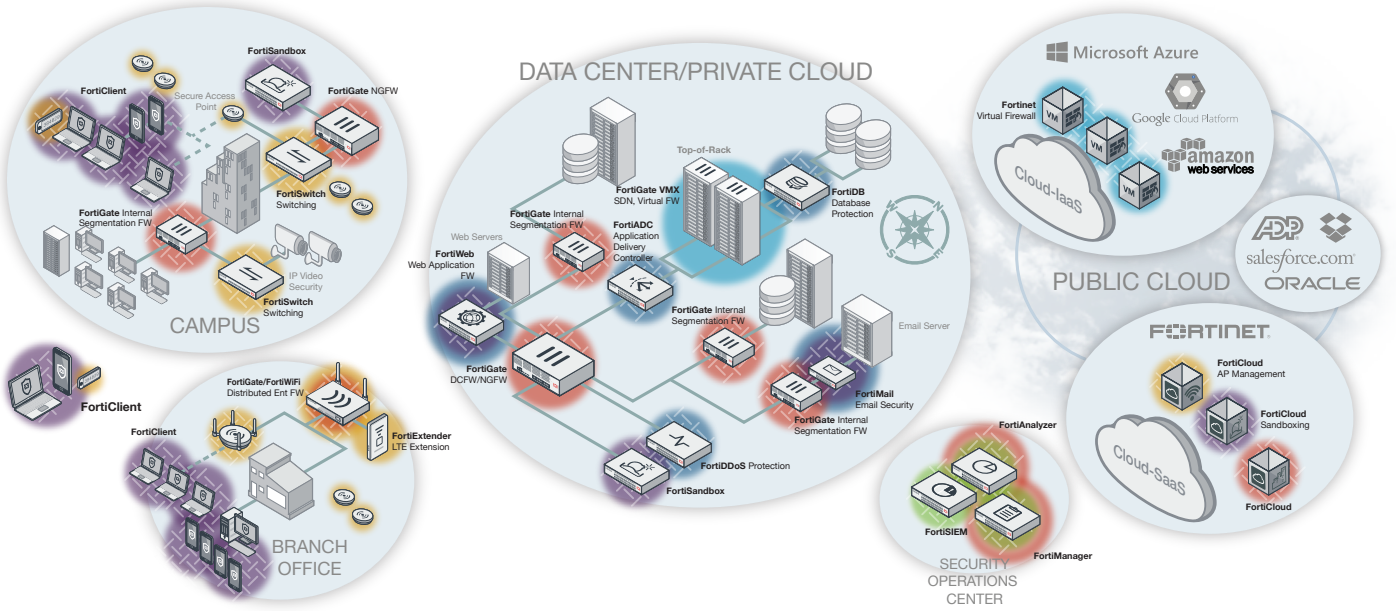
To date, the common approach has been to keep adding new security devices to an already overburdened security closet. But as the continued increase of network compromises indicates, this approach isn't solving the problem. The fact is that while the new devices you are buying and deploying are helping to decrease the time it takes to discover some new threats, data shows that threats are compromising organisations even faster. You just can't keep up using this approach. Silo security solutions, with separate management interfaces and no meaningful way to gather and share threat information with other devices on your network, are only marginally useful in addressing these threats.

FORTINET SECURITY FABRIC – BROAD, POWERFUL & AUTOMATED

What if the data and security elements across all of an organisation's various environments could be well-integrated, cohesive, and coherent, like a seamlessly woven fabric? Such an approach would allow companies to see, control, integrate, and manage the security of their data across their entire organisation, even into the cloud, enabling a secure digital business model. Such an approach would also allow security to dynamically expand and adapt as more and more workloads and data are added, and at the same time, seamlessly follow and protect data, users, and applications as they move back and forth between IoT and smart devices, borderless networks, and cloud-based environments. The Fortinet Security Fabric provides a collaborative, coordinated and intelligent approach to security that enables enterprises to weave together all of their discrete security solutions into an integrated whole, delivering security without any compromise on performance.



FORTINET SECURITY SOLUTION SUITE



Broad Complementary Solution Portfolio

Enterprise Firewalls—The Fortinet Security Fabric's core foundation is built on Fortinet's Enterprise Firewalls—for branch, campus, data center, and internal segmentation deployment—all interconnected by a single, unified operating system for simplified and coordinated deployment and control. This architecture actually delivers the benefits of standardisation claimed by many "platform" vendors. Additionally, the Enterprise Firewall solution allows segmentation of network elements, enforcing traffic, device, and data separation for stronger control.

Cloud Security— With the Fortinet Security Fabric, security can be deployed in private, hybrid and public cloud environments. Coupled with Fortinet's Cloud Security, existing enterprise firewall as well as the same intelligence and dynamic risk mitigation to applications can be seamlessly extended to the cloud, located either in the cloud or on premise.

ASD has awarded ASD Certification to a number of cloud providers. This Certified Cloud Services List (CCSL) was updated in March 2017 and now includes both Unclassified DLM and Protected classification providers. Fortinet alliance partners within this list include Amazon Web Services, Microsoft, Macquarie Telecom, Vault Systems and Sliced Tech. To find out more, go to **https://asd.gov.au/infosec/irap/certified_clouds.htm**

Fortinet's Advanced Threat Protection solution delivers the ability to detect and mitigate previously unknown threats, sharing global and local intelligence across security elements in the Security Fabric. They are designed to work together to automatically and continuously hand off data from one to the next to prevent, detect, and mitigate attacks across the entire network and all attack vectors.

Application Security—The Fortinet Security Fabric ensures the security and availability of your email or web-based applications that have long been favorite targets of hackers because they have been relatively easy to exploit with devastating consequences. Fortinet's application security solution delivers a complete, single-vendor solution with the proven performance and security effectiveness required to meet the increasing demands of today's applications.

Secure Access—The Fortinet Security Fabric goes well beyond just integrating security solutions. It extends the coordinated security policies to the very edge of the wired and wireless network where it is most vulnerable and often targeted.

Security Operations—Adaptive visibility and control across the Fortinet Security Fabric is a requirement for the security operations team tasked with monitoring and responding to incidents throughout the organisation. A range of tools is available to manage, monitor, and report on multiple fabric components from one place, whether they are multiple instances of the same Fortinet product, multiple Fortinet products, or multiple products across multiple vendors.

SUMMARY

Evolving organisations and its transition to digital models is one of the most challenging aspects of security today. As significant trends in computing and networking continue to drive changes across critical infrastructures, architectures, and practices, organisations are looking for innovative network security solutions to help them embrace and ride that evolution. The Fortinet Security Fabric is designed around scalable, interconnected security combined with high awareness, actionable threat intelligence, and open API standards for maximum flexibility and integration to protect even the most demanding environments. Fortinet's security technologies have earned the most independent certifications for security effectiveness and performance in the industry. When woven together, the Fortinet Security Fabric closes gaps left by legacy point products and platforms by providing the broad, powerful, and automated protections today's organisations require across their physical and virtual environments, and from endpoint to the cloud.

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 Valbonne
France
Tel: +33.4.8987.0500

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

ANZ SALES OFFICE
Level 8, 2-10 Loftus Street
Sydney NSW 2000
Australia
Tel: +61.2.8007.6000

61250 0 1 EN