



Staying safe in the digital world



**Business
Services**

Growing cyber threats in the digital era

In recent years, cyber criminals and malicious agents have stepped up their operations, with attacks growing in both frequency and sophistication. On average businesses can experience more than three attacks every single day¹. Threats range from cryptomining bots, mobile malware, ransomware, massive DDoS, social engineering and IoT hacking to cyber warfare between nations and attacks on critical national infrastructures.

Phishing techniques are becoming more sophisticated and yet many network equipment vendors are still deploying products with default passwords or vulnerabilities built in. Marry to this the difficulty of recruiting experienced cybersecurity professionals, and you have an ideal environment in which cyber threats can create business disruption.

While cybersecurity is topping the list of enterprise priorities, research has found that 60 percent of executives believe there are more emerging threats than they can currently control. Despite this, 55 percent admit their security strategy is still more reactive than proactive.²

All of this is in the face of a greatly changing degree of risk; there is simply more data that is exposed to attack, amplifying the cost of breaches. The average cost of a data breach today is \$362 million, according to the Ponemon Institute³, with a 27% probability the organization will experience another data breach in the next two years that will cost it between \$1.1 million and \$3.8 million.

A sizable portion of the increase in the cost of data breaches comes from new regulations affecting organizations worldwide. For example, the EU's GDPR will levy fines of up to €10 million or 2% of the company's global annual turnover for a breach of personal data – and this is only for the first offence. For a second offence, the fine will double to up to €20 million or 4% of turnover.

Poorly-managed digital risk causes real harm



Maersk: \$300 million costs from NotPetya attack



UK National Health Service: 19,494 appointments cancelled



Equifax: 23 lawsuits from data breaches



Saint-Gobain: NotPetya losses could be as high as €330 million



Contents

Growing cyber threats in the digital era	2
Ever-changing IT landscape	3
The evolving firewall	3
Why managed security services?	4
Changing the security mindset	5
Next steps	6
Why Orange?	7

1. Fortinet estimates that in Q4 2017, it detected average of 274 attacks per business that it monitors.

2. Cognizant: The Future of IT Infrastructure

3. Ponemon Institute 2017: Cost of a data breach

Ever-changing IT landscape

Protecting the enterprise has become increasingly complex. Data and software abound at unprecedented levels, with the Internet of Things (IoT) widening the vectors of attack dramatically.

The rise of cloud and mobile working has also seen a redefinition of the network perimeter. Traditionally, network security solutions operated within a defined and limited environment, but cloud and mobility have disrupted this with many users and devices now operating outside of office locations.

In addition, today's cyber attackers are much better equipped than previously, and have the capabilities to identify and target your weak points – and with an extended network perimeter, there are more potential points of attack.

Cloud, for example, puts data beyond the traditional ring-fenced network and mobile devices push data to a host of endpoints. These encompass Wi-Fi, Bluetooth and apps which further create security risks. It all makes risk management a more complex challenge. Malware is persistent problem; almost 18,000 different malware variants were recently detected in single quarter,⁴ and this level of variation shows no sign of abating.

Beyond protection from attacks, organizations also need to have application control along with visibility of users, application and web usage. It is not sufficient to just add a protection layer because the danger can also come from within. For example, employees could leak confidential data and documents outside the organization, knowingly or not. To ensure cyber resilience, it is therefore critical to monitor and manage application and web usage.

4. Fortinet detected 17,671 unique malware variants in Q4 2017, up 19 percent in one quarter alone.

The evolving firewall

A technology upgrade is required to combat these new and diverse threats, and this includes the enterprise firewall.

A key part of enterprise security, firewalls help secure legitimate FTP or other valid external requests, while preventing unwanted connections such as malware or denial-of-service (DDoS) attacks. Firewalls also protect traffic initiated from within the network, such as internet browsing or downloading files from external sites.

Next generation firewalls (NGFW) have been developed to cope with this ever-expanding attack surface, along with the increase in encrypted traffic and ever-more sophisticated threats. NGFWs provide a more granular view of what is happening in your network and features include intrusion prevention systems (IPS) and deep packet inspection (DPI) for SSL traffic. This latter functionality is vital because an increasing amount of internet traffic is SSL encrypted, so not inspecting it leaves a major hole in cyber protection.

Other benefits include greater visibility and control, simplified management, enhanced security through detailed, real-time traffic inspection. In addition, NGFWs also offer a lower total cost of ownership due to needing fewer security appliances helping reduce capital and operating expenditure. Their effectiveness is being driven by continuous evolution and dynamic upgrades of firewall policies and configurations, all of which require time commitment and expert resources.



Why managed security services?

Although security budgets are growing, they are not keeping pace with threats. Enterprise chief security officers (CISO) and chief information officers (CIO) must balance budget allocation between managing existing security infrastructure, while investing in new technology and services to keep their security up to date and prevent business disruption.

In many cases, when looking to upgrade security infrastructure, investment is better channeled into managed services. It allows access to the latest technologies and security skills, while allowing internal staff to focus on business-critical security activities. The managed security service provider (MSSP) deploys the next generation firewall, either on site or in the cloud, and monitors and maintains the equipment. This includes assessing any compromises and updating the firewall security policy accordingly. In co-managed scenarios, enterprises have the freedom to self-configure and add new sites or users easily, although the entire service itself is managed.

Managed services also allow enterprises to access sufficient security skills. With security skills in great demand and short supply, enterprises often find it hard to hire and retain security staff. Those that are with the enterprise are typically deployed in critical strategic roles, rather than day-to-day operational management.

Ultimately selecting a managed firewall from an MSSP is a business decision not just a technical choice. Effective firewall management significantly improves the security of your day-to-day business operations. It allows you to buy a service layer that better defends critical business assets and ensures continuous uptime and availability. Additionally, it enables an OPEX-based model instead of a CAPEX one, which may be easier budget to secure, provides improved flexibility to scale and can enable a more positive financial picture.

Benefits of an end-to-end approach

- Greater visibility of services
- Consolidation of vendors
- Easier partner orchestration
- Investment efficiency
- Crisis management and remediation: qualify, contain and remediate attacks
- Access to scarce expertise

Changing the security mindset

In this new data-driven era, a new approach is required to manage risk. Traditionally protection revolved around stonewalling known risks with strong firewalls and anti-virus software, for example, in an ad hoc, passive way. Security infrastructures were built and left to do their job.

To get past security solutions that block known threats, however, attackers are continually coming up with new code, creating threats never seen before. Organizations must now predict attacks and locations and react quickly to deliver protection to the enforcement points before there is a crisis. But, despite the dramatic increase in these unknown threats, only 37 percent of organizations have a cyber-incident response plan in place.⁵

Modern cyber defense is more than choosing the right technology – it also requires a cultural shift. Threats are dynamic and inevitable, which means organizations need to continuously improve their defense lines. This goes beyond patching vulnerabilities. It requires next-generation cyber security. A proactive approach that identifies, detects and protects against threats to keep an organization's data secure.

Instead of attempting to deploy security everywhere, organizations need to place greater emphasis on their business essentials – the critical data and assets that are core to their business. This requires building different security zones with different levels of access, depending on the sensitivity of the data.

Attacks will continue to grow in terms of frequency, scale and sophistication. By taking a proactive approach your organization can predict and isolate attacks as well as minimize the attack surface. It enables you to defuse major attacks before they can cause damage and disrupt your business.

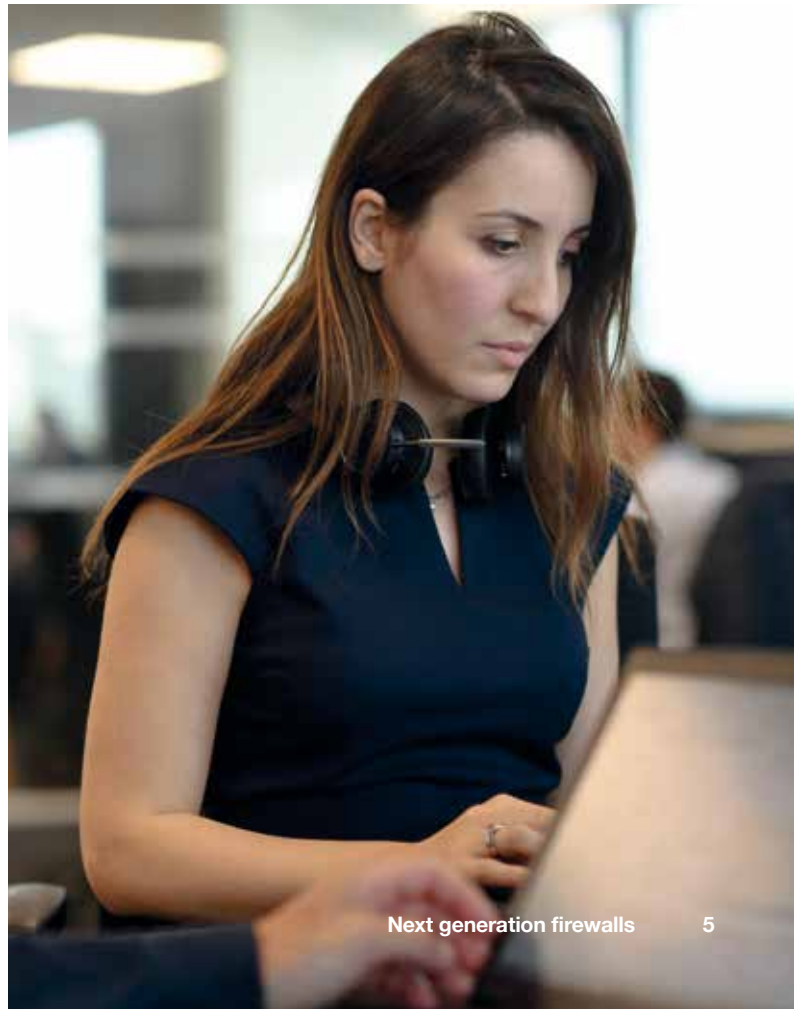
An MSSP has access to collective security threat intelligence that improves overall detection and management capabilities. This allows it to reconfigure firewall and content policies as threats evolve, ensuring continuous cyber resilience.

Focus on users

Today's workforce has an expectation that their workplace digital experience will be comparable to the experience they have in their personal lives. But despite their increasing digital sophistication, users are still often the weakest link.

Training is the key to helping mitigate this risk. For example, users need to be trained to use VPNs safely. Even simple things such as effective password management are essential in making security infrastructure more resilient.

As ever in security there is a balance to strike between being too strict and too lax on compliance with security rules and regulations. Training can help improve security practices without having to be too draconian.



Next steps

Today enterprises face greater likelihood than ever of experiencing a data breach. The ever-expanding nature of the network, cloud and IoT era makes it essential to upgrade the existing security layer for defense against the latest threats while enabling the digital enterprise. Next-generation firewalls are an essential component in upgrading enterprise security and delivering the high effectiveness and performance that you need without slowing down your business.

There are two main approaches for deployment of next-generation security services, premise-based and cloud-based. On-premise security services may provide increased control over critical data, but the advantage of cloud is that it is quick to deploy, and users can pay for only what they use. The decision between the two options depends largely on the connectivity model and the risk appetite. For example, some industries keep security management in house because of regulatory reasons.








Regarding the connectivity model, a device-based option could suit a company that operated its own data centers with a hybrid or private MPLS network better, while those that only used internet connections and cloud services could benefit more from a cloud solution. However, given that most organizations use a mix of different network infrastructure depending on their site, a hybrid cloud and on-premises approach will probably suit most.



Why Orange?

Orange offers a full range of security services, including managed and co-managed next-generation firewalls, to help you protect yourself against the new range of cyberattacks. We are the largest security services provider in France and a leader in Europe, with over 30 years' experience in securing critical infrastructure. And our position as a network provider enables us to view the first signals of a new threat.

Orange Cyberdefense in brief

-  60,000 managed devices, including firewalls and proxies
-  4 Computer Emergency Response Teams (CERT) including an Epidemiology lab
-  4 Cyber Security Operations Centers (CyberSOC)
-  3 Scrubbing Centers
-  Over 1,200 Orange Cyberdefense experts
-  720 multinational customers
-  9 Security Operations Centers (SOC)



Find out more about security services from Orange Business Services at:
<https://www.orange-business.com/en/solutions/security>



**Business
Services**

Copyright © Orange Business Services 2018. All rights reserved. Orange Business Services is a trading name of the Orange Group and is a trademark of Orange Brand Services Limited. Product information, including specifications, is subject to change without prior notice.