Security

Are you prepared for a changing threat landscape?

The cyber threat vector is getting larger, thanks to digital transformation. Integrating connectivity across businesses comes with huge benefits, including enhanced agility, performance and productivity. But it also creates more ways for cybercriminals to get in.

The sophistication and volume of today's cyberattacks demands a proactive security posture. Perimeter security is still basic security hygiene, but it needs to evolve. With millions and millions of touchpoints across the internet it is now paramount that enterprises monitor, analyze and prepare for threats coming at them from all directions. Point products and static defenses must be replaced by agile integrated and automated solutions that can perform at scale.

Cyberattacks are getting cleverer and more persistent – and this trend is not going to change. Attacks are increasingly skillful – aiming to infiltrate networks, stay hidden and siphon off data without detection.

Understanding the cyber kill chain

A "kill chain" is a term used by the military to describe the various steps in an attack. The cyber kill chain describes the different stages of a cyberattack, so they can be identified and stopped. The closer to the beginning of an intrusion an attack can be halted the better, especially as malicious actors are working overtime to get to the operational side of networks. In addition, the sooner they can be apprehended the less information they can pass on for future attacks.

Prime targets for exploitation

Microsoft may stand out as the prime software prey for cybercriminals, but it definitely isn't the only one being actively hunted. Netcore follows closely behind Microsoft in terms of attack volume. In addition, a number of web based technologies are also high on their trophy agenda, including SSL, Telnet, SHH, HTP, Bash, PHP and Apache. Wordpress. Drupal and Joomla web content management systems (CMS) also feature.

Cryptojacking: the new ransomware

Malware is evolving. It is becoming more targeted and difficult to detect. Cybercriminals are carrying out reconnaissance of organizations to maximize success rates. Cryptojacking malware, or the unauthorized use of someone's computer for mining cryptocurrency, has shown incredible diversity for such a new threat. Miners are targeting different operating systems as well as cryptocurrencies including Bitcoin and Monero and using any vulnerability they can find to weaponize themselves. They are also upping their game including creating stealthier file-less malware that can inject infected code into browsers.

Orange
Cyberdefense

28%

of enterprises observed cryptomining malware in first three months of 2018

The zero day challenge

The bounty market for vulnerabilities is maturing. This market is driven by white hats looking for new vulnerabilities to protect against possible exploits, while black hats are looking to develop zero-day attacks for their own use or sell to cyber criminals.

Zero day is an enormous challenge for organizations, trying to shore up defenses against unknown software flaws. Zero day requires an integrated approach to security that combines traditional with advanced threat protection (ATP).

The solution

Managing risk in a digital world

Moving to the cloud is a key component in any organization's digitization strategy, and this trend has completely redefined the network perimeter. Enterprises face a threat landscape that is unprecedented in size and diversity. With new threats appearing every day and attackers continually coming up with new techniques, organizations must be at the top of their game to secure their data assets.

Moving security from technology to service

Orange Cyberdefense Flexible Security Platform is our latest generation security service designed to meet the challenges of today's threat landscape. Designed to provide 360-degree visibility and control, it allows you to set up state-of-the-art security in a matter of seconds.

As a co-managed service, Orange Cyberdefense configures, deploys and maintains the service, while you retain control of day to day configuration such as policy, sizing the protected bandwidth, subscribing to options and accessing logs.

Flexible Security Platform Portal: security on demand

The co-managed web portal lets you quickly and easily access options to control security via an intuitive user interface (UI). You decide what applications or web categories your users can access. There is no need to call up a provider and wait days for security functionality to be added, and security reports can be generated in a few clicks.

Local or cloud: your choice

Flexible Security Platform Cloud is a co-managed offering using Fortinet next generation firewall virtualization technology. As an outsourced service, we take the complex management away and you keep control.

Flexible Security Platform Local uses Fortinet next generation firewall appliances at customer premises. It uses Fortinet pre-packaged security services that can be accessed and managed via the Flexible Security Platform portal. Installation, supervision and operational maintenance are all handled by Orange Cyberdefense specialist teams.

Number of unique malware exploit detections up 11 percent as attacks get more sophisticated

Business needs to proactively manage new threats by:

- Protecting applications to ensure business continuity
- Controlling the rights and access of users
- Detecting suspicious behavior early to defend information systems both on site and mobile
- Safeguarding internet usage to prevent intrusions and fulfill governance and compliance

Better security through trusted partnership

Here at Orange Cyberdefense we can provide a complete ecosystem to address every stage of your risk management cycle. We are here to anticipate, identify, protect, detect and respond.

To find more about Orange Flexible Security Platform and our wider security portfolio go to:
https://www.orange-business.com/en/solutions/security

Orange
Cyberdefense

Source: Fortinet, Threat Landscape Report, Q1 2018