A Security Fabric to Solve CISOs' Top 5 Worries
By Michael Xie, Founder, President and Chief Technology Officer, Fortinet

In my role, I meet many chief information security officers (CISOs) from around the world. You would think that hailing from such diverse environments, their concerns would be very different. In reality, however, they do not stray very far from the five issues outlined below:

1. Cloud Application Security

Cloud computing is an unstoppable trend in the enterprise. More and more employees use public cloud applications to discuss work-related topics. These applications range from email services like Gmail and public storage like Dropbox, to chatting software like Whatsapp on mobile devices.

It is becoming increasingly difficult for enterprises to block these applications altogether, so managing them and mitigating their risks is one of the most pressing tasks for CISOs.

2. Advanced Persistent Threats (APTs)

Out of the many types of security threats out there, perhaps none strikes as much fear in organizations as Advanced Persistent Threats, or APTs. There are many guises to these threats, but APTs are generally characterized by their sophistication, multi-pronged approach, stealthiest, and dogged intent to target an organization.

Often able to foil conventional defences, APTs usually target business sensitive information and personal data such as credit card details. This means all entities, from very large organizations to individuals, are in their crosshairs.

3. Event Management

Data logging, reporting, and event management have been a key part of a system administrator's job description for as long as I can remember. This age-old practice is not going away, but poised to become even more important as a big part of the defence against complex threats like APTs, and as enterprises get inundated with more network data due to trends like smart cities, the internet of things (IoT) and big data.

An indication of its importance can be seen in the growth of the security information and event management (SIEM) market, which is expected to hit US$4.54 billion by 2019 from $2.47 billion in 2014, according to research firm Markets and Markets.

To CISOs, having too much (disjointed) information is almost as bad as having no information on an attack at all. How can they make sense of the deluge of event logs collected from all kinds of network, server and security devices, and then correlate them to identify those needle in a haystack-like real threats, such as the seemingly unrelated network probing attempts that are part of an APT attack?

4. Compliance

Regulatory and industry standards like the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX) and similar local regulations are the modus operandi for commerce today.

Compliance provides a health check for businesses and instils trust in the market. But achieving compliance − and staying that way − can be costly and cumbersome. The PCI standard, for instance, involves meeting a 12-step list of requirements that cover firewall, encryption, antivirus, authentication, logging and monitoring, systems testing and more. Plus, businesses have to address new complexities with every new iteration of a standard.

I often hear CISOs lament about the sheer effort it takes to stay compliant. The time, effort, and expense spent meeting regulations can often be put to more strategic uses that reward the organization's business goals. How do CISOs break out of this conundrum?

Solving it All

Each of these four headaches point to the need for a security fabric that weaves together security hardware, software, and communication protocols with advanced internal segmentation into a single architecture to deliver seamless, comprehensive threat protection across the expanding attack surface that comes from cloud and IoT.

Cloud, in particular, must be treated like an extension of the enterprise network, and firms need to deploy a security strategy that can see and govern the vast volumes of data traversing an entire borderless network, comprising wired and wireless access points, through both public and private networks, and across traditional and cloud infrastructures.

To effectively counter **APTs**, firms will need to look beyond traditional perimeter firewalls, and even beyond conventional multi-layer defence measures.

An effective APT defence framework will require the adoption of an internal segmentation firewalling (ISFW) architecture. ISFW works by restricting malware flow between different segments of the organization. When used in conjunction with real-time threat intelligence and APT detection solutions like sandboxing and endpoint security solutions, APTs can be promptly detected and quarantined.

The other aspect to spotting an APT is a good **logging** mechanism that can capture all network traffic − both internal and external − and make sense of all the logs. Here again, a security fabric that delivers total awareness across devices, users, content, and data flowing into and out of the network, as well as insight on traffic patterns, will come in handy.

In addition, such a fabric can use a single cooperative policy, optimizing the logging process by logging each session once instead of multiple times. This makes it much easier for a log analyzer to figure out the traffic pattern and discover the real threats.

In terms of **compliance**, most CISOs follow a certain methodology (e.g. PCI, or ISO 27001/2, or NIST Cybersecurity Framework) to mitigate network risks. A security fabric, together with an ISFW deployment, allows all deployed firewalls to collectively provide a richer picture of compliance status and a security maturity assessment. This helps the CISO better understand which parts of the network are more at risk than others, and take corrective actions to address those weak points.

For the CISO, knowing what is connected to his network at any point in time is key to understanding his organization's security posture and the effectiveness of his other policies and processes. A security fabric will discover all network assets, let the administrator set up security goals, and then audit the policy on all fabric nodes to see whether the correct protection is in place for each asset.

A security fabric also goes to some extent towards addressing **the 5th concern** many CISOs have − **protecting their information security investment**.

An architecture like the proposed fabric, developed from the ground up to work with fundamental elements of the network, is inherently obsolescence proof. The individual network components can change over time, as can the nature of cyber threats, but the solid foundation laid down by the fabric will stay relevant and protect your enterprise for many years to come.

/ENDS