BIZCOMMUNITY

Stay ahead of emerging cyber threats

By Doros Hadjizenonos

8 Jul 2019

Over the past couple of decades, changes in the threat landscape have driven changes in how we design, implement and manage security. Organisations have spent the last two decades updating their security gear to keep up with the latest threats and attack vectors.

Doros Hadjizenonos, Regional Director – SADC at Fortinet

The thing these security tools tended to have in common is that they were all signature based. And because cybercriminals tend to be as invested in ROI and TCO as their victims, they learned that attacks that could be countered by a new signature were less profitable.

So, they switched their tactics.

Advanced threats and ransomware began implementing advanced strategies - such as polymorphism, multi-stage attacks, file less malware, and obfuscation techniques - that could detect and bypass signature-based solutions.

The playing field tipped strong in favour of cyber adversaries and security developers invented behavioural analytics and ATP solutions to detect zero-day attacks and identify anomalous and malicious behaviours.

That was before digital transformation, where providing consistent and timely security is once again becoming increasingly difficult to accomplish.

Adapting to the new digital world

Addressing the needs of our new digital world is going to require us to transform how and where we deploy security. That will require four things to happen:

- ### Networking and security will need to converge

  Security cannot possibly hope to be everywhere it needs to be if it has to be overlaid across every new digital environment by hand. The edges of the network are exploding with new devices, applications, and workflows, replacing the traditional perimeter while creating literally billions of new potential attack vectors. Only by weaving security deep into the infrastructure itself can security be expected to be where it needs to be when it needs to be there and to automatically adapt as the network evolves.

- ### Security will need to be much, much faster

  No one is going to tolerate slowdowns in their immersive application experience because a security component can't keep up while processing live streaming content. Keeping up will require deploying physical and virtual processors that can secure and process data at digital speeds.

- ### Security will need to be interconnected

  As data and workflows pass between devices, networks, and ecosystems, things like security policies, tags, and protocols will need to follow them across and between different networked environments, including operating natively across every major cloud platform and providing full support for the new branch and 5G edges.

- ### Finally, security will need to be smarter

  Because new applications and services are becoming more interconnected (think smart cars and cities) and applications are less tolerant of latency issues (think VR/AR and immersive, interactive solutions), security cannot afford to wait for a decision on an event to make a round trip between the sensor and some security engine in the cloud. This requires solutions that can make local and autonomous decisions in real-time.

Advanced security solutions

For security to continue to not only be effective, but actually get out ahead of the fast-moving threat landscape, a new generation of tools, such as advanced behavioural analysis, intent-based segmentation, automation, machine learning, and

artificial intelligence will need to be developed and incorporated into everyone's security strategy. This starts by automating not just detection and protection, but also predictive systems that empower prevention.

We also need to be able to teach machines to identify threats and respond in an appropriate manner. This starts with a predefined set of protocols and a pre-programmed decision tree - which is what most vendors mean when they claim to have embedded AI into their systems.

Securing today's networks requires automating the identification, detection and remediation of malicious tactics - particularly those techniques designed to evade discovery. And even more challenging, the creation of new techniques for searching beyond patterns in code and malware behaviour.

Again, Fortinet has led the way by being an early adopter of AI, which has enabled us to significantly improve the immediate detection and remediation of global threats with amazing accuracy - a task that previously required an entire team of trained researchers.

Out-innovate your adversaries

Gaining the upper hand requires more than playing catch-up with threat actors. It means developing broad, powerful, and automated solutions built around deeply integrated security tools designed not just for today's increasingly complex and distributed networks and network edge, but for the networking challenges of tomorrow.

Artificial intelligence and machine learning, especially when combined with other advanced security solutions, will be tremendous aids in this process.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet

- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...