Infopaper

Is the network the new firewall?

Konstantin Heldt
Senior Product Manager.

verizon

The sheer number of cyber attackers – and the easy access they have to state-of-the-art attack tools – has made it more likely that they'll succeed. This is why many organizations struggle to protect themselves and stay up to speed with the latest developments and trends in the security market. One of the most serious security gaps is the time it can take for organizations to become aware of a threat. And if they don't notice a threat, they can't take other steps to block it.

Growth in IoT and mobility means that signature-based approaches often fail to find critical incidents among all the new connections.

It is not a question of if you will be attacked; it's a question of when the next breach will occur, and if you can detect threats early enough and take appropriate action. In this context, it's worth asking if the network can complement current security systems and become an essential element of a modern security strategy.

Today, typical multi-layered security architectures consist of security gateway and perimeter solutions, data leak-prevention mechanisms and application-aware protection. Sophisticated companies also enforce a set of strong policies to manage content or documents, especially for classification and rights management of critical content. All these measures should be strong weapons against modern attacks, but recent developments change the picture dramatically.

Today's challenges.

The number of mobile devices as well as mobile applications has drastically increased in the past few years. In addition, devices for the Internet of Things (IoT), such as webcams, televisions and even refrigerators, are increasingly plugged into the internet. There is now a large variety of proprietary communication and security standards that add massive complexity to the task of creating common industry standards. We've already seen some of the consequences. Thousands of "dumb" IoT devices with poor security have been used to launch powerful distributed denial-of-service (DDoS) attacks on web hosting companies, Domain Name System (DNS) providers and more.

This makes it challenging for security vendors to create new solutions and additional protection. Signature-based security still dominates the market. In signature-based protection, firewalls, intrusion detection and prevention systems (IDS/IPS), or other security devices protect organizations against known bad actors or attack patterns. But with all the new device connections, most of the signature-based approaches fail to find critical incidents in the noise. Signatures simply can no longer cover the sheer variety of different standards and volume of unique malware targeting specific endpoints.

For this reason, many vendors are trying to develop new ways to uncover unknown security threats. They typically try to find the unknown by applying various filters (watchlists, customer database information, etc.), or by sandboxing potential threats.

A better solution: the network.

Modern network providers can help customers address the latest threats at a very early stage. It starts with greater visibility.

How can network providers give their customers the ability to spot potential threats in their networks? This is a crucial point since visibility ideally drives defensive strategy. First, global network providers are in a perfect position to oversee their entire backbone and also all customer connections end-to-end. They can easily extract network-related log data such as NetFlow, DNS, simple network management protocol (SNMP) or border gateway protocol (BGP) and use it for further preparation and analytics. No deep-packet inspection is really needed to find potential threats.

Pairing this capability with modern analytics engines and advanced threat intelligence, a network provider can then offer actionable intelligence. Based on its findings, the provider can also drive risk mitigation directly in the network by re-routing or explicitly blocking traffic before it reaches the customer perimeter. To avoid false positives, this requires a very deep integration between customer and provider, starting at the policy level and ending with extensive mitigation reporting.

Can the network solve all your security challenges?

The next question is how modern network threat analytics solutions interact with existing security solutions. The strength of a firewall is that it sits directly at the network border, controlling egress and ingress traffic and denying traffic when necessary. Furthermore, modern security gateways also detect malicious behavior on all layers based on signatures. In combination with a well-tuned security information and event management (SIEM) engine, you can build a pretty good picture of what's happening in and outside of your network. So what does an additional layer of security sitting on the network add to this equation that makes it worthwhile?

There are several good arguments that support this strategy. As noted earlier, signature-based approaches can't keep up with today's security demands. So traditional security solutions are becoming less and less effective. Security in the network offers its own, additional benefits.

The quality of threat intelligence and effectiveness of detection engines are key to the success of the network-driven analytics approach.

A network provider has the visibility needed to spot malicious or suspicious behavior already in the network. In other words, a provider can see threats before they reach the firewall. Additionally, the provider controls all of the backbone's ingress and egress points and possesses all the log data you need to feed an analytics service – NetFlow, SNMP, DNS and BGP.

Ingesting this data and analyzing it using high-quality threat intelligence and advanced detection engines takes security protection to a new level. If the network provider can prioritize meaningful findings and make the findings actionable for the customer, this becomes a truly valuable solution on top of your existing security analytics.

Network analytics done right.

Threat intelligence powers the detection of known bad actors or attack patterns. The quality of the threat intelligence is key to the success of the network-driven analytics approach. Low-quality intelligence more often than not leads to false positives and outdated findings.

Possibly more important is the quality and effectiveness of the detection engines finding the unknown behavior. Once normal behavior is determined using profiling or baselining of traffic, these engines use anomaly detection to look for deviation from norms and find unknowns.

How can we classify known and unknown behavior?

- "Knowns" can be detected using up-to-date signatures from security devices or threat intel providers.
- "Known unknowns" are unexpected behaviors that fit into known patterns.
- "Unknown unknowns" are the residual rest. These may simply indicate network misconfigurations or insufficiencies, but they could also indicate false positives or the next zero-day attack.

To better understand these unknowns, you need a combination of human intelligence and predictive analytics. In the future, artificial intelligence will also play a vital role in this task. In fact, it will be interesting to see what role human intelligence ends up playing in discovering unknown threats. But for now at least, human intelligence is vital to analyzing network traffic anomalies.

After analyzing network traffic and creating findings, network providers can provide that threat information through traditional security operations offerings or by feeding the actionable intelligence directly into their customer's SIEM solutions.

The next logical step will be network providers preventing or mitigating attacks by either re-routing traffic in the case of DDoS attacks or blocking malicious traffic directly on edge routers. When network providers can do this reliably and work closely enough with their customers to reduce false positives, would we finally be looking at a true and genuine clean-pipe solution?

In the future, artificial intelligence will play an ever-increasing role in finding unknown threats.

verizon

A combination designed to defeat modern attacks.

Finally, we come back to the question: Is the network the new firewall? Certainly modern network analytics and threat mitigation services are capable of providing high visibility into potential threats before they hit your firewall. And network providers can even offer the impressive ability to mitigate attacks already in the network, thus helping prevent you from being attacked in the first place. On the other hand, firewalls and other security devices will continue to play an important role in protecting your network and in filtering ingress and egress traffic as well as content.

Advanced network analytics are not a silver bullet. Instead, they must play a role alongside existing perimeter and in-house analytics capabilities. This will create a complementary security architecture that allows organizations to better cope with modern attacks. The network may not be the new firewall, but it will be the firewall's best ally in keeping your environment secure.

Contact Us.

Learn how you can make network analytics a part of your security solution. Contact your account manager or visit:
verizonenterprise.com/products/security

verizon

WP16913 2/17