IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Sponsored by: NETSCOUT

Network security tools must become "smarter" to detect the latest emerging threats. This IDC Technology Spotlight looks at the need for a network-based threat intelligence and detection solution.

Work Smarter, Not Harder: Incorporating Threat Intelligence into Security Architecture

April 2019

Written by: Christopher Rodriguez, Research Manager, Cybersecurity Products

Introduction

The digital transformation (DX) era presents tremendous new opportunities for business innovation and differentiation. Information technologies are reshaping industries around the world. However, this transformation also increases the cybersecurity attack surface.

In response, a slew of new security products has emerged in recent years such as endpoint detection and response (EDR), user and entity behavior analytics (UEBA), sandbox, artificial intelligence (AI), and microsegmentation. These solutions will continue to evolve, change, and mature — a trend that exacerbates the challenge of preparing for future security requirements. One constant remains: "The network" remains an important security control point available to IT organizations.

AT A GLANCE

KEY STATS

- The worldwide datacenter network equipment market will grow at an 8% CAGR during the 2017–2022 forecast period.
- Attacks targeting stateful perimeter protection devices jumped from 16% in 2017 to 31 % in 2018.

KEY TAKEAWAYS

Organizations should incorporate continuous threat intelligence into stateless network perimeter enforcements to complement stateful components of the security stack.

The network, as the connective tissue that enables authorized users to access sensitive data and computing resources for legitimate purposes, will continue to be a top target for threat actors. Therefore, the network must also continue to play a foundational role in the enterprise cybersecurity architecture. This technological lodestar provides much-needed consistency in the cybersecurity planning process.

The security team is tasked with the immense challenges of closing security gaps and predicting possible techniques that attackers might use to gain illicit access. Network security tools are a necessary requirement to perform these tasks, with the stipulation that they have a minimal impact on legitimate users or business activities. The challenges are compounded by the growing demands on the network from DX trends including video, "big data," and the Internet of Things (IoT). For example, in ***Worldwide Datacenter Network Forecast, 2018–2022***, IDC forecasts a compound annual growth rate (CAGR) of 8% from 2017 to 2022 for the worldwide datacenter network equipment market and notes that "given the growth of public and private clouds, and the continued proliferation of video and other bandwidth-intensive applications, there will be an ever-expanding need for more speed in datacenter networks." Under these requirements for accuracy and efficiency, network security technologies must become smarter. Security solutions cannot alert on what they do not know. High-quality threat intelligence is a key missing ingredient.

Definitions

- **Unified threat management (UTM):** UTM security products include many security features in one device. For a product to be considered a UTM appliance, it must have the ability to perform network firewalling, network intrusion detection and prevention, and gateway antivirus. All these functions must exist in the appliance, but not all the capabilities need to be utilized. UTM appliances may include other networking features in addition to those required to be in this category.
- **Threat intelligence gateway (TIG):** A TIG is an appliance or software designed for network-based deployment to automatically identify and block known indicators of compromise (IOCs), including malicious URLs and command-and-control servers.
- **Intrusion detection and prevention (IDP):** IDP products provide continuous monitoring of the network as well as report or react to malicious activities. They compare current activity with a list of known signatures to identify threats and utilize protocol analysis, anomaly, behavioral, or heuristics to discover unauthorized network activity. IDP products could also use other detection methods.
- **Distributed denial-of-service (DDoS) mitigation:** The DDoS mitigation market includes solutions that detect as well as mitigate DDoS or DoS attacks. While DDoS defense features can exist in firewalls, IDP products, and other security products, this market considers only dedicated products targeted at DDoS prevention. Such products can be on-premise or through the cloud — or a hybrid of the two.

Benefits

The limitations of current network perimeter security solutions provide ample opportunity for threat actors to penetrate and siphon off valuable customer data, intellectual property, and other sensitive information. An intelligence-based approach to shore up perimeter-based cyberdefenses offers benefits in terms of security efficacy and network performance.

Security Intelligence Enables Bidirectional Network Defense

Threat actors continually update tactics and procedures, inventing and reinventing ingenious new methods of subverting established security practices and evading detection tools. The most innovative and sophisticated threat actors are rare; however, the threat landscape features many copycats. The upshot of this pattern is that an effective network defense is possible but requires ongoing dedication to threat research and security intelligence.

Threat intelligence provides a valuable first layer of defense, checking for known threats attempting to penetrate the corporate network. However, utilizing the network perimeter as a bidirectional threat intelligence–based checkpoint effectively doubles the opportunities to detect threats and related suspicious network activities. Bidirectional network detection can identify threat actors as they attempt to extract data, establish command and control channels, or download additional malware. A bidirectional detection approach avoids the limitations of a traditional "preventive only" security strategy and promotes a "continuous detection" model.

Enriched Threat Intelligence Provides Context and Prevents False Positives

Contextual threat intelligence provides a necessary frontline protection layer and reduces false positives. IDP solutions on their own lack the context necessary to identify all threats, relying primarily on signatures or anomaly detection. Unfortunately, signatures attempt to apply a static approach to a dynamic threat landscape, and anomalies are unreliable indicators of security events. IDP solutions that rely solely on signatures or anomaly detection are susceptible to false positives and may be vulnerable to evasion techniques.

A network-based threat intelligence and detection solution is differentiated from an IDP solution by its ability to deliver high-quality threat intelligence, including accurate IOCs and contextual data, which security teams can use to make decisions and act. In terms of "accuracy," network-based threat intelligence and detection solutions are designed to deliver IOCs that are curated, validated, and thoroughly researched to improve accuracy and deliver intelligence with a high level of confidence.

Similarly, "contextual information" provides a holistic understanding of suspicious activities, including the ability to correlate IOCs and related events. Enriched intelligence offered in a network-based threat intelligence and detection solution is valuable for immediate action such as blocking as well as more involved efforts such as threat hunting. To achieve this benefit, the solution must integrate with the full security stack and third-party threat intelligence sources. It also must support threat intelligence formats such as STIX and TAXII.

Overcoming Performance Limitations in Stateful UTM Solutions and Next-Generation Firewalls

UTM solutions are expected to perform a range of functions, including stateful packet filtering, IDP, web filtering, and sandboxing. Convergence of multiple security technologies into a common platform is welcome, where possible. However, these platforms are constrained by limited computing resources. The ability to use the full suite of security protections featured in a UTM solution can diminish network throughput significantly — some estimates indicate that enabling the full suite of UTM protections can reduce network throughput by well over 50%. An intelligence-based network defense system must be stateless, thereby preventing an impact on network performance. For example, a stateless threat intelligence and detection solution can detect reputation-based IOCs more efficiently than a stateful firewall or UTM solution.

Additionally, despite the versatility of UTM solutions, DDoS is one type of attack for which firewalls and IDP solutions are ill-equipped. These devices are vulnerable to state exhaustion attacks and often end up becoming the target of a DDoS attack. According to IDC's ***DDoS Protection Is Now a Necessity and Still Growing: U.S. DDoS Prevention Survey, 2018***, 55% of respondents reported experiencing state exhaustion DDoS attacks in the past year. State exhaustion DDoS attacks can be used to knock down IDP systems and firewalls, resulting in network problems or a perilous lack of network protection.

Trends

Modern threat actors are highly motivated and continue to find innovative methods to subvert network defenses, which forces a gradual evolution in network security architecture. A network-based threat intelligence and detection solution is a missing piece of the cybersecurity puzzle that helps advance emerging security technologies and practices.

Multivector and "Smokescreen" Attacks

Multivector attacks often involve the use of multiple DDoS attack techniques in combination for greater effect, or a DDoS attack in combination with other attempts at data theft or network intrusion. According to IDC's *U.S. DDoS Prevention Survey,* 44% of respondents reported a multivector attack in the past year. Multivector DDoS attacks targeting infrastructure may disable firewalls or IDP systems, and targeted organizations may be defenseless against other intrusion attacks and data theft.

A similar concept, the "smokescreen" attack is difficult to quantify but represents a high-risk threat. This tactic uses a DDoS attack to draw attention away from standard security practices. During a DDoS attack, responders may be distracted and not notice unusual activities or security alerts. Additionally, DDoS attacks tend to be highly visible, and they can signal to other would-be attackers that an organization under DDoS siege is a vulnerable target. As a result, the risks associated with a DDoS attack are often underestimated. The lesson: Security programs cannot afford to compartmentalize security threats as "unrelated" events.

East-West Detection

DX has contributed to the erosion of the traditional network perimeter. IT organizations are supplementing perimeter-based network protection with the use of internal network segmentation and lateral (east-west) threat detection. Although lateral movement may be frequent, threat actors must eventually pass the perimeter (north-south) either to enter the network or to extract data. Therefore, while "east-west" detection is a recommended supplemental security practice, bidirectional "north-south" network perimeter protection remains a foundational requirement.

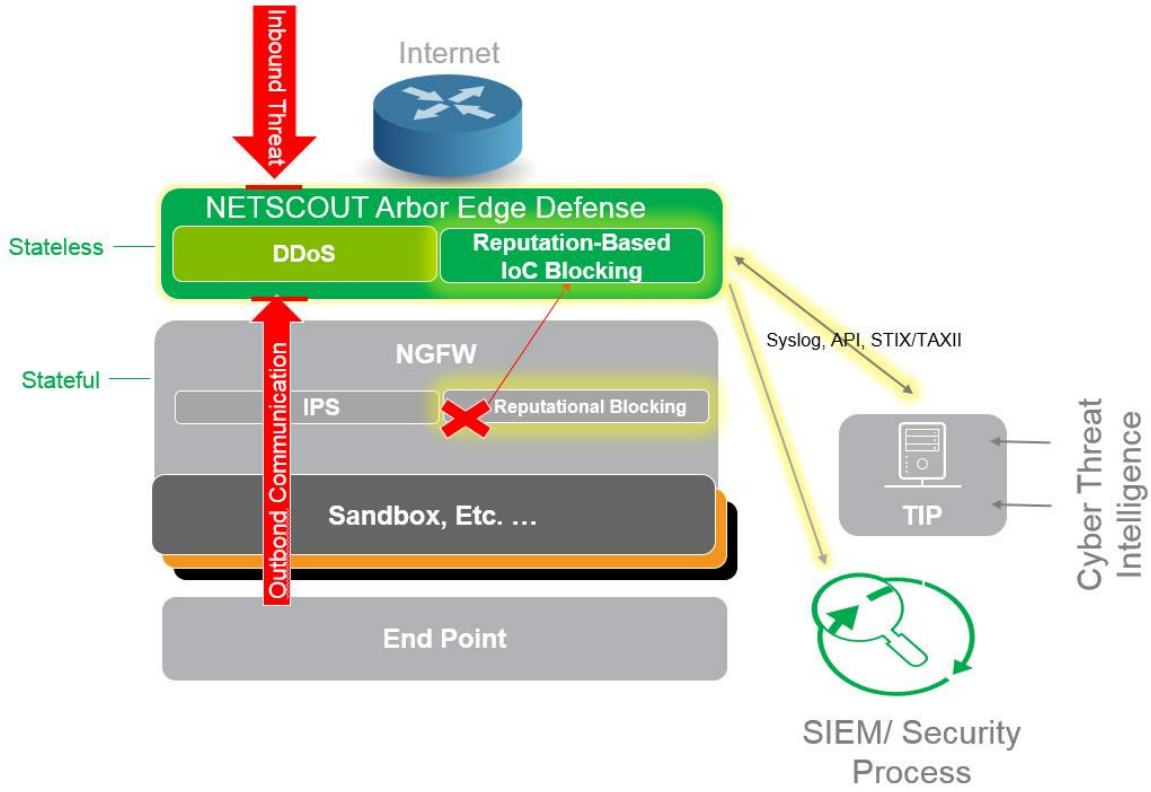
Analytics and AI

AI is a popular new technology emerging in the security industry. Although AI is proving to be far more than smoke and mirrors, the technology is still maturing. AI promises to be a tremendous addition to the security toolbox, but it will not replace all the tools and is not intended to be a replacement for the "tool user" either. A mature understanding of best practices for AI security technologies is vital to prevent overreliance and inflated expectations. Simply put, AI can be a useful predictive technology, but until full technological maturity, AI must be backed up by hard threat intelligence.

Considering NETSCOUT Arbor Edge Defense

NETSCOUT Arbor Edge Defense presents a useful example of a network-based threat intelligence and detection solution. It provides stateless protection for the network edge based on contextual, curated security intelligence. Deployed in between the internet router and firewall, NETSCOUT Arbor Edge Defense protects both inbound and outbound traffic, blocking pernicious threats such as scanners, loaders, remote access trojans (RATs), and advanced threats, in addition to application layer DDoS attacks (see Figure 1).

Figure 1: ***NETSCOUT Arbor Edge Defense***



Source: NETSCOUT, 2019

The NETSCOUT Arbor Edge Defense solution is supported by the ATLAS Intelligence Feed service, which provides analytics, IOCs, and additional contextual data. This contextual security intelligence has been vetted by the ATLAS Security Engineering & Response Team (ASERT) for accuracy and actionability. After blocking IOCs, Arbor Edge Defense delivers additional information, such as malware hash values, domain names, and IP addresses, to enable security teams to better understand the threat in full context and arm the teams with information that they can use with other security tools in their environment — with the goal of stopping the data breach from occurring.

This curated contextual threat intelligence, along with scalable stateless protection, provides the option to deploy the solution in blocking mode with low false positives. Importantly, the solution integrates within the security stack, including integration with security information and event management (SIEM) solutions (via Syslog CEF and LEEF formats) and third-party IOC sources via REST APIs, as well as support for STIX and TAXII threat information formats.

Challenges

For enterprises facing a vast number of threats and an equally expanding number of security solutions, new products can be a difficult addition for already strained security budgets. The NETSCOUT Arbor Edge Defense solution comes with additional costs, although they are minimized for existing NETSCOUT customers.

The NETSCOUT and Arbor Networks brands are known for DDoS mitigation. Over the years, NETSCOUT's ASERT has accumulated a large database about a variety of cyberthreats beyond DDoS, gathering information about advanced threats and threat actors, tactics, and procedures. However, NETSCOUT will have to educate customers about its abilities to detect malware.

In addition, NETSCOUT Arbor Edge Defense represents a combination of TIG and IDP products. This solution defies categorization, which may require the company to provide additional customer education.

Conclusion

DX is changing the nature of IT and networking while introducing cybersecurity challenges along the way. And yet, conventional wisdom still applies: The network is a top target for attackers and the quintessential security control point.

The DX era has included hard-learned lessons as well: It is a matter not of "if" but of "when" an attacker will test any given network's defenses. Naturally, the next question is: How long will it take for customers to detect these activities — minutes, hours, days, or months?

Security solutions cannot alert on what they do not know. High-quality threat intelligence is a key missing ingredient.

Network security is an ongoing, never-ending process, requiring dedication and diligence. Unfortunately, these efforts alone will not suffice. Security tools must become "smarter" to detect the latest emerging threats. The value of contextual threat intelligence enforced at a stateless network perimeter becomes of greater importance to enable the security at scale required to operate online while minimizing threats.

MESSAGE FROM THE SPONSOR

Stateless Technology Complements and Scales Security at Network Perimeter

Though a vital component of the network security stack, the Next Generation Firewall (NGFW) has expanded beyond its original use case, is struggling to perform and is a target for TCP-state exhaustion DDoS attacks.

Deployed in between the Internet router and NGFW, NETSCOUT Arbor Edge Defense is a stateless packet processing solution which enforces threat intelligence at the network edge to detect and block:

- All types of inbound DDoS attacks (e.g., TCP state exhaustion attacks) to protect availability of stateful devices like NGFWs
- Inbound reputation-based IoCs, which takes pressure off downstream stateful devices like NGFWs
- Outbound communication to known bad sites that have been missed by other components in the security stack

To learn more about NETSCOUT Arbor Edge Defense and how its stateless technology can complement and scale security at the network perimeter, visit our website at: ***https://www.netscout.com/products/netscout-aed***

About the analyst:

Christopher Rodriguez, *Research Manager, Cybersecurity Products*

Chris Rodriguez is a Research Manager in IDC's Cybersecurity product research group focused on the products designed to secure today's complex enterprise networks. IDC's cybersecurity research offerings to which Chris contributes include Endpoint Security; Network Security Products and Strategies; Security Analytics, Intelligence, Response, and Orchestration (Security AIRO); and Identity and Access Management research programs.

IDC Custom Solutions

IDC Corporate USA
5 Speen Street
Framingham, MA 01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com