White Paper

Securing the Evolving Enterprise Network—Inside and Out

By Jon Oltsik, Senior Principal Analyst; and Jack Poller, Analyst

April 2017

This ESG White Paper was commissioned by Hewlett Packard Enterprise and is distributed under license from ESG.

Contents

Executive Summary

Network security can be an intimidating discipline for most organizations. The threat landscape is becoming increasingly dangerous, as malicious actors focus their energy on developing sophisticated, targeted attacks. At the same time, the anywhere, anytime mobile workforce, digital workplace transformation, IoT applications, and the move to the cloud are increasing the size and complexity of IT infrastructures and their associated attack surfaces.

What is the state of network security today and what can be done to improve it? This paper concludes:

- **New business objectives are making network security more difficult.** ESG research reveals that most organizations believe network security is getting more complex every year. Why? More on-premises and cloud applications, devices, users, and network traffic are increasing the attack surface, making it increasingly difficult to prevent, detect, and respond to security incidents. The persistent cybersecurity skills shortage and ever-increasing sophistication and volume of threats and targeted attacks also compound the challenge.

- **CISOs must think in terms of "closed-loop" network security.** Given the growing complexities of the network, security executives must focus on improving threat prevention, detection AND response. This goal can be facilitated through a closed-loop approach to network security. This strategy includes:

  - **Complete visibility of all devices connected to the network.** IT needs to continuously monitor the network to provide the security team with an up-to-date inventory of every device and user on the network.

  - **Granular network access policies governing who gets access to network assets (i.e., users and devices).** With policy management, network access policies can be centrally enforced for all wired and wireless connections regardless of location, user, or device type. Applying the principle of least privilege, granular policies can ensure that access is granted to the minimum number of necessary resources. This helps to mitigate risk and reduces the attack surface as each device or user connects.

  - **Strong network security controls for policy enforcement.** Network security policies must be enforced through tight integration between network access control and other security technologies, such as threat intelligence, endpoint management, IDS/IPSs, and firewalls, as well as network infrastructure, such as switches, routers, and wireless access points. Working together, all of these technologies can be used to develop and enforce security policies while providing the ability for policy adjustments based upon changing threats and vulnerabilities.

  - **User and entity behavior analytics (UEBA) to monitor for post-connection suspicious/malicious behavior emanating from users and devices.** UEBA technology can be applied to help security analysts detect suspicious behavior or patterns of anomalies after connections have been established. UEBA can also be used to process the millions of log entries generated by every device on the network, contextualize and enrich security telemetry, prioritize events, and greatly reduce false positives.

The Changing Cybersecurity Landscape

Most information security professionals would readily admit that they are engaged in a persistent cyber-war that puts their organizations under a constant barrage of attacks often based upon 0-day malware that easily circumvents signature-based security controls. Facing persistent cyber-adversaries is a difficult challenge. According to ESG research, 79% of IT

and cybersecurity professionals believe that network security (i.e., network security administration, operations, monitoring, etc.) had become more difficult between 2012 and 2014.[1]

Network security has become more difficult because of:

- **An explosion in the number of users, devices, and traffic.** The proliferation of laptops, smartphones, IoT devices, and the ubiquity of network connectivity has enabled the anywhere, anytime mobile workforce, but has also made network security increasingly difficult. In fact, 36% of cybersecurity professionals said in 2014 that it was the increase in the number of overall devices with access to the network that made network security more complex, while 29% said that it was specifically the number of mobile devices with access to the network that made network security more difficult.[2] More devices, more users, and more traffic make it harder to apply security controls, monitor traffic, and respond to incidents. These increases in users, devices, and network traffic also make it more difficult to prevent, detect, and respond to insider attacks by malicious or careless credentialed users.

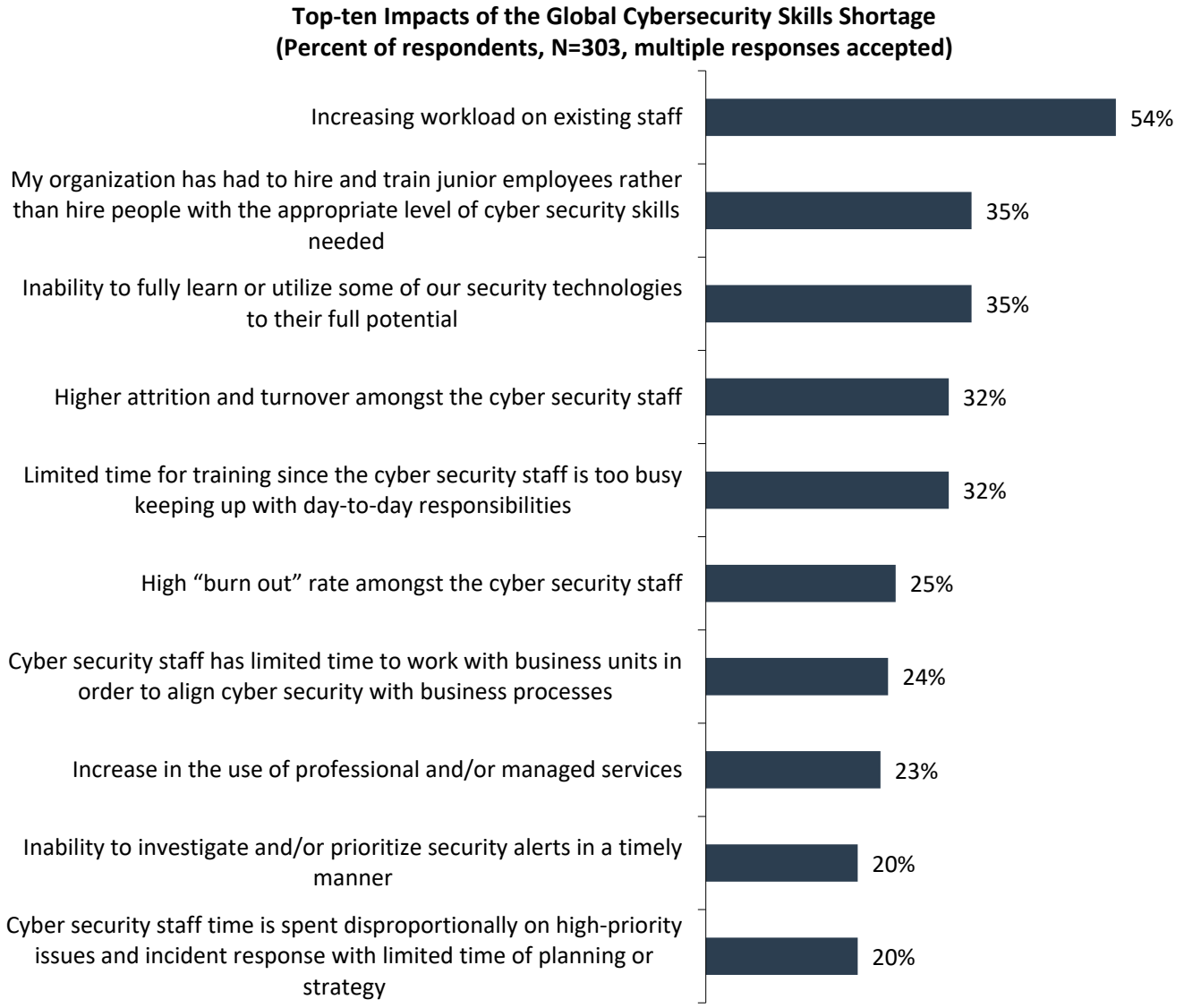
- **Disparate security policies, controls, and technologies.** Thirty one percent of respondents said that one of their biggest network security challenges is the fact that network security policies and controls are not cohesive, as they must be implemented across many different security and networking technologies.[3] This is especially true as organizations embrace the mobile workforce and transition to cloud services. The externalization of IT blurs the boundaries between what is considered inside or outside of the corporate network, and forces internal network security controls to extend to the cloud.

Digital transformation. The use of technology to radically improve the performance and reach of enterprises brings new types of applications with new security issues. IoT applications, though immature today, will arguably have the most impact on network security. IoT devices typically have limited security features, forcing most security controls to be implemented at the network layer. In fact, one of the largest known distributed denial of service (DDoS) attacks was executed by the Mirai botnet in late 2016. Comprised of more than 100,000 security cameras and other IoT devices, the botnet generated sustained attack traffic exceeding 1 Tbps. Network security teams face the daunting task of protecting their networks from such attacks while simultaneously ensuring that their own deployed masses of IoT devices do not get compromised. Organizations are trying to cope with these changes while operating within the constraints posed by the global cybersecurity skills shortage. According to ESG research, 45% of organizations report that they have a problematic shortage of cybersecurity skills.[4]

In a separate survey of cybersecurity professionals, 54% reported that the cybersecurity skills shortage increased their workload, 35% said the shortage led to an inability to fully learn or utilize security technologies to their full potential, and 32% reported higher attrition and turnover (see Figure 1).[5]

[1] Source: ESG Research Report, *Network Security Trends in the Era of Cloud and Mobile Computing*, August 2014.
[2] Source: Ibid.
[3] Source: Ibid.
[4] Source: ESG Brief, *2017 Cybersecurity Spending Trends*, March 2017.
[5] Source: ESG/ISSA Research Report, *Through the Eyes of Cyber Security Professionals: Annual Research Report (Part II)*, December 2016.

Figure 1. Top-ten Impacts of the Global Cybersecurity Skills Shortage



Source: Enterprise Strategy Group, 2017

What's Needed? "Closed-loop" Network Security

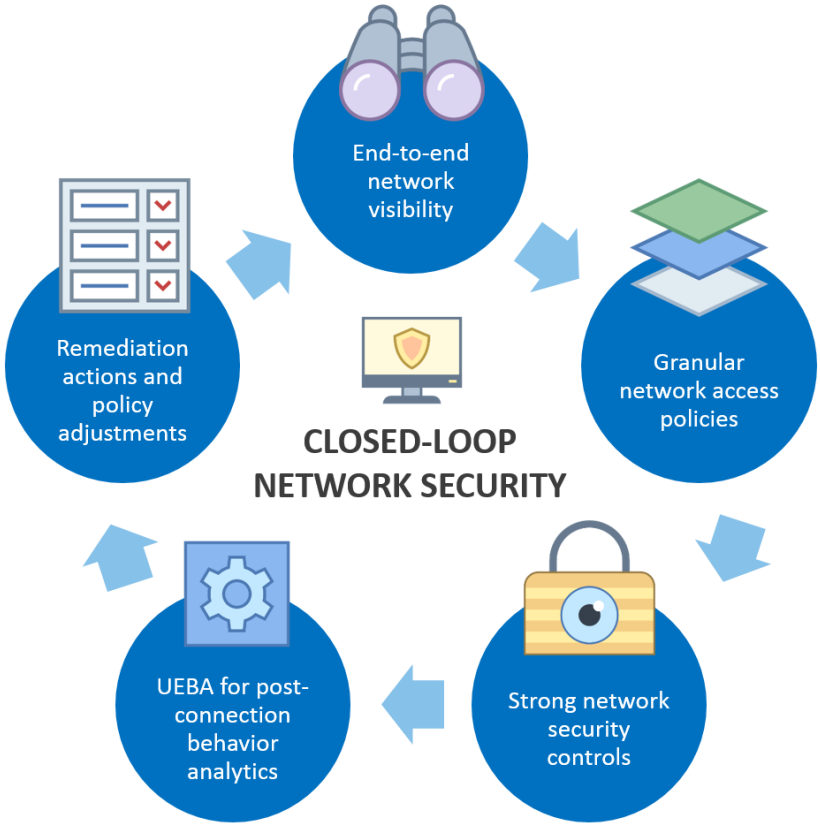
Enterprise IT is evolving, with digital transformation, IoT, the cloud, and the mobile workforce driving an explosion in the volume and variety of devices, all of which are connected to the network. ESG research indicates that these new IT initiatives are pushing existing network security policies and controls to a breaking point, greatly increasing complexity and IT risk. This unacceptable situation must be addressed as soon as possible.

To address the scale and scope of IT initiatives and digital transformation, CISOs must adopt a "closed-loop" approach to network security by (see Figure 2):

- Starting with a comprehensive visibility into all devices. Every user and every device on every network must be identified and classified, as you can't control what you can't see. Once devices are identified, network access controls should include services such as user and device authentication and authorization. A device that is profiled as a printer

should not suddenly appear to act like a server and be left on the network. Likewise, that printer should not be communicating with an external website located in Bulgaria, without a change in authorization privileges.

Figure 2. Closed-loop Network Security



Source: Enterprise Strategy Group, 2017

- Establishing granular policies. Traditional security policies were mostly binary, denying or allowing access to the network for users with an unmanaged or managed device. Binary policies are no longer sufficient to capture the complexity of today's business networks, which include access for non-employees, as well as IoT devices like telephones, manufacturing robots, cameras, or drones. Policies must be expanded to include more refined and granular controls, taking into consideration user and device classification, business processes, identity attributes, and changes in IT risk. Devices should follow the rule of least privilege by being granted access to the minimum resources necessary. For example, a computer-controlled valve on the manufacturing floor should only have access to the programmable logic controller (PLC) controlling the valve. Should that valve suddenly exhibit anomalous behavior, such as scanning the network, the network access control policy can be used to limit visibility and the potential for damage.

- Adjusting security policies and controls with risk-based, real-time security. The threat landscape is always evolving as malicious actors attempt to overcome the latest security systems and develop exploits for new and existing applications. Security teams should adjust their policies immediately based on new intelligence that reveals security holes in their environments. For example, access policies should be adjusted when new critical software vulnerabilities are announced and threat intelligence indicates that cyber-adversaries have developed exploit kits targeting these weaknesses.

- Maintaining continuous network monitoring. Today's enterprise IT environment is extremely dynamic. Users, devices, configurations, threats, and vulnerabilities are in a perpetual state of flux, driving the need for continuous monitoring to gather real-time knowledge of the state of the network. Monitoring should cover devices, device profiles, and device behavior, such as the connections established by these devices, and the network communications taking place. User behavior, such as failed and successful logins and times, the systems that are accessed, and from where, should also be monitored.

- Implementing UEBA capabilities to detect and respond to post-connection security events. While organizations have traditionally focused on external threats, the risk to the business from internal threats is growing. User identities can be compromised by malware, phishing emails, and social engineering, enabling malicious actors to gain access to the network. Furthermore, malicious and/or negligent credentialed users can wreak havoc on the network. Critical company information, financial data, customer and supplier contacts, and other proprietary information can be stolen by malicious employees. This is where UEBA can play a central role. UEBA systems based upon artificial intelligence (AI) and machine learning (ML) systems apply algorithms and statistical analyses to detect meaningful anomalies from the behavior profiled by continuous network monitoring. AI and ML systems can be used to look across multiple systems for related events, identifying, correlating, and consolidating patterns of anomalies or suspicious behavior. This helps organizations move from hundreds or thousands of individual security alerts to aggregated suspicious cases composed of multiple and related anomalous events. UEBA is especially effective when combined with policy-driven network access controls. When UEBA detects an attack in progress, it can coordinate and modify network access controls to quarantine a device or send it to a remediation VLAN. This combination effectively closes the security loop by enhancing threat and breach detection while automating a proportional real-time response for remediation.

Finally, effective and timely network security policies require tight integration between security tools such as threat intelligence, network access controls, user and device identification and authentication systems, IDS/IPSs, firewalls, and behavior analytics solutions. The entire security infrastructure can then translate business-centric policies such as "only accounting employees and executive staff can access the financial accounting systems" into updated routes, firewall rules, ACLs, and policies that are then enforced and monitored at any time. Networks have long been dependent on things like distributed management and static security controls, which have proven to be antithetical to the strong security necessary with today's dynamic enterprise network environments. What's needed? A single system to manage all security policies across all wired and wireless networks, devices, and users, defining which users and devices have access to which networks and network resources.

By following the steps outlined above, organizations can get the benefits of a closed loop: knowing all assets connected to the network, establishing trusted network connections, enforcing least privileged connections, fine tuning security policies and controls based upon risk factors, and leveraging intelligent analytics to identify and prioritize the most critical security incidents. From a business perspective, this translates into IT resiliency.

Enter Aruba, a Hewlett Packard Enterprise Company

To security professionals, Aruba is often thought of as a leading provider of wireless networking, acquired by HPE in 2015. This is a rather narrow perspective, however, as Aruba's portfolio also includes all of the elements needed for closed-loop network security, including:

- Centralized policy management and enforcement across wired and wireless networks. Aruba ClearPass is a template-based policy management and enforcement system. Security teams can develop policies with an extensive and granular parameter set such as user roles, device types, MDM/EMM attributes (mobile device management / enterprise mobility management), certificate status, location, and time of day. Organizations can create policies for employees, executives, guests, IoT devices, and other groups. These policies can control who has access to specific

resources and ensure that only certain types of devices with up-to-date software are allowed.

ClearPass extends beyond a system of record into a system of engagement used directly by employees. ClearPass Onboard provides a self-service portal for users to configure and provision their own devices for access to the secure network without involving IT or security teams. Security policies control the types of devices allowed, the users allowed to onboard new devices, and the policies that can be applied to newly onboarded devices.

- Extending centralized policy management to IoT applications. Many IoT devices have limited processing power and memory, and are unable to directly enforce security policies. Aruba's Connect-and-Protect methodology moves policy enforcement for these devices to a point on the network as close to the device as possible. For example, the network access switch used by the device can be used to enforce network ingress access policies while coordinating with other technologies for network segmentation. In this way, organizations can add security to their IoT applications while maintaining the benefits of centralized policy management.

- Integration into a broader security architecture. ClearPass Exchange provides standard and micro-service interfaces to exchange information between ClearPass and other security systems. Network access controls can be dynamically updated based on changing risk information from threat intelligence. ClearPass can incorporate external data, such as device jailbreak status from MDM/EMM tools, or user authentication and authorization from MFA and directory services, in policy definitions. A SIEM or other tool can use network events, such as multiple login attempts, to trigger an action, such as moving the user to a partitioned, protected network with limited access, until the user successfully authenticates with a multi-factor authentication (MFA) tool. Users can benefit from simple password authentication until there is an issue, when they are promoted to more secure MFA, and the automation can provide the security team with additional confidence in the user identity.

- Continuous monitoring and visibility. ClearPass Insight can provide visibility into login and authentication events to help security teams monitor connection activity, such as the number of failed logins throughout the day or during a large event. Detailed reporting can also provide insights into user behavior that may also present security risks, such as users not updating down-rev software or using unwanted peer-to-peer applications on enterprise networks.

- UEBA—combined with comprehensive network access policy management and enforcement. From sensors to systems to users, attacks on the inside require a new security approach. Fortunately, innovative security solutions using machine learning-based analytics and big data platforms can now provide enterprises with a new dimension of protection that traditional security products lack.

  HPE recently acquired Niara to integrate into the Aruba security portfolio and its User and Entity Behavior Analytics (UEBA) solution that uses supervised and unsupervised machine learning to automatically baseline user and device behavior while actively looking for anomalous activity that may indicate a threat. When the Aruba UEBA is integrated with Aruba ClearPass, the combined solution delivers three key security innovations: advanced attack detection, accelerated investigation, and automated, policy-based enforcement. With these capabilities, compromised or malicious users or systems participating in attacks or IoT devices conscripted into a latent botnet army can be discovered and remediated before damage is done to an organization's infrastructure, assets, or reputation.

In aggregate, the Aruba network security portfolio can help any organization address the scale and scope of digital transformation with tighter access controls and more effective incident detection and response. Furthermore, Aruba network access policies and controls integrate into the existing network security infrastructure, improving its efficacy in the process.

CISOs looking to improve security efficacy and operational efficiency while supporting new business initiatives would be wise to investigate how Aruba can help.

The Bigger Truth

Today's IT infrastructure, featuring a mobile workforce, IoT applications, digital transformations of the business, and the cloud, is evolving at a pace that's exceeding the capabilities of legacy security approaches. Network security has proven to be insufficient, lacking the visibility, control, and intelligence necessary to keep up with changing needs. Organizations and their infrastructures are left exposed to a dangerous threat landscape where persistent cyber-attackers have proven adept at bypassing aging security mechanisms.

To shrink an organization's attack surface and reduce potential avenues of compromise, cybersecurity should look to improve network visibility and enforcement capabilities. After all, it's impossible to protect users and their devices when you don't know who they are, what they've connected to, and what they allowed to do.

Enterprises can use thorough and up-to-date user and device data to take actions aimed at reducing the attack surface by applying the principle of least privilege, and developing granular access policies that ensure access is granted to the minimum resources necessary. Security teams need to be able to update policies to reflect changes in behavior that have been detected through continuous monitoring, regardless of user or device type.

With the ever-present cybersecurity skills shortage, enterprises need to supplement security staff, leveraging emerging technologies such as artificial intelligence and machine learning to offload human analytics while accelerating threat detection and response.

Given the need for network visibility, tight access controls, continuous monitoring, and real-time security policy flexibility, ESG believes that Aruba's expanding portfolio of integrated security solutions, including integrated network discovery and monitoring, centralized policy management, and user and entity behavior analytics, can act as a comprehensive platform for addressing evolving network security requirements.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188