SOLUTION OVERVIEW

PONEMON SURVEY

INTRODUCTION

In many ways, the IT security gap is old news, but its size and complexity are growing rapidly. Brazen, well-funded and highly skilled criminals, nations and other attackers continue to breach company and government networks to steal sensitive information, disrupt business operations or sow the seeds of societal unrest. Coupled with an increasingly mobile user experience, cloud solutions and IoT access to IT networks, building a cyber defense is also more challenging.

To understand what makes the IT security gap so difficult to close, the Ponemon Institute partnered with Aruba, a Hewlett Packard Enterprise company, to survey 3,866 IT and IT security practitioners in Asia-Pacific, EMEA and North America. The goal was to understand what's behind the gaps in IT security programs that diminish an organization's ability to identify, detect, contain and resolve data breaches and security incidents. The research also explored what types of technologies and processes security teams are using to deal with this new threat landscape.

As is outlined below, the study, entitled "How AI and Automation Can Close the IT Security Gap in the Era of IoT," highlights the current thinking around security teams' lack of visibility and control into the activity of users and devices and how they expect to deal with these challenges.

The data is contained in a report supporting the study and can be found at https://connect.arubanetworks.com/ponemonsecurityreport. This paper provides an overview of the results and how Aruba solutions help close the security gap.

The Ponemon Institute exclusively focuses on surveying the global security community on a wide variety of topics, much of which is sponsored by F500 companies. Given the Ponemon Institute's stellar security credentials and global reach (a database of over 100,000 across all verticals and sizes of organizations), their survey results are both comprehensive and relevant.

ISSUE 1: SECURITY GAPS

OBJECTIVE FOR THE TOPIC

Better understand what is top of mind for security professionals in terms of threats and corresponding exposure.

KEY CONCLUSIONS

- Top factors the survey identified that cause security gaps include:
  - Expanding attack surface (BYOD, IoT, etc.)
  - Security skills shortage
  - Security teams lack visibility and controls into the activity of users and devices connected to their organizations' IT infrastructures
  - Attackers are persistent and well-financed
- Compromised users, negligent users and IoT devices are top three insider risks

THE ARUBA SOLUTION

The Aruba 360 Secure Fabric is a security framework that gives security and IT teams an integrated set of solutions to achieve the required visibility and control. The components of the fabric use machine learning to detect slowly-gestating attacks that have eluded traditional defenses, while proactively responding to these advanced cyberattacks across any network infrastructure. Aruba security solutions are open and integrate with over 140 technology partners from both the security and broader IT ecosystem.

ISSUE 2: AI/MACHINE LEARNING

OBJECTIVE OF THE TOPIC

Determine the level of interest in security AI-based technology and the projected level of adoption

KEY CONCLUSIONS

- The majority of survey respondents agree that AI/machine learning (ML) is essential to detect attacks on the inside before they do damage
- When asked about the value of AI/ML
  - 68% say ML will help reduce false positives
  - 63% cited increased effectiveness of the security team
  - 60% envisioned more efficient investigations
  - 56% anticipated that they could find stealthy attacks using AI/ML technology
- 25% currently use some form of AI/ML for security and another 26% plan to implement in the next 12 months

THE ARUBA SOLUTION

It is clear that security professionals believe AI/ML is viable and they are counting on the technology to help them deal with emerging threats. Aruba IntroSpect User and Network Behavior Analytics (UEBA) aggregates and analyzes network traffic, flows, logs and alerts with supervised and unsupervised machine learning to detect attacks on the inside before they do damage and to accelerate incident investigations and attack remediation.

ISSUE 3: VISIBILITY AND ACCESS CONTROL

OBJECTIVE OF THE TOPIC

Focus on the importance of user and device visibility and the role that network access control plays in an organization's overall security strategy.

KEY CONCLUSIONS

- Visibility is a critical factor in detecting attacks from the inside. A large majority of survey respondents said visibility is critical to detecting attacks
- 63% percent of respondents highlighted the importance of network traffic visibility
- Over half said that Network Access Control (NAC) provides network visibility and was a key component of their overall security strategy
- Over half deploy NAC today for visibility
- 52% say NAC is a key solution for both wired and wireless networks

THE ARUBA SOLUTION

Role-based network access control for both wired and wireless access is one of the key functions of Aruba ClearPass. With over 8,000 customers from small organizations to global enterprises, ClearPass not only simplifies the problem of controlling who and what can access IT resources, but also provides device discovery and profiling—which is particularly important for organizations that need visibility for what is connected to their network. As the network gatekeeper, ClearPass can also be used for attack remediation based on pre-configured policies that can be invoked either manually or automatically.

ISSUE 4: IOT SECURITY

OBJECTIVE OF THE TOPIC

IoT security is a very relevant and hot topic and the survey questions were designed to better understand both the perceived challenges of IoT security as well as how the respondents expected to deal with those challenges.

KEY CONCLUSIONS

- Less than one quarter of the survey respondents believe IoT devices to be secure
- 2/3rd's say they have little or no ability to secure IoT
- 60% believe even simple "things" pose a threat
- When asked for preferred approaches to secure IoT devices, they listed:
  - Continuous monitoring of network traffic
  - Network Access Control
  - Closed-loop detection and response
  - Peer group/anomaly detection
- When asked who in the organization is responsible for IoT security, responses ranged from the CIO, CISO, CTO to the line of business. The top answer was CIO at 33% and no other organization registered above 20%, with "No function" coming in third at 15%.

THE ARUBA SOLUTION

These survey responses clearly demonstrate that IoT security is a top of mind issue, that it is recognized to be a pervasive problem, difficult to solve and not yet settled organizationally in terms of who is responsible. Clearly, "things" do not log, cannot be scanned and will not support an agent. The only way to determine if a device has been compromised is to monitor its network traffic. The combination of ClearPass and IntroSpect delivers a security solution that is particularly tuned to IoT. ClearPass does the device discovery and profiling and traffic segmentation. IntroSpect provides the continuous monitoring based on network traffic visibility, and ClearPass can quarantine or block a device if IntroSpect determines that it is compromised.

ISSUE 5: AUTOMATION

OBJECTIVE OF THE TOPIC

Security automation is a topic that has recently gained attention as security teams struggle with advanced attacks and staffing shortages. The questions around automation are intended to understand where automation is likely to occur and in what areas.

KEY CONCLUSIONS

- Security automation benefits cited within the survey include:
  - Reduce time to investigate alerts
  - Find attacks before they do damage
  - Improve coordination between security and network teams
- Likely places to automate
  - Attack containment and remediation
  - Alert investigation

THE ARUBA SOLUTION

Several years ago, security teams were reluctant to use technology to short cut the attack detection and response workflow. Now, it is clear that security teams are looking to compensate for staffing shortages and a complex threat environment by automating. As noted above, the power of ClearPass as the "network gatekeeper" now becomes important both for network admission as well as attack response. In addition, the forensic data aggregation and machine learning-assisted threat hunting and investigation can dramatically reduce the time and effort to diagnose an attack and formulate a response.

ARUBA WORKS TO CLOSE THE GAP FOR YOU

Aruba continues to innovate to close the IT security gap, enabling businesses, schools and government organizations to protect their sensitive data and operations from the rising tide of successful attacks. With a secure foundation, complete visibility and control, and AI-powered threat detection and investigation, organizations can gain better protection with fewer resources.

GO DEEPER

Read the Ponemon Institute research report, "How AI and Automation Can Close the IT Security Gap in the era of IoT".

To learn more about Aruba's enterprise network security solutions, visit https://www.arubanetworks.com/products/security/.

aruba
a Hewlett Packard
Enterprise company