NETSCOUT

I WHITE PAPER I

A Double-Edged Sword

As Enterprise Networks Increasingly Move to The Edge, CIOs and CISOs Have To Address Security, Customer Experience

SECURITY

TABLE OF CONTENTS

Workforce Shift Drives Security and IT Updates

Today's enterprises continue to adjust IT and security resources in response to changes wrought by the pandemic. Regardless of when the pandemic finally ends, enterprises are now faced with the reality that 65 percent of pandemic-era remote workers want to continue working from home – and 58 percent say they will look for a new job if their company requires returning to the office.

As enterprise security and IT teams continue to grapple with changes in the network necessary to support remote access, they increasingly turn to the edge to do so. Edge computing provides a common abstraction across a range of local and remote IT assets in order to support next-generation security and management technology. Moving resources to the edge enables data to be more quickly processed, analyzed, filtered and stored, reducing both network latency and operational expense.

By the end of 2022, it's estimated that 90 percent of enterprises will employ edge computing, shifting information processing and content collection closer to the sources and users of that information. But for all of the benefits that edge computing creates for enterprises, it also opens them to new security risks.

With more devices connected to the internet and performing compute actions, attackers have an expanded threat landscape that includes access to sensitive data and access to other systems. The expanded landscape includes devices that are part of the Internet of Things (IoT). By 2025, it's estimated that there will be 55.7 billion connected devices worldwide, giving attackers an unprecedented number of additional attack vectors. Overall, the number of applications, devices and connections enabled by edge computing will require a scale that is 10 to 100 times the size of today's deployments.

As enterprises have had to expand services and rely more heavily on the edge, attackers have expanded the threat landscape, as well as the size and scope of their attacks. In the first half of 2021, attackers launched 5.4 million distributed denial of service (DDoS) attacks, an 11 percent increase from the same period a year earlier.

It's no surprise, then, that security concerns are on the minds of enterprise IT and security teams that are relying upon the edge. In a survey of 268 IT execs, 55 percent said edge devices were not built with security in mind, and 69 percent said network security has already been or will be affected as a result of edge computing.

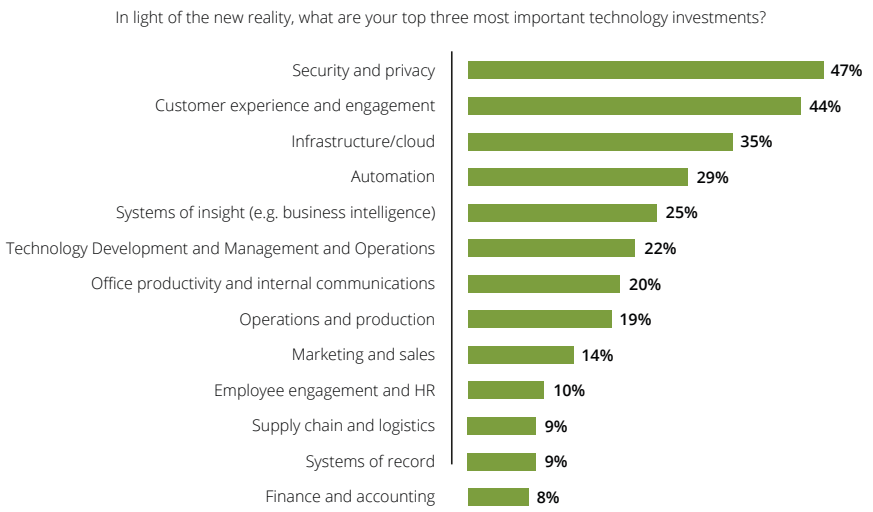

Figure 1: Responses to question on Top 3 Most important technology investments.

The biggest concerns are the expanded attack surface and greater exposure to threats like DDoS campaigns, data theft and intrusions into the enterprise network. When asked to identify the most important technology investment to address changes the pandemic has wrought, almost half of CIOs chose security and privacy (47 percent), followed by customer experience and engagement at 44 percent (Figure 1).

As more action is moved to the edge, it's important for CIOs and CISOs to ensure their teams understand the challenges of securing the edge, while also ensuring that end-user experience doesn't suffer from the policies and procedures put into place to do so.

Impact of Edge on CIOs & CISOs

The call for better collaboration, communication and consistency between security and IT teams is not a new one. But explosive growth in cyberattacks since the beginning of the pandemic have added additional pressure, especially given that 41 percent of enterprise CIOs say they experienced additional incidents as a result of supporting remote access.

Now more than ever, it's vital for security and network operations teams to have consistent goals, unified processes and interoperable technologies that protect the network, while also maintaining network uptime and performance for business operations. Doing so reduces costs through shared instrumentation, training, and operational efficiencies.

Other challenges that must be addressed to protect the edge include:

- **Control tool sprawl:** Almost 30 percent of CIOs say it's difficult to get an accurate status of network security because networking and security teams maintain separate tools and reports. Security teams largely view network security through network traffic analysis (NTA) and network detection and response (NDR) tools, while networking teams use various tools to manage devices, traffic flows, and network performance. These divergent views of network reality invariably create situations in which each group is missing data and details necessary for keeping the network running at peak performance. While security and network operations teams need to collaborate in areas like threat detection and response, 44 percent of organizations say it doesn't happen because the teams use different tools and data as their sources of truth.

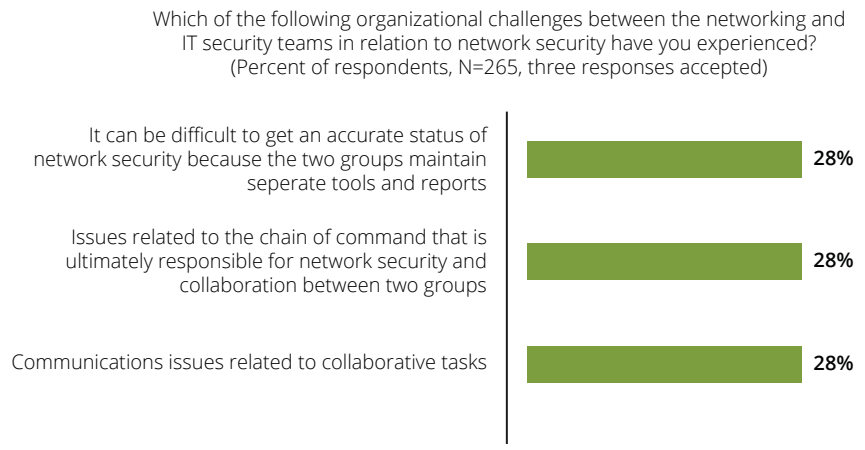

Figure 2: Respondents identify Top Organizational Challenges between networking and IT security teams related to their company's network security.

Focus On Healthcare

The healthcare market is one of the fastest growing users of IoT devices, as hospitals, care providers, insurance companies and others in the healthcare ecosystem embrace remote monitoring to improve patient outcomes and drive down costs. The healthcare IoT vertical is expected to expand at a compound annual growth rate of 20 percent, increasing in value to $534 billion by 2025.

One western U.S. healthcare system supports more than 20 hospitals and 150 clinics, as well as thousands of patients, and more than 40,000 physicians, nurses, clinicians, and staff. The pandemic created a number of challenges related to security risks in relation to their IoT devices. NetOps and SecOps teams had to work together to reduce the threats and investigate potential incidents of compromise related to distributed IoT devices, including smart phones, tablets, carts on wheels (COWs), and smart beds.

The healthcare system primarily depended on networked packet traffic as its preferred source of data intelligence to secure IoT devices. As such, the IT team needed ways to share data between both the IoT security tool and their service assurance solution. The tool selected for IoT security leveraged packet data, as well as network taps placed in strategic segments throughout data centers, hospitals, and medical buildings. These simultaneously feed the appropriate packet data downstream for performance management and cybersecurity analysis of IoT devices.

Not only did this reduce the risk of cyber threats, it improved device safety and availability. Likewise, it enabled the healthcare system to consolidate vendors and tools for network and application service assurance solution, ultimately resulting in improvements in performance and availability of applications, services, and devices.

- **Achieve multi-cloud visibility:** Networking and security teams need network and cloud visibility to ensure strong performance, as well as to detect and respond to security incidents. Both teams need solutions that go beyond raw data capture and storage to include processing, indexing, and enriching network data. Doing so increases its usefulness for incident detection, security investigations, threat hunting, and troubleshooting disruptions.
- **Build network security without borders:** This requires a solution stack that can be used to monitor and manage the network, while also providing security. As such, security teams can use a common data repository, analytics tools, and security controls for threat prevention, detection, and response, while networking teams leverage the same data to achieve network throughput, availability, and end-to-end application performance.
- **Develop a common source of network truth:** Rather than operate different tools that collect the same network data, teams should utilize common sources of line-rate packet acquisition classification. This should go beyond raw data capture and storage to include processing, indexing, and enriching network data, which increases its usefulness for incident detection, security investigations, threat hunting and troubleshooting disruptions.
- **Combine smart edge monitoring and smart edge protection:** Stateless edge protection provides a first line of defense and stops inbound threats like DDoS attacks, probing/reconnaissance, and brute force password attempts. Additionally, it should detect and stop outbound indicators of compromise that have been missed by the cybersecurity stack. Doing so provides visibility into the edge for both performance and security.
- **Prevent known and volumetric attacks as early as possible:** Stateless protection devices should be deployed in front of stateful firewalls to help them block command and control (C2) traffic, state exhaustion DDoS attacks, known bad DNS domains, and other threats.
- **Utilize network traffic analysis:** To keep the network running smoothly and safely, security and networking teams need to understand the behavior patterns of network traffic – as well as the posture of every device connected to the network. Doing so enables the identification and remediation of rogue devices, misconfigurations, and vulnerable systems, while maintaining application performance for business operations.

RESOURCES

FlexJobs Survey Finds Employees Want Remote Work Post-Pandemic

90% of Industrial Enterprises will Utilize Edge Computing by 2022 (frost.com)

IoT Growth Demands Rethink of Long-Term Storage Strategies, says IDC

The Top Security Threats at the Edge, and How to Mitigate Them | CIO

Cyber Security & Threat Intelligence Report | NETSCOUT®

Network World 2020 State of the Network: SD-WAN, edge networking and security are hot | Network World

Harvey Nash / KPMG CIO Survey 2020: Everything changed. Or did it? (assets.kpmg)

Network Security without Borders (netscout.com)

IoT in Healthcare Market Worth $534.3 Billion By 2025 | CAGR: 19.9% (grandviewresearch.com)

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

© 2021 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor Networks, the Arbor Networks logo, ATLAS, InfiniStream, InfiniStreamNG, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.

SECCWP_026_EN-2101 12/2021