ExtraHop and SANS Institute Survey Finds Huge Gaps in Security Visibility During Large-Scale Shift to Remote Work

Two-Thirds of Organisations Have Suffered a Successful Attack in the Past 12 Months, While Almost Half Identified Employee Desktops as the Most Likely Entry Point for Cyber Criminals

SEATTLE – APRIL 21, 2020 – ExtraHop, the leader in cloud-native network detection and response, today announced the results of a SANS Institute survey, Network Visibility and Threat Detection. According to the report (https://www.extrahop.com/resources/analyst-reports/sans-network-visibility-and-threat-detection-survey) more than 64 percent of respondents reported suffering at least one successful attack within the last year, and 59 percent believe a lack of network visibility poses a high or very high risk to their operations. Perhaps most concerning in light of the recent large-scale shift to remote work, 44 percent of respondents see employee desktops as the most likely attack vector. As enterprise organisations and government agencies grapple with how to enable, manage, and secure newly distributed remote workforces, network visibility is more critical than ever as they adjust to the new IT reality. The survey exposes key gaps in enterprise security, including that 98 percent of respondents are concerned about their ability to see into encrypted traffic, while over 80 percent identified east-west traffic and network connected devices as areas of opacity. "Having visibility of every device and how they are meant to behave on your network is crucial to understanding what constitutes normal traffic and what could be considered a deviation," writes survey author Ian Reynolds. Bryce Hein, SVP of Marketing at ExtraHop, concurs. "At a time when organisations are rapidly transitioning to remote work and cloud usage is surging, network visibility has never been more critical," said Hein. "Organisations need to be able to see into east-west traffic to identify threats in the growing number of cloud workloads, as well as get visibility into which devices are accessing enterprise resources. The fewer tools, less time, and less friction required to get that visibility, the better." In addition to identifying critical gaps in network visibility, key survey findings include: - Growing complexity within the enterprise environment. Over 93 percent of respondents indicated that they manage more than a thousand endpoints, and almost 90 percent manage between hundreds to thousands of servers.

- Lack of cloud visibility affects security posture. 40 percent of respondents identified cloud-based systems as a potential entry point for malicious actors. At the same time, only 17 percent reported high visibility into their lateral communication inside their network (east–west traffic), including all cloud traffic.
- Need to reduce tool sprawl. The majority of companies use tooling from more than 10 vendors, with nearly one-fifth utilizing more than 20. 68 percent of respondents expressed a desire to reduce the complexity of their systems by reducing the overall number of tools involved in their operations. The survey also found that, while organisations want more network visibility, there are operational impediments. Lack of staff (62 percent), lack of time - including having other issues with greater importance—(51 percent) and lack of appropriate skills in the existing staff (46 percent) were the leading concerns. According to Reynolds, machine learning will play a key role in overcoming these challenges. "Choose tools that use machine learning to provide improved analytics for access to the right data in less time," he writes. "This might assist in meeting staffing concerns and provide faster resolution of unexpected behaviours, threats and incidents." To download the complete SANS Institute survey titled Network Visibility and Threat Detection, click here: https://www.extrahop.com/resources/analyst-reports/sans-network-visibility-and-threat-detection-survey/ Watch the on-demand SANS Institute Webinar on the survey here: https://www.extrahop.com/resources/webinars/cybersecurity-spending-survey/ About ExtraHop ExtraHop delivers cloud-native network detection and response to secure the hybrid enterprise. Our breakthrough approach applies advanced machine learning to cloud and network traffic to provide complete visibility, real-time threat detection, and intelligent response. With this approach, we give the world's leading enterprises including The Home Depot, Credit Suisse, Liberty Global, and Caesars Entertainment the perspective they need to rise above the noise to detect threats, ensure the availability of critical applications, and secure their investment in cloud. To experience the power of ExtraHop, explore our interactive online demo: https://www.extrahop.com/demo or connect with us on Linkedin (https://www.linkedin.com/company/extrahop-networks/) and Twitter (@ExtraHop)

Contacts

David Bass
+61 2 9922 6820
mailto: david@basspr.com.au