Enterprise Strategy Group by TechTarget

EXECUTIVE SUMMARY

MAY 2024

Organizations Seek Modern, Continuous, and Integrated Approaches to Penetration Testing to Support Business Growth

Melinda Marks, Practice Director, Cybersecurity; and Adam DeMattia, Director of Custom Research

Abstract: Penetration testing (pentesting), which launches attacks to identify where organizations have weaknesses that bad actors may exploit, is a powerful method helping security teams to identify and remediate security issues in applications and infrastructure before attackers can act. This is important for enterprises as they rapidly develop and deploy applications and services for their employees, partners, and customers that they need to keep secure against attacks. Synack, in partnership with TechTarget's Enterprise Strategy Group, recently completed research to evaluate enterprise usage of pentesting solutions and their effectiveness as organizations increasingly modernize application development processes and their IT infrastructure, including deploying applications using cloud platforms.

The research revealed that, although organizations view pentesting as a critical component of their risk and vulnerability management programs to identify and remediate security issues in their applications and infrastructure, they also face multiple challenges successfully mitigating risk and preventing security incidents with the pace of rapidly scaling attack surfaces and increasingly dynamic modern applications and infrastructure. The data shows organizations are actively looking for more modernized, continuous, and integrated approaches to pentesting that can drive increased efficiency and value to meet their needs supporting business growth.

Key Findings

- 50% of organizations find it more difficult to manage their attack surface than 12 months ago.
- Only 47% of business-critical apps and 26% of the attack surface are tested.
- 60% struggle to test frequently enough to keep pace with the rate of application development.
- 58% say detecting vulnerabilities is getting more difficult.
- 65% recognize that traditional pentesting is not a viable approach to cover their attack surface.
- 75% said it's likely they'll consider a switch to the new generation of platform-based testing solutions.

Overview

Enterprise Strategy Group completed a survey of 200 technical decision-makers responsible for their organization's investments in cybersecurity solutions and knowledgeable about their organization's current approach to pentesting. The study surveyed enterprise (i.e., 1,000 or more employees) organizations in the United States across industry verticals, including manufacturing, technology, healthcare, and retail/wholesale, among others. The research revealed that, although pentesting can identify exposure to threats, traditional testing methods and reporting cannot scale to support enterprise needs. Instead, these organizations need an approach that keeps pace with the rate of application development and that is is integrated with development, IT, and operational processes to continuously identify and efficiently remediate exploitable vulnerabilities to protect applications and assets.

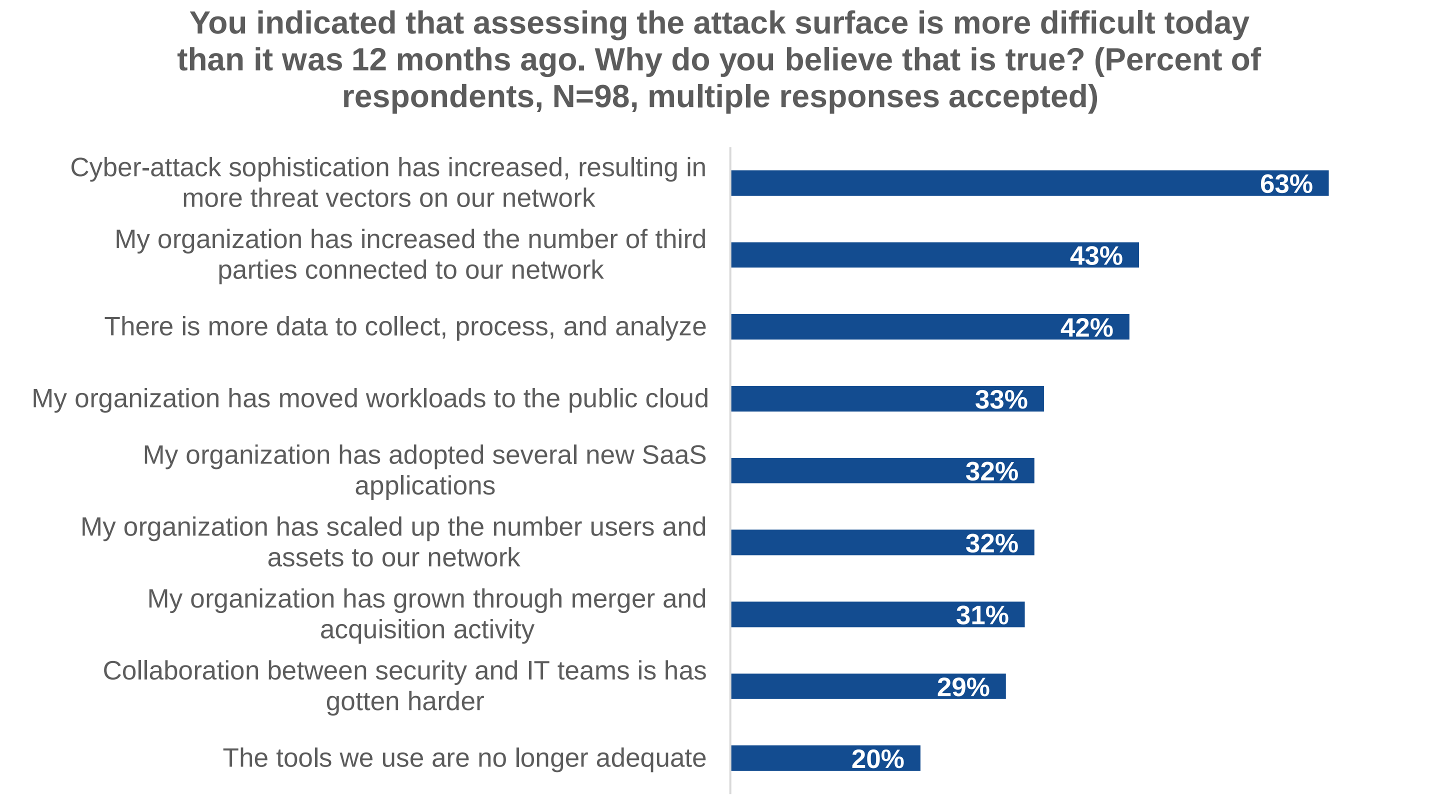
This Enterprise Strategy Group Executive Summary was commissioned by Synack and is distributed under license from TechTarget, Inc.

© 2024 TechTarget, Inc. All Rights Reserved.

Research Summary

Defending the external attack surface is getting more difficult due to increasing complexity, with 50% of organizations finding that discovering and managing their attack surface is getting more difficult than 12 months ago. This is due to factors including attacker sophistication, third-party risk, and security data complexity (see Figure 1).

Figure 1. Reasons the Attack Surface Is More Difficult to Secure



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Less than half of an organization's external attack surface and business-critical applications are being tested like an attacker would, as pentesting covers only 47% of business-critical apps and 26% of the attack surface. In addition, nearly 2 out of 3 (64%) respondents say it is challenging to align the proper testing methodology with different parts of their organization's attack surface. Meanwhile, 65% of respondents agree that traditional pentesting does not offer a viable and/or affordable approach to adequately cover their attack surface, outnumbering those that disagree by 3:1.

The complexity, size, and rate of change of an organization's attack surface create challenges for traditional pentesting approaches. Furthermore, 58% say detecting vulnerabilities is getting more difficult, with respondents saying that one of the biggest challenges their organizations face today is keeping up with the number of open vulnerabilities.

Faster development cycles also create a mismatch between the application rate of change and testing frequency, with 60% of respondents finding it difficult to test frequently enough to keep pace with application development. Moreover, organizations face challenges leveraging test results to improve security posture. 66% find pentesting reports or data difficult to operationalize into security operations processes, while 62% find them difficult to integrate into other data or reports to assess overall organizational risk.

Despite these challenges, respondents believe pentesting can drive value with risk mitigation and program improvements. Organizations have varied views on what drives their pentesting strategies and processes the most. For 31% of organizations, strategies are primarily driven by a need to remain in and prove compliance. While this use of pentesting to meet a compliance checkbox is not ideal, many organizations use it to reduce risk and improve posture, with 38% reporting that they use pentesting to tactically discover and remediate vulnerabilities and only 32% reporting that they use it to improve overall security strategies and posture. Additionally, the majority of respondents believe pentesting drives value related to risk mitigation, with 55% believing that pentesting is a best practice that helps them assess and mitigate risk, 52% believing that conducting pentesting after experiencing an incident helps them to better assess risk, and 51% saying that pentesting enables them to confidently accelerate business transformation initiatives.

Our research found that organizations are in search of more scalable alternatives to traditional pentesting approaches to overcome their challenges and support their needs, with 75% of respondents saying it's likely they'd consider a switch to the new generation of platform-based solutions, like pentesting-as-a-service (PTaaS) offerings. In comparison, 0% of respondents said it's unlikely that they'd consider this switch.

Finally, respondents expect their organization's funding level for pentesting to increase in the future and are in search of more scalable alternatives to traditional approaches. In fact, 66% plan to increase spending for third-party testing services or technologies in the next 12 months. Consequently, new platform-based pentesting solutions are poised for growth over the next 36 months, with the percentage of organizations that will be most reliant on PTaaS expected to grow 79% in the next 36 months, while traditional approaches are poised for contraction.

Conclusion

As organizations modernize and accelerate their software development processes to increase productivity, security teams need scalable ways to ensure they can secure their applications and infrastructure. The research shows that, as security teams strive to manage risk to support business needs, they see the value in pentesting, as it enables them to catch and remediate critical security vulnerabilities before an attacker can exploit them. However, with rapidly growing attack surfaces, organizations are challenged applying traditional pentesting solutions to their entire attack surfaces due to the cost and time requirements of managing ad hoc testing and reports.

The research shows that organizations seek a platform approach that offers continuous pentesting, integrated with development and reports operationalized in security operations for efficient remediation. It also shows they plan to invest in solutions that support scale and growth using pentesting as a foundational element for security program effectiveness.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

✉ contact@esg-global.com
🖥 www.esg-global.com