IDC

SPOTLIGHT

Sponsored by: Bishop Fox

With 62% of hackers reporting they can find an exploitable perimeter exposure in less than five hours, it is of paramount importance for organizations to constantly monitor their attack surface.

Continuous Prevention: How Attack Surface Management Reduces Risk

January 2023

Written by: Michelle Abraham, Research Director, Security and Trust

Introduction

Organizations know that both proactive and reactive approaches to security are necessary to a good risk posture. Using cybersecurity tooling to close gaps to prevent attacks helps reduce the number of reactions required. With 62% of hackers reporting it takes less than five hours to find an exploitable weakness in an environment, staying ahead of attackers has never been more critical because there is only a small window in which to fend off a breach.

With the expansion of the attack surface to include cloud assets, third-party connections, and organizational acquisitions, organizations need to employ continuous monitoring and testing of their external-facing assets to get the same ever-changing view a threat actor has, gaining information on how it would get in and what damage it would do.

AT A GLANCE

KEY STATS

- IDC survey respondents said that proactively addressing evolving threats is the top goal of their cybersecurity transformation efforts.
- In a survey of hackers, 62% of respondents revealed they can find an exploitable perimeter exposure in less than five hours.
- Time is of the essence since 72% of hackers surveyed said they can perform an end-to-end attack in less than a day.

Definitions

While traditional vulnerability management performs internal scans using an agent scanner or a network scanner, attack surface management (ASM) platforms scan the internet; provide an external view of an organization, which is the same scene the attacker sees; and surface weaknesses in external-facing systems of which cyberattackers could take advantage. Discovery is common across all ASM solutions to provide visibility into all internet-facing assets — both on premises and cloud, known and unknown. An ASM platform will show the valid exposures associated with the discovered systems and provide information on how an attacker could gain access to critical assets such as a customer database. Guidance is offered on how to resolve the concerns found. Once the issue has been addressed, ASM can take another look to see if the fix has remediated the problem.

Benefits of ASM

Organizations can expect the following benefits from implementing an ASM platform:

- Offers continuous understanding of the organization's security posture instead of the point in time view that comes with a penetration test
- Provides a proactive solution to help bolster the organization's security defenses by helping it understand holes and gaps that allow attackers entry
- Promotes cyberhygiene by finding unknown or forgotten assets and systems that could unknowingly create exposures so they can be decommissioned or secured
- Validates the exposures and determines the impact on the business (Vulnerabilities with low CVE scores may still present a high risk to the business.)
- Guides the security team on how to fix and then validates the remediation

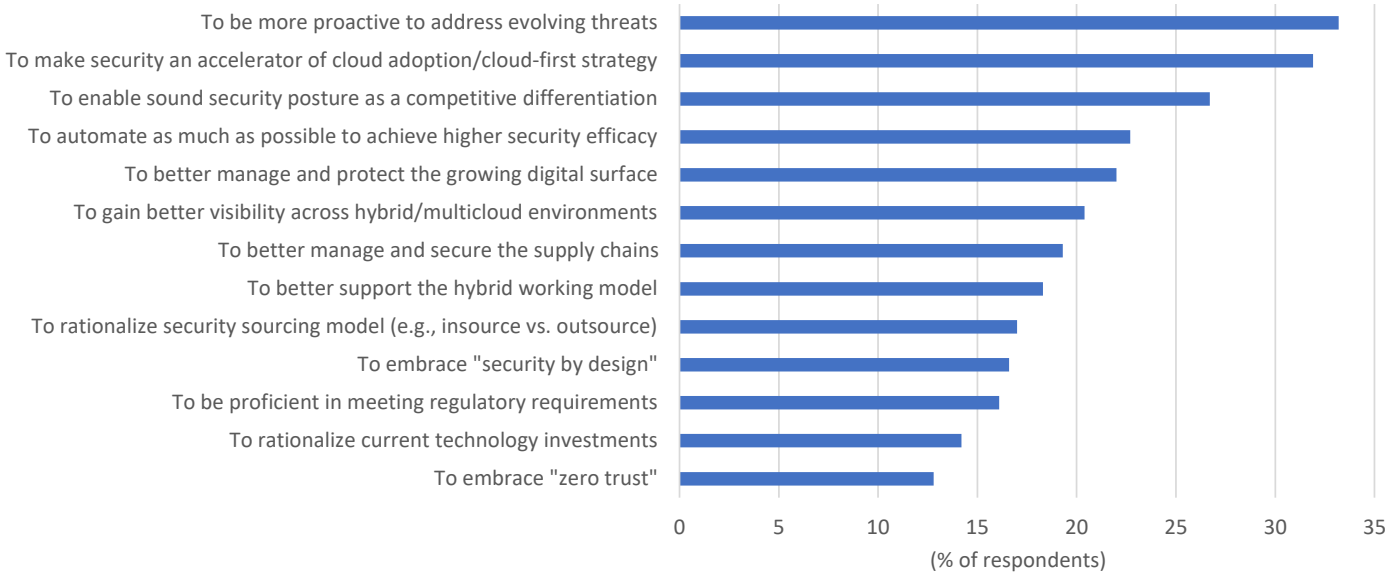
Key Trends

The concern over shadow IT is growing as digital transformation, the shift to remote work, and the move to hybrid cloud environments have made it harder for organizations to keep track of assets, particularly those spun up in the cloud without the knowledge of the IT department. Organizations are increasingly understanding the risk their shadow IT poses to the business because it is not managed — vulnerabilities are unknown and the lack of knowledge heightens the risk. Organizations are looking to gain visibility and reduce their risk — especially in the wake of growing regulations in some industries.

In IDC's *Security ServicesView Survey,* respondents indicated that the top goal of their cybersecurity transformation efforts is to take a more proactive approach to addressing evolving threats (see Figure 1). The visibility into exposures on external-facing assets provided by ASM helps organizations learn of issues before hackers can take advantage. Security teams can then decide whether to deploy mitigating controls or patch the vulnerabilities, in either case closing the potential gaps before they can be exploited.

FIGURE 1: ***Top Goals for Cybersecurity Transformation***

Q *Which of the following statements best reflect the primary goals of your cybersecurity transformation?*



n = 1,414

Base = respondents who indicated that they are the responsible party in charge of implementing the cybersecurity transformation, encouraging the cooperation of relevant parties to facilitate the cybersecurity transformation, and putting the strategy into practice

Source: IDC's Security ServicesView Survey, February 2022

In addition to proactively addressing evolving threats, ASM supports several other cybersecurity objectives. For example, making security a competitive differentiator first requires an understanding of the organization's security posture and then ensuring all security gaps are closed and new exposures are remediated as quickly as possible. The continuous monitoring and discovery of exposures in external-facing assets automate the visibility of those exposures. Teams do not need to seek out information; it is placed in their hands.

A survey of hackers conducted by Bishop Fox and SANS shows that the speed of attackers is accelerating. In the survey, 62% said they can find an exposure in less than five hours, 42% said it takes under two more hours to exploit the discovered exposure and break in, 76% said it takes under another five hours to gain access to their target, and 51% said the last step of collecting and exfiltrating data can be done in another two hours or less. In addition, 55% of hackers said they can complete an end-to-end attack in under 20 hours.

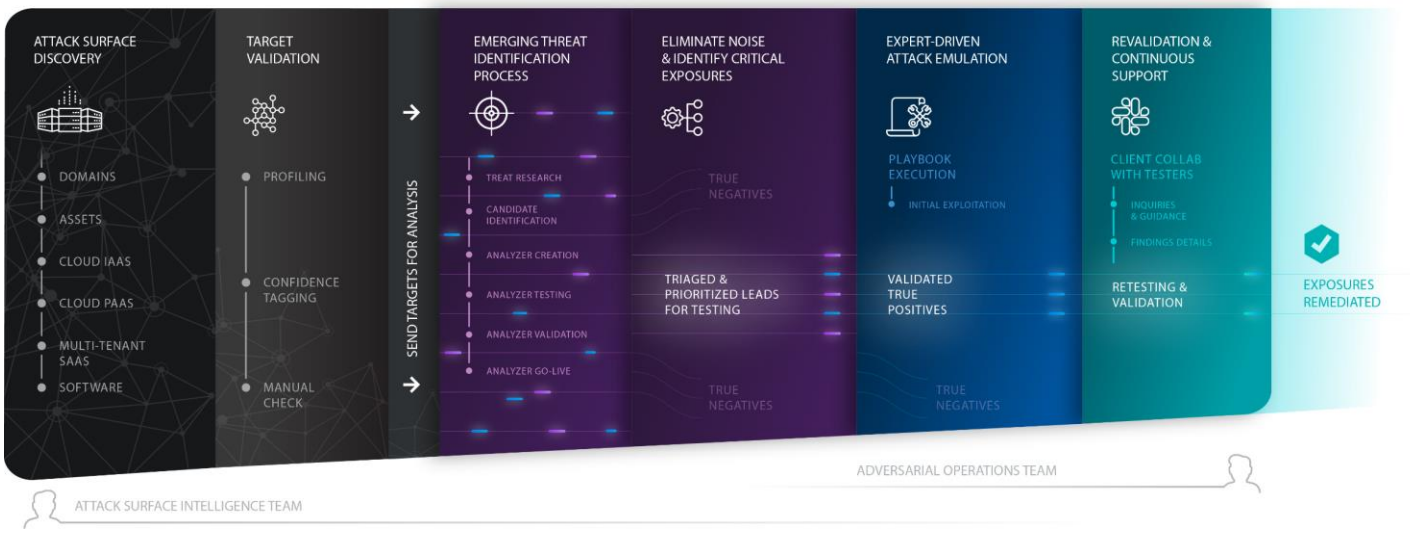
There are many ways for attackers to infiltrate an organization, and ASM platforms help with the discovery and prioritization of vulnerabilities. According to findings from Bishop Fox's Cosmos platform, sensitive information disclosure was the top issue for most industries over the past 12 months. However, vulnerable software was the top issue in hospital and healthcare, while abandoned subdomain takeover was the top issue in consumer goods and services.

Considering Bishop Fox

Bishop Fox, founded in 2005, is one of the largest private firms focused exclusively on offensive security. It offers a portfolio of penetration testing, application security, cloud security, red teaming, and ransomware readiness services and solutions. As the attack surface in many organizations grew and attackers became more sophisticated and moved at a faster pace, Bishop Fox recognized that organizations needed continuous monitoring and testing to help protect themselves against cyberattacks. In 2020, the firm leveraged expertise from thousands of point-in-time security engagements to create its Cosmos platform for continuous proactive defense of dynamic attack surfaces.

Cosmos is designed to integrate technology and human expertise with automation in a unified solution, which Bishop Fox sees as the best way to identify, validate, and enable remediation of dangerous exposures before attackers know they exist (see Figure 2).

FIGURE 2: ***Features of the Cosmos Platform***



Source: Bishop Fox, 2023

Bishop Fox's key differentiator is the following combination of automation used for discovery and human expertise to validate an exploit and determine the business impact:

- Discovery starts with the domains — the same way attackers see their victims.
- Once discovery is conducted on the attack surface, the assets found are validated by humans.
- The exposure reconnaissance engine looks for vulnerabilities, misconfigurations, anomalies, and changes in the internet-facing assets.
- The false positives are eliminated through coordinated automation and human validation, and the true positives are prioritized by the attack surface intelligence team for further testing.

- An adversarial operations team validates the true positives via safe exploitation and post-exploitation activities to identify systems, pathways, and data at risk.
- The testers work with customers to provide detailed findings and remediation guidance. Customers have direct access to the testers to ask questions about the discoveries.
- The testers prioritize the results of their work based on the impact on each unique customer.
- Once problems are corrected, the testers validate that the issue is fixed.
- Customers with audit and compliance requirements can receive letters of assessment and annual reporting to satisfy those mandates.

Challenges

While there are many good reasons to make ASM part of the security operations, there are also challenges:

- Ensuring customers use ASM to its fullest capability, including retesting exposures after remediation
- Prioritizing the work because ASM is going to add to the already large number of vulnerabilities that are surfaced in an organization's environment

Bishop Fox is using both human and machine resources in its Cosmos solution, so the company will need to make certain that Cosmos can scale to the demands that continuous monitoring of a growing customer base places on it.

Conclusion

More than ever, emphasis is being placed on proactive cybersecurity measures that enable organizations to see their cloud and IT assets, understand their vulnerabilities and exposures, and determine the paths to critical assets so there are fewer surprises when under attack. ASM tooling provides visibility into and testing of the ever-changing attack surface, enabling security teams to quickly discover new and recurring problems and to retest and validate remediations so the same issue does not arise endlessly, closing that gap for all time.

About the Analyst

Michelle Abraham, *Research Director, Security and Trust*

Michelle Abraham is the Research Director in IDC's Security and Trust Group responsible for the SIEM and Vulnerability Management practice. Core research coverage includes application and device vulnerability management, attack surface management, breach and attack simulation, and security information and event management (SIEM) platforms.

MESSAGE FROM THE SPONSOR

Security is an evolving challenge, but we don't believe breaches aren't inevitable. We believe the best way to manage risk is adopting a "forward defense" approach — focusing on prevention, not reaction. We are committed to offensive security because we believe that the best way to secure modern organizations is by subjecting their networks and applications to the same attacks they see in the world. We have worked with more than 25% of the Fortune 100, half of the Fortune 10, eight of the top 10 global technology companies, and all the top global media companies to improve their security. Visit us at bishopfox.com to learn what Bishop Fox and our Cosmos platform can do for you.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com