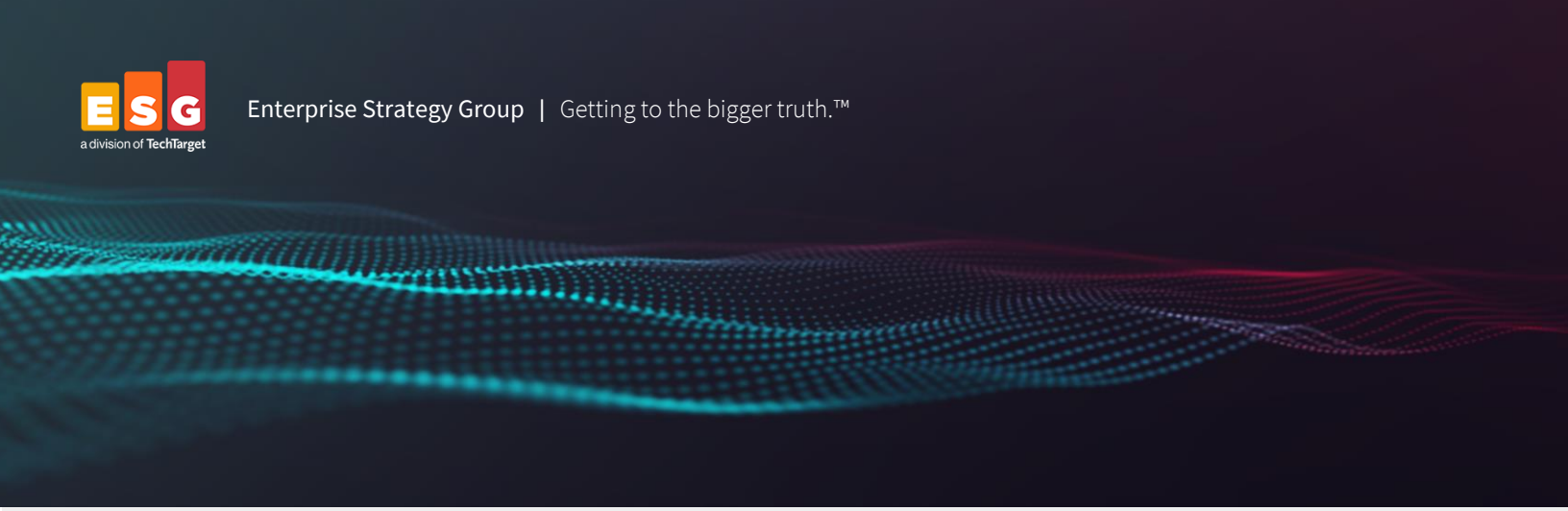


ESG WHITE PAPER

Value Drivers for an Attack Surface Management (ASM) Program

By Jon Oltsik, ESG Senior Principal Analyst and Fellow

April 2022

This ESG White Paper was commissioned by Palo Alto Networks and is distributed under license from TechTarget, Inc.

© 2022 TechTarget, Inc. All Rights Reserved.

Contents

© 2022 TechTarget, Inc. All Rights Reserved.

Executive Summary

A few years ago, the term attack surface management (ASM) wasn't part of the common cybersecurity lexicon. Most organizations employed a few security and IT personnel who could identify their internet-facing assets and manage security hygiene and posture using an assortment of tools like vulnerability scanners, CMDBs, and threat intelligence feeds.

Unfortunately, this quaint picture has become ancient history. A modern Internet-facing attack surface is often composed of a variety of thousands of assets, including websites, user credentials, sensitive data, open ports, code fragments, and much more. Beyond scale and scope, the attack surface is incredibly dynamic, changing and growing all the time.

Given this progress, one would assume that organizations have modernized their ASM processes and technologies to keep up. Unfortunately, that's not really the case. This white paper concludes:

- ASM continues to lag. Despite massive attack surface growth, organizations continue to perform ASM manually, using an assortment of data sources, security/IT tools, and even spreadsheets. Furthermore, organizations only monitor a portion of their attack surface, it takes ample time and resources for attack surface discovery, and most organizations continue to do discovery on a periodic basis. These haphazard steps result in an incomplete and out-of-date picture of the attack surface, leaving organizations vulnerable to attack.

- ASM weaknesses lead to security incidents. While security teams muddle through ASM, sophisticated adversaries use automated scanning tools to quickly identify vulnerable assets for exploitation. The results are alarming—69% of organizations surveyed report that they've experienced a cyber-incident resulting from an unknown, unmanaged, or poorly managed internet-facing device.[1]

- It's time for ASM automation. CISOs can't bridge the ASM gap with tactical adjustments, but rather need ASM processes and technologies that can address the scale, scope, and dynamic nature of the growing attack surface. New, innovative, and automated security ASM solutions like Cortex Xpanse can discover assets across the internet, collect and centralize the data, provide analytics for risk scoring, and integrate with other security and IT tools for remediation and risk mitigation.

Current ASM Is Inadequate

Existing ASM processes and technologies are a complete mismatch for today's threat landscape. As part of attack campaigns, cyber-adversaries use automated attack surface scanning tools and work around the clock to find vulnerable systems on enterprise networks. The *2021 Attack Surface Threat Report* published by Cortex Xpanse indicates that on a typical day, attackers conducted a new scan once every hour. Alternatively, most organizations have ASM programs with limited coverage, manual processes, and various technologies. For example, ESG research reveals that many organizations:

- Monitor some but not all their attack surface. Only 9% of security professionals believe their organization actively monitors 100% of their attack surface, while 29% say they actively monitor between 75% and 89% of the attack surface.[2] Others monitor even less. Aside from the obvious "blind spots," many firms have an assortment of internet-facing assets they don't even know about. In fact, vendors in this space report that organizations often discover somewhere in the range of 40% more (previously unknown) assets when they use automated ASM scanners. So, the

[1] Source: ESG Research Report, *Security Hygiene and Posture Management*, January 2022. All ESG research references and charts in this white paper have been taken from this research report, unless otherwise indicated.
[2] Source: ESG Complete Survey Results, *Security Hygiene and Posture Management*, January 2022.

© 2022 TechTarget, Inc. All Rights Reserved.

ASM problem is bigger than many organizations believe, and even organizations that think they have things under control probably don't.

- Conduct ASM using multiple tools and data sources. Like other areas of cybersecurity, many organizations piece together an ASM puzzle by gathering data from a wide assortment of security and IT tools. For example, 41% of organizations use threat intelligence sources, 40% utilize IT asset management systems, 33% employ cloud security monitoring solutions, and 29% rely on vulnerability management.[3] Of course, someone must bring together this data, correlate it, and try to make sense of it. Often, this is (still) done with static spreadsheets—a mismatch for the dynamic attack surface.

It's also worth noting that all this attack surface discovery work is necessary to *start* ASM processes like analyzing the data, determining which assets face the highest risks, and prioritizing remediation and risk mitigation actions. And since attack surface discovery remains inconsistent and incomplete, ASM decisions are really nothing more than educated guesses.

The Absence of an ASM Program Comes at a Cost

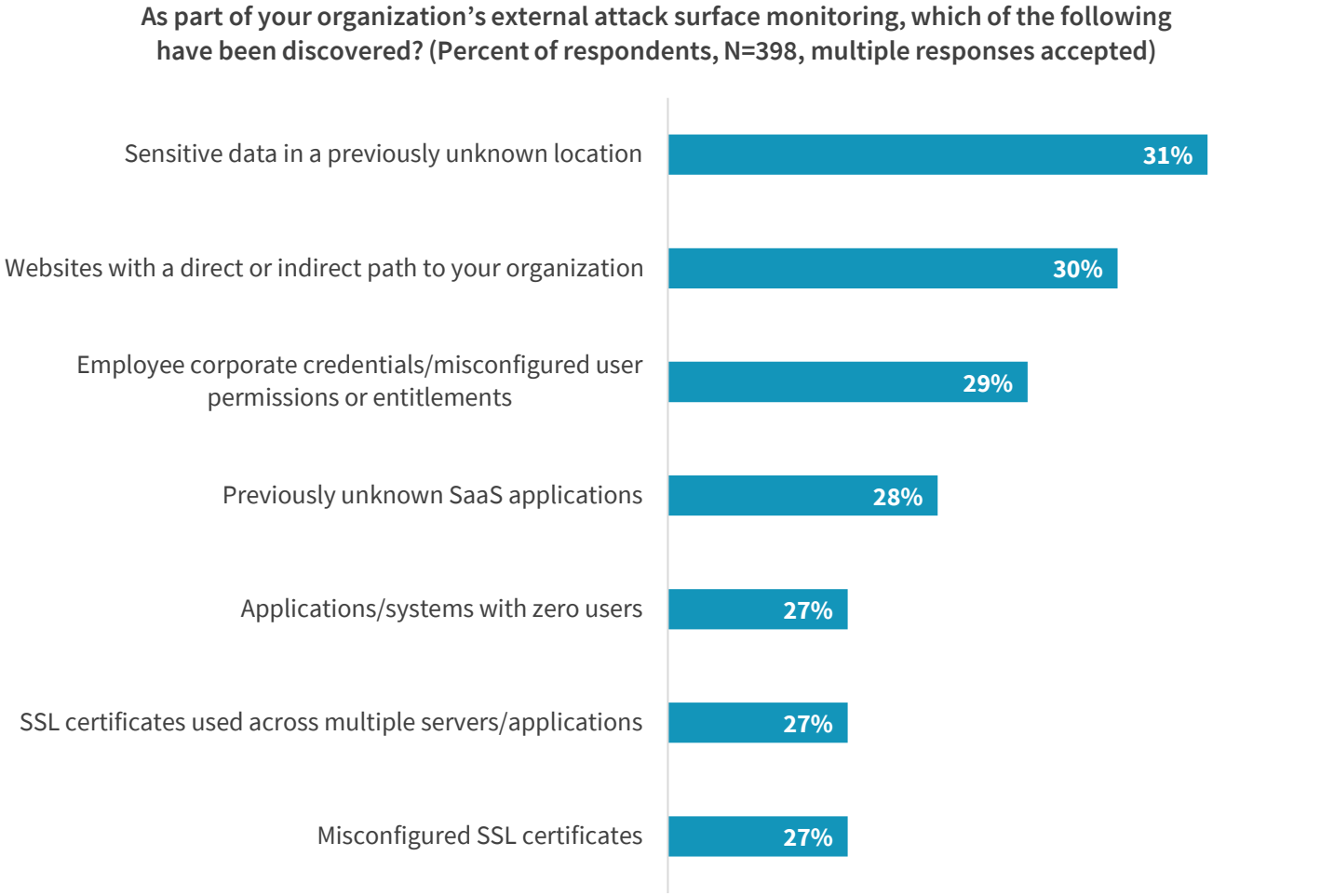
Why do organizations continue to muddle through attack surface management? Because they haven't yet recognized the importance of ASM or the costs associated when ASM best practices are neglected. Based on ESG research, these costs can include:

- Increased attack surface risk. While organizations may believe they know about their Internet-facing assets, ESG research tells a different story. For example, ESG research reveals that organizations have discovered an assortment of vulnerable assets like sensitive data in a previously unknown location, websites with a direct or indirect path to their organizations, employee credentials (that may be misconfigured), previously unknown SaaS applications, and applications with zero users (see Figure 1). In fact, unknown attack surface assets tend to be the rule rather than the exception. ESG has seen that when organizations use automated attack surface management discovery tools, security teams regularly find that their attack surface is at least 40% greater than they perceived. These exposures represent easy targets for cyber-adversaries and create significant risks for organizations. While security professionals labor to keep up with monitoring the attack surface, cyber-criminals use automated tools to continually scan the attack surface looking for vulnerabilities. The *2021 Attack Surface Threat Report* published by Cortex Xpanse indicates that malicious actors start scanning the internet within 15 minutes of a critical vulnerability or exposures (CVE) announcement. By comparison, organizations can take weeks to discover and remediate these exposures.

[3] Ibid.

© 2022 TechTarget, Inc. All Rights Reserved.

Figure 1. Top Seven Attack Surface Assets Discovered

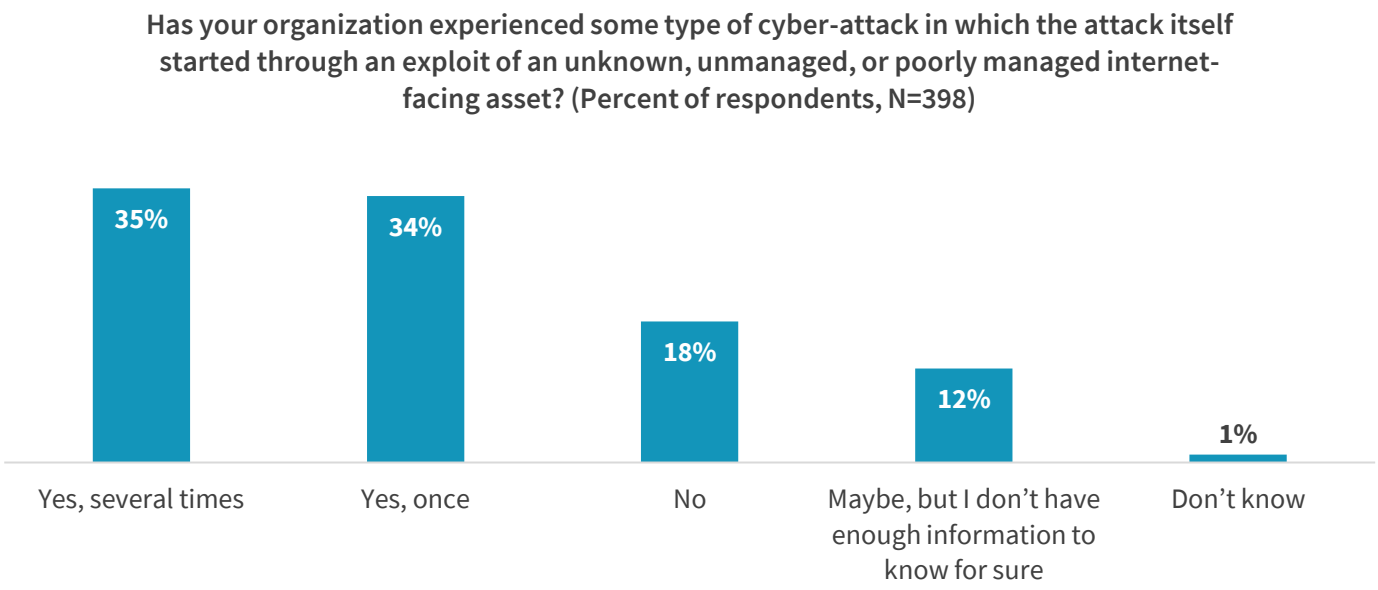


Source: ESG, a division of TechTarget, Inc.

- Security incidents. Once discovered, cyber-criminals utilize these vulnerabilities to conduct cyber-attacks, and these attacks are becoming more frequent. In fact, ESG data indicates that 69% of organizations have suffered at least one cyber-attack due to an unknown, unmanaged, or poorly managed internet-facing asset (see Figure 2). Cyber-attacks emanating from the exploitation of an attack surface asset can be extremely costly. For example, in 2017, online marketing firm and data analytics company Alteryx left the personal information of more than 120 million US households exposed on the internet. The incident was caused by a misconfigured Amazon Web Services (AWS) S3 Bucket that exposed the 36GB worth of data to the public. This breach and many others could have been prevented if the organization adopted diligent attack surface management and strong processes for change management and security remediation.

© 2022 TechTarget, Inc. All Rights Reserved.

Figure 2. Cyber-attacks Resulting from Attack Surface Vulnerabilities



Source: ESG, a division of TechTarget, Inc.

- A reliance of threat detection and response. When discussing public health, Microsoft founder Bill Gates proclaims that "treatment without prevention is unsustainable." Regrettably, the same philosophy is true with cybersecurity. Organizations eschewing ASM will have to anticipate more attacks and then compensate by investing more in threat detection and response technologies and processes. This assumes addressing growing alert volumes, triaging, prioritizing, and investigating alerts; staying abreast of cyber-adversary campaigns; and building best practices for rapid incident response. Yes, these organizations are always required, but the absence of ASM best practices will make the scale, scope, and pace of threat detection and response unsustainable for all but the biggest and most adept security teams.

Benefits of Automating an ASM Program

As part of a recent ESG research survey, security professionals were asked directly what their organizations could do to improve attack surface management. These infosec pros recommended:

- Improving risk scoring (29%). It's simply not enough to discover Internet-facing assets. Security professionals need to understand which ones are vulnerable and most at risk. New, intelligent ASM solutions use analytics to calculate risk scores for vulnerable assets, helping security professionals prioritize remediation actions.

- Establishing KPIs and metrics (26%). In this area, attack surface management metrics should be closely aligned with vulnerability management. Therefore, metrics could include scanning frequency, scanning coverage, number of critical attack surface vulnerabilities discovered, number of critical attack surface vulnerabilities addressed, time necessary to address critical attack surface vulnerabilities, and the number of attack surface vulnerabilities that qualify as exclusions. Security teams can use these metrics to establish KPIs, share performance with business executives, and develop plans for continuous improvement.

© 2022 TechTarget, Inc. All Rights Reserved.

- Enhancing collaboration between security and IT teams (26%). While security teams are responsible for attack surface discovery, analysis, and prioritization, they need IT operations for ultimate remediation measures. Accordingly, security and IT teams must establish the proper processes and vehicles for communications and collaboration. Security professionals should address this by mapping out workflows, using SOAR tools to automate runbooks, and, if possible, orchestrating remediation procedures. Leading SOAR tools will extend these processes through integration with ITSM tools for ticketing and case management.

Figure 3. Recommendations for Improving Attack Surface Management

Source: ESG, a division of TechTarget, Inc.

An ASM program can also help lower costs by proactively shutting the door on ransomware. According to a report published by Palo Alto Networks Unit-42, RDP servers have overtaken phishing as the attack vector of choice for ransomware. In 2019, the average cost of a successful ransomware attack was $312,493. This number is only likely to be much higher for 2021 given high-profile cases of ransomware in the news. The average cost of an ASM solution is lower than ransomware, and ASM can help security teams discover and remediate non-zero-day vulnerabilities in an organization, preventing possible security exploits.

© 2022 TechTarget, Inc. All Rights Reserved.

Paying for ASM

ESG research reveals that 80% of organizations will increase security hygiene and posture management overall in 2022, and that includes direct investments in attack surface management.[4] Unfortunately, many organizations haven't allocated budget dollars for ASM yet. How can they find money to pay for this increasingly important requirement? ESG finds that many organizations are:

Creating discretionary budgets

Some organizations are creating discretionary budgets in response to recent ransomware attacks that make attack surface management a C-suite level concern. Part of any ransomware budget should be dedicated toward technology and processes that can help prevent those attacks before they occur.

Given the value in ASM in terms of overall security cost savings, as well as the value in improving operational efficiency of a SOC, the proactive nature of an ASM plan should be of interest to any C-suite or board of directors. Ransomware attacks often begin with a breach through vulnerable RDP or other exposures, so being able to find those risks and remediate them quickly is invaluable.

Additionally, the comprehensive asset inventory and exposure discovery provided by a quality ASM vendor can benefit multiple other security products such as vulnerability scanners, antivirus/antimalware scanners, etc., which can help minimize mean time to detect in the case an attack does occur.

Rerouting point-in-time ASM analysis budgets

As previously mentioned, old methods of asset inventory fail on multiple levels, so it is highly encouraged that organizations move away from conducting services-led point-in-time analysis or reduce the frequency of their point-in-time analysis program. The budgets for these activities could easily be redirected and invested in continuous monitoring with an ASM solution.

Establishing a preventative security budget

While harder to quantify, preventing cyberattacks before they occur is certainly a way to save money. The cost of cleaning up a breach, the cost of operational downtime, and of course the costs associated with ransomware can be exorbitant.

Investing in technologies and processes that can prevent breaches before they occur is a viable way to save money. A foundational component of those technologies and processes should be ASM. The comprehensive asset inventory can benefit all security products to ensure there are no unknown assets creating unknown risks. Additionally, the exposures and risks uncovered by ASM are tangible touch points to show reduced risks that keep your organization safer.

Justifying ASM spending to lower cyber-insurance premiums

ASM best practices can provide measurable improvements in cyber-risk management. A successful implementation of an ASM plan should reduce exposures and help close down high-risk vulnerabilities. Insurance providers understand these efforts for risk mitigation and may be willing to translate these improvements into lower cyber-insurance premiums.

Alternatively, cyber insurance providers may require a security ratings score upon which insurance premiums will be based. These scores are often opaque, making it difficult for organizations to negotiate insurance costs. The visibility provided by

4 Source: ESG Complete Survey Results, *Security Hygiene and Posture Management*, January 2022.

© 2022 TechTarget, Inc. All Rights Reserved.

ASM can add context and actionable information to those scores, giving organizations the opportunity to reduce risks and earn lower insurance premiums.

Turning ASM spending from CapEx and OpEx

Some ASM solutions are available on popular cloud marketplace services (AWS, GCP, Azure, etc.), helping to convert ASM investments from a capital to operational expenditure. If an organization is unable to make a yearly subscription to an ASM solution, then it can convert it into a monthly subscription if purchased on several of the popular cloud provider marketplaces.

Sharing the cost of ownership across multiple teams

In a modern organization, security is not, and should not be, the sole responsibility of any one group. Security practices are most effective when understood and shared across teams. Given this holistic view of security, it makes sense for multiple groups to share the costs associated with foundational security items, such as ASM.

In the latest ESG report, we found that the responsibility for managing an external attack surface is split across the security group (16%), IT and operations group (41%), or a combination of the two groups (43%).[5] The common theme is that multiple teams within an organization can find value from an ASM solution.

These short-term suggestions are meant to bridge budget gaps in 2022. Moving forward, ASM should be considered a critical security safeguard deserving a dedicated budget.

ASM from Cortex Xpanse

Security teams, hamstrung by manual processes and technology silos, can't possibly execute the recommendations described above. Rather, ASM processes and technologies need a transformation focused on scale, intelligence, and automation.

Recognizing the growing ASM gap, in November 2008, Palo Alto Networks acquired Expanse Networks, a leading ASM technology vendor, and now calls its ASM offering Cortex Xpanse. Xpanse provides an attacker's "outside-in" view of an organization's attack surface by continuously discovering and monitoring assets across the entire internet. Using Xpanse, security teams can discover, analyze, prioritize, and mitigate risky attack surface management assets.

Cortex Xpanse can act as a central repository and single source of truth for ASM, obviating the need for existing time-consuming and cumbersome discovery and management processes. With continuous data collection and analysis, organizations can proactively mitigate risks before adversary exploitation. Finally, Cortex Xpanse is integrated with other Palo Alto Networks products like Cortex XSOAR and Prisma Cloud to streamline end-to-end security workflows and process automation.

Cortex Xpanse is built for today's ASM requirements, offering the scale, analytics, and automation necessary. Consequently, CISOs seeking to modernize their ASM capabilities may want to see how Cortex Xpanse aligns with their security and risk management strategies.

[5] Ibid.

© 2022 TechTarget, Inc. All Rights Reserved.

The Bigger Truth

As the saying goes, "An ounce of prevention is worth a pound of cure." Attack surface management is intended to bring this axiom to life, but constantly discovering internet-facing assets, determining which ones are vulnerable to attack, and providing integration with remediation processes to mitigate cyber-risk is difficult, if not impossible, using current processes and technologies.

Security professionals understand that maintaining security hygiene is a cybersecurity best practice, and sound ASM is a critical best-practice component. In the past, security teams could probably keep up with ASM using assorted tools and manual processes, but those days are long gone. CISOs must recognize that the combination of digital transformation, remote workers, cloud computing, and third-party IT connections requires new processes and technologies that can provide the scale, scope, intelligence, and automation for modern ASM requirements.

© 2022 TechTarget, Inc. All Rights Reserved.

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

This publication is copyrighted by TechTarget, Inc. 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, Inc., 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.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188

© 2022 TechTarget, Inc. All Rights Reserved.