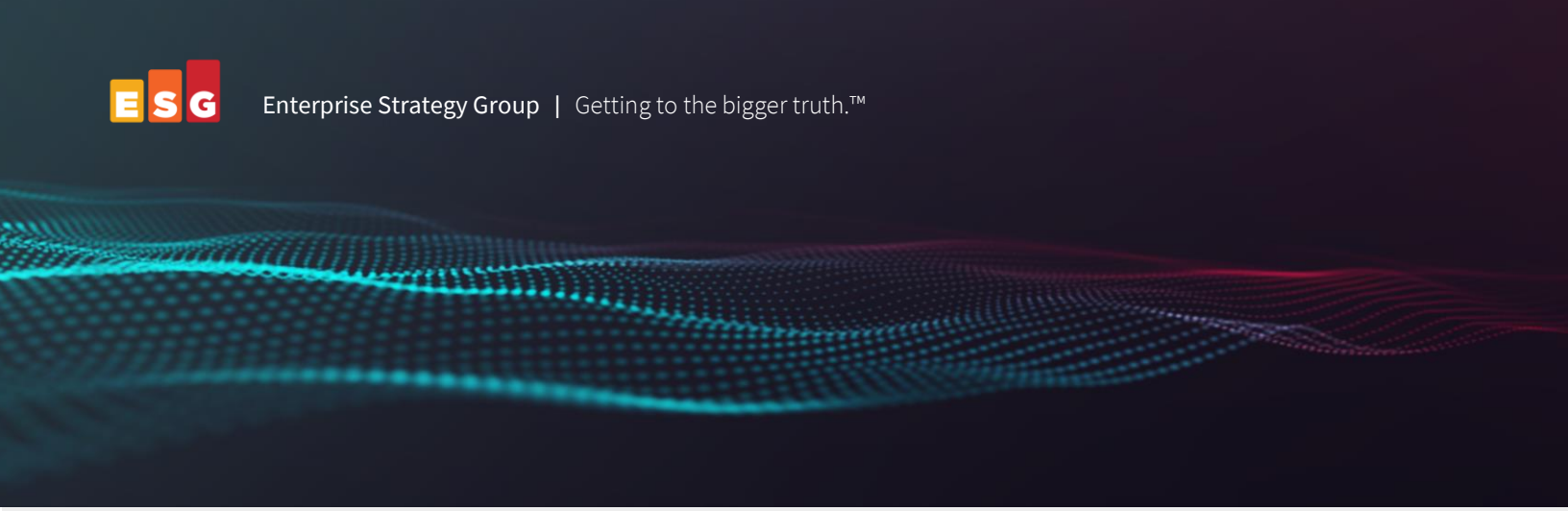


ESG WHITE PAPER

Meeting the Challenges of Securing Modern Web Applications with WAAP

By John Grady, ESG Analyst

November 2020

This ESG White Paper was commissioned by Google and is distributed under license from ESG.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Contents

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Executive Summary

The development, composition, and deployment location of web applications have fundamentally changed in the modern enterprise. DevOps methodologies have been increasingly adopted to improve the agility and speed with which applications can be deployed. The shift to microservices-based architectures has helped facilitate this transition and created more flexibility relative to location to ensure resources are hosted wherever the needs of the application dictate. Yet while delivering numerous benefits to the enterprise, the byproduct of these developments is often the decentralization of control, moving it outside of the traditional IT organization, especially relative to security.

At the same time, the threat landscape web applications face is more varied and dynamic than ever. Attackers still seek to exploit traditional application vulnerabilities through code and availability-based attacks, while also expanding their methods to target the connective tissue of modern web applications: APIs. To meet these challenges, a new model is emerging to overcome the limitations of a siloed approach to application security. Specifically, the integration of WAF, DDoS prevention, bot mitigation, and API protection into a consolidated web application and API protection (WAAP) solution is becoming the preferred approach to streamline management, simplify operations, and improve security.

The integration of WAF, DDoS prevention, bot mitigation, and API protection into a consolidated web application and API protection (WAAP) solution is becoming the preferred approach to streamline management, simplify operations, and improve security.

Modern Web Applications Have Introduced New Security Challenges

The number of applications supported in enterprise environments has continued to rise. In fact, 62% of those surveyed indicate their organization supports at least 250 business applications. Further, more than three-quarters (78%) say more than 20% of these applications were internally developed.[1] To achieve this scale, most organizations have begun to adapt their processes and supporting infrastructure in order to increase the speed, agility, and flexibility with which they develop and deploy new applications. Unfortunately, these improvements can come at the expense of security.

Nearly all organizations use some type of cloud service, but it has become commonplace to see multiple cloud platforms in enterprise environments either as the natural result of sprawl over time or as a formal business strategy. This is not to say that on-premises infrastructure has or will disappear. Many organizations expect to maintain on-premises infrastructure to support legacy applications, ensure performance requirements, or maintain data residency and compliance. The adoption of container-based architectures is also contributing to this multi-location trend. Specifically, while 23% of organizations currently report container-based applications are deployed in a combination of public cloud platforms and private data centers, 46% expect to use a hybrid model in the future.[2]

Security organizations that are not closely tied to DevOps programs may have limited control and visibility into the applications being deployed and run out of these teams.

Further, application development and management are increasingly decentralized, with developers scattered throughout the lines of business and many organizations employing DevOps methodologies. In fact, 57% of organizations using public cloud services report using DevOps to some extent, with an additional

[1] Source: ESG Master Survey Results, *Trends in Modern Application Environments*, December 2019.
[2] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications*, December 2019.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

16% reporting plans to employ these practices in the future.[3] The level of security integration into DevOps programs can vary from one organization to another. Security organizations that are not closely tied to DevOps programs may have limited control and visibility into the applications being deployed and run out of these teams. This, coupled with the fact that many application security tools were not built for the cloud and are predicated on in-line appliance-centric architectures, makes applying consistent security across all web applications much more difficult.

Finally, the composition and interaction of modern application components further compounds these issues. The shift toward microservices-based architectures has resulted in a dramatic rise in API usage to support faster and more agile application development. Unfortunately, the sprawl of these endpoints can make it difficult to maintain the proper security controls. Misconfigurations, poor identity controls, and limited visibility can be exploited by attackers to improperly escalate privileges, access sensitive data, or launch fraudulent account takeover attacks via insecure APIs.

Traditional Application Security Capabilities Remain Important, but Critical Gaps Exist

While organizations should ensure protection across the major application threat vectors, they must be aware of the limitations under which some of these tools operate.

This does not mean that traditional application security capabilities have become irrelevant. In actuality, the threat landscape evolves as attackers identify new methods and vectors to exploit, and application security is no different. Organizations are likely to experience a range of attacks related to web applications, from exploits targeting software vulnerabilities, availability attacks against the application itself or supporting APIs, to fraud targeting user credentials. So, while organizations should ensure protection across the major application threat vectors, they must be aware of the limitations under which some of these tools operate.

Web Application Firewalls

Web application firewalls remain widely deployed and are the core component of most application security strategies. The Open Web Application Security Project (OWASP), publishes its Top 10 list of application security flaws and corresponding remediation guidance every 2-3 years. While the goal should be to mitigate these issues during development and deployment, the reality is that errors do occur, and web applications are often deployed with vulnerabilities. Many WAFs have specifically focused on providing baseline protection against the OWASP Top 10, to shield against the most common application threats. Compliance is also a factor in the broad adoption of WAFs, especially relative to public-facing applications. However, there has been increased interest in WAF as an avenue to improve the security of applications, rather than as just a checkbox item. Unfortunately, the architecture of many traditional WAFs make achieving this difficult, specifically due to deployment and detection.

The biggest issue facing legacy WAFs is that many were built to defend on-premises, monolithic applications, making it difficult for them to scale to meet more dynamic application deployment practices. These solutions may be offered in virtualized form-factors to address cloud applications, but the scalability, flexibility, and integration in cloud-native processes may not meet the needs of cloud-centric organizations. This has begun to change, but in many cases remains a work in progress.

Finally, WAFs have historically been expensive from both an acquisition and operational perspective. Appliance-centric approaches require significant upfront capital investments. Further, the dependence on signature-based detection models makes deployment, tuning, and maintenance a labor-intensive and expensive process. This is not to say that signatures are

[3] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications*, December 2019.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

irrelevant. However, more advanced WAF solutions are moving toward augmenting signatures with machine learning capabilities to reduce false positives and adaptively tune defenses. This helps organizations reduce the overhead costs associated with WAF while improving security.

Distributed Denial of Service Prevention

DDoS attacks are relatively easy to launch and can cause significant business disruption, leading to brand reputation impact and lost revenue. These attacks may ebb and flow but remain a top security concern for organizations of all types with public-facing web applications and are increasingly difficult to defend against. In fact, 44% of organizations report that DDoS attacks have become more sophisticated over the last two years, though longer durations, larger volumes, and increased frequency are common, concerning trends with these attacks as well (see Figure 1).[4]

Figure 1. DDoS Attack Trends

Source: Enterprise Strategy Group

As a result, many organizations have shifted toward cloud-based DDoS protection services primarily to defend against large attacks, but also to simplify operations and achieve cost savings. With attacks commonly reaching well into the 100Gbps range, and even over 1Tbps on rare occasions, an appliance-based approach cannot scale to the required level of mitigation capacity. DDoS solutions are often focused on either network-centric, volumetric attacks targeting layers 3 and 4, or layer 7 application attacks. However, coverage for attacks across both vectors is needed and more importantly, must incorporate telemetry from the application to ensure adequate protection.

[4] Source: ESG Master Survey Results, *Network Security Trends*, March 2020.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

API Protection

Protection for the APIs that support modern web applications has seen increased focus over the last few years. In fact, 34% of respondents indicate that API security will be the area in which their organization will make the most significant investments to protect cloud-native applications over the next 12-18 months.[5] However, how this investment translates into tools can vary significantly. Many WAFs have some API security capabilities, yet in most cases the functionality remains somewhat limited and a secondary focus of the solution. Also, this model does not typically provide discovery capabilities to identity APIs that have not been inventoried, requiring integration with a separate API gateway or management tool to provide a more complete solution. Finally, WAFs deployed at the edge do not have visibility into the intra-application API traffic flowing behind them.

34% of respondents indicate that API security will be the area in which their organization will make the most significant investments to protect cloud-native applications over the next 12-18 months.

Bot Mitigation

The use of bots to facilitate application attacks has only increased over time. Yet malicious bot traffic is difficult to defend against due to the different types of bots and nature of bot traffic. Because not all bots are malicious, differentiating between a bad bot and a benign web-crawling bot is critical. Additionally, bot actions may only become malicious when their scale reaches a critical mass, or the outcome leads to a bad outcome such as account takeover, automated account creation, or something similar. Until that happens, a bot is simply mimicking human actions but at a greater scale.

Bots continue to evolve, making detection more difficult. Early generation bots could easily be identified through cookie or JavaScript challenges. Advanced bots now use legitimate browsers and more accurately simulate human activity in minutia, making detection at scale without impacting user experience or creating false positives much more difficult. While strong bot management solutions exist, the degree with which bots are used to target applications and APIs limits the effectiveness of these solutions relative to an overall application security approach.

Siloed Tools Cannot Adequately Protect Modern Web Application Environments

Incorporating all these security capabilities into a modern web application environment can significantly increase security complexity and cost when the tools are siloed and managed independently of one another. Management complexity is only compounded when application environments are spread across a mix of on-premises and cloud environments. In fact, ESG research has found that 43% of organizations indicate that maintaining security consistency across the data center and public cloud environments where cloud-native applications are deployed is one of the biggest application security challenges.[6] Along these lines, engaging the different vendors providing these tools adds cost and inefficiency from a procurement and vendor management perspective.

This complexity may be compensated for to some extent by dedicating skilled security personnel, but that is not a realistic option for most organizations. Unfortunately, application security ranks as the cybersecurity segment with the most acute shortage of skills, as indicated by 33% of respondents.[7] This is only exacerbated by the decentralization of applications discussed earlier and the growing number of applications the enterprise supports. Ultimately, this can impact efficacy as well, both when solutions do not natively share information about application attacks to improve protection, and due to the potential for misconfigurations across multiple toolsets. As a result, consistency and ease of use become paramount.

[5] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications*, December 2019.
[6] Source: ESG Master Survey Results, *Leveraging DevSecOps to Secure Cloud-native Applications*, December 2019.
[7] Source: ESG/ISSA Research Report, *The Life and Times of Cybersecurity Professionals 2020*, July 2020.

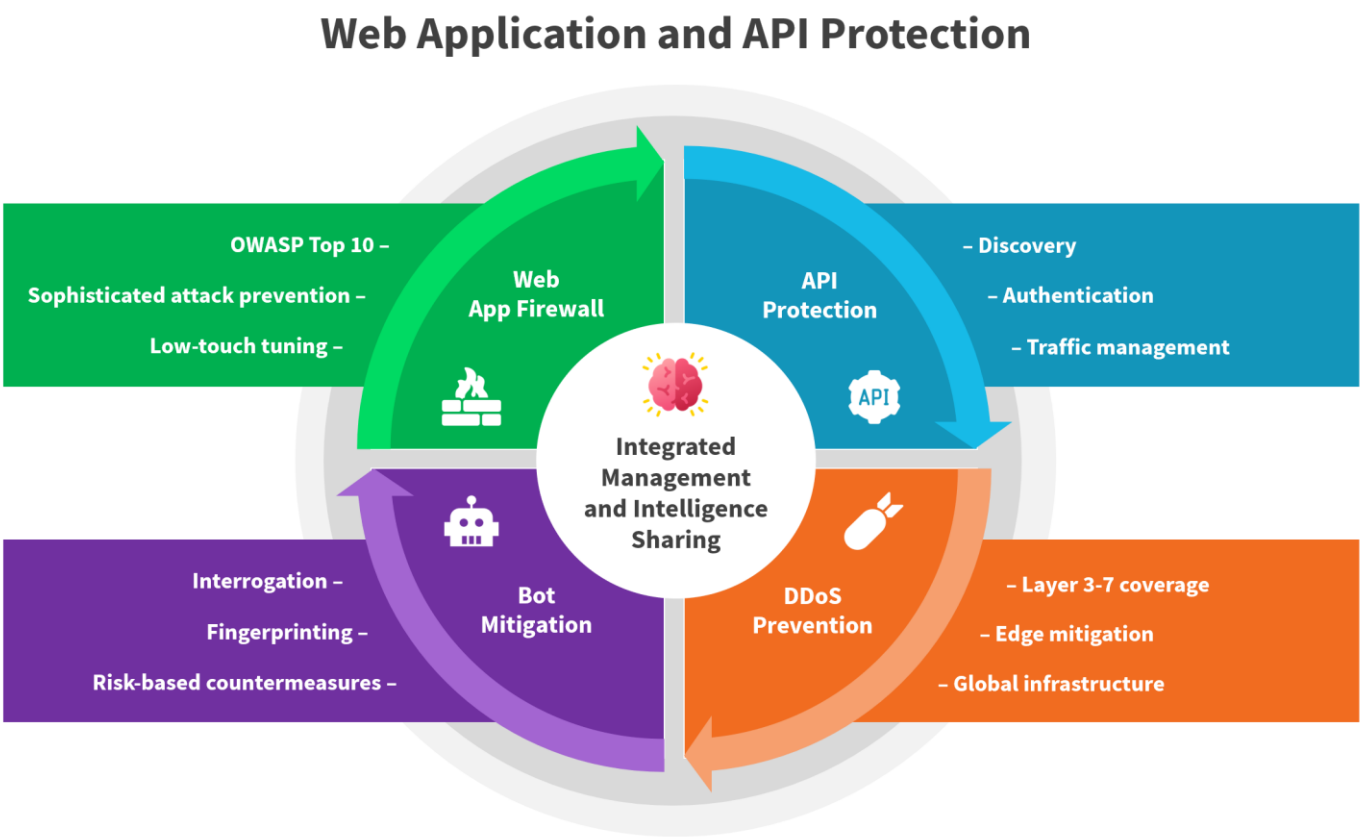
© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Finally, security budgets are clearly in flux as organizational priorities have shifted to ensure the remote workforce is supported and secure. Application security tools can be among the more expensive solutions to deploy and maintain in an enterprise, in part due to the broad coverage required to fully shield applications from attackers. Securing web applications will undoubtedly continue to garner a sizeable share of security budgets. However, many organizations will be looking for ways to reduce spending wherever possible.

Key Attributes for Modern Web Application Security Solutions

To address these cost, complexity, and efficacy issues, security solutions combining WAF, DDoS prevention, bot mitigation, and API protection have begun to emerge. Sometimes called web application and API protection, or WAAP, these solutions represent a shift from siloed to unified application protection (see Figure 2). As with any security consolidation approach, users expect improved threat prevention, greater operational efficiencies, tighter integration between previously disparate controls, and improved vendor relationships. Relative to WAAP, this transition is still underway, and solutions are just beginning to come to market, leading to significant variance in architectures and capabilities across vendors. Yet even with this being the case, there remain a handful of critical attributes organizations should look for when considering WAAP solutions.

Figure 2. Web Application and API Protection



Source: Enterprise Strategy Group

Cloud-centric but Location-agnostic

As more applications shift to the cloud, it only makes sense that protection should follow to remain close to the resource. Unfortunately, the modern, multi-cloud environment many enterprises support can make this difficult. Additionally, supporting on-premises applications remains a reality for most organizations. To deliver on the promise of fewer products,

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

fewer vendors, and less complexity, WAAP solutions that can protect applications across hybrid, multi-cloud environments are critical. Perhaps just as importantly, organizations should consider WAAP solutions that plug into the CI/CD workflow and integrate with DevOps automation tools used for application development, configuration, provisioning, monitoring, and remediation.

Integration

While WAAP promises an integrated runtime application security approach, the reality is that most solutions are just beginning to transition toward this concept. This leaves a sizable grey area for practitioners to navigate when assessing WAAP solutions, which makes striking the right balance all the more difficult. Solutions may comprise discrete products joined by a centralized management interface. However, even this management component can range from a single dashboard providing visibility into attack traffic and application response across all vectors, to fully unified policy management across WAF, DDoS, bot, and API protection.

Some solutions do offer integrated functionality across WAF, DDoS, bot, and API protection via a single product where traffic is scanned once to detect malicious activity across all four vectors. Yet in many cases, the main focus is on one or two functions, with significant limitations across the remaining capabilities. Commonly, WAF and DDoS are emphasized, with only limited bot and API protections. For most organizations, efficacy remains the most important factor when considering a security solution. In fact, ESG has found that while there is significant interest in consolidating the number of vendors and products used in enterprise environments, 68% say their organization continues to purchase best-of-breed security products, indicating a high bar for a platform approach.[8]

Telemetry and Risk

A major component of any WAAP solution should be the ability to collect telemetry across all the applications it sits in front of, across all vectors, and use that information to assess risk and improve defenses in real time. For example, as potential bot traffic is identified and sourced to a particular set of IP addresses, that information should be shared with the DDoS mitigation component so that traffic associated with those IP addresses is not allowed above a specified threshold to ensure the availability of the application.

A major component of any WAAP solution should be the ability to collect telemetry across all the applications it sits in front of, across all vectors, and use that information to assess risk and improve defenses in real time.

Additionally, understanding the risk an attack may pose based on the threat and the application allows mitigation to be implemented that reduces false positives, improves customers' experiences, and allows for additional telemetry to be collected prior to blocking. In other words, if questionable traffic is simply blocked, limited intelligence is gathered. By taking limited measures such as requiring multi-factor authentication, security teams can ensure availability for valid users while better understanding the types of attacks and tactics targeting their applications and using that information to improve the organization's security posture. Ideally, these capabilities are native to the WAAP solution. However, at a minimum, strong integration with SIEM, logging, and monitoring tools are necessary to collate collected intelligence.

Ease of Use

Finally, for most organizations to realize the benefits WAAP can offer, there must be an emphasis on usability. The difficulty of managing web application firewalls is a well-worn topic, but for good reason. Administrators must manage thousands of rules and often must choose between learning mode, which takes time; monitoring mode, which does not prevent attacks;

[8] Source: ESG Master Survey Results, *Enterprise-class Cybersecurity Vendor Sentiment,* March 2020.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

and blocking mode, which runs the risk of false positives impacting the experience of legitimate users. DDoS, bot, and especially API protection are no less complex.

Combining these capabilities into a practical WAAP solution requires streamlining rulesets to simplify the number of parameters administrators must manage. Preconfigured rules can certainly help to an extent and have become table stakes for WAF and WAAP solutions. Incorporating natural language descriptions, grouping rules into broader exploit protection categories, and using machine learning to automatically suggest rules can all help reduce the complexity typically associated with application protection.

Organizations should consider solutions with strong individual capabilities across all four WAAP components that are able to natively share telemetry to improve threat detection and prioritize usability, with centralized management and functional integration as an added benefit.

Overall, organizations should consider solutions with strong individual capabilities across all four WAAP components that are able to natively share telemetry to improve threat detection and prioritize usability, with centralized management and functional integration as an added benefit. Vendor transparency and communication is incredibly important as well. Users should ensure a thorough understanding of their vendor's roadmap for clarity on the priority of, and timetable for, full integration across the component parts of WAAP.

Google's WAAP Approach Protects Web Applications Across Hybrid, Multi-cloud Environments

Google's web application and API protection solution is based on the same technology Google uses to protect its public-facing services and provides protection against web application exploits, DDoS attacks, fraudulent bot activity, and API-targeted threats. The solution comprises three components:

- Cloud Armor. Hosted in Google's global load balancing infrastructure, Cloud Armor provides WAF and anti-DDoS capabilities, protecting applications against the OWASP Top 10, sophisticated application exploits, and both volumetric and application layer availability attacks.
- Apigee. Google's dedicated API platform provides overall API management capabilities, but with a heavy focus on security. The solution verifies API keys, generates and validates OAuth access tokens, rate limits traffic, enforces, quotas, and provides analytics on API trends.
- reCAPTCHA Enterprise. Google's bot mitigation capabilities have been defending millions of websites for almost a decade. The reCAPTCHA Enterprise service builds on this technology with capabilities designed specifically for enterprise security concerns. The solution defends against fraudulent activity such as scraping, credential stuffing, and automated account creation. The solution is built to not interrupt users with challenges, but can be customized to enforce countermeasures, such as two factor authentication or email verification based on the risk tolerance of the organization.

Google offers integrated visibility and telemetry through its Cloud Logging and Monitoring dashboard for simplified operations and ease of management. As a cloud-delivered solution, Google's WAAP is more cost effective than on-premises solutions. In addition to protecting applications hosted in the Google cloud, Google's WAAP can secure applications in other public clouds or on-premises by leveraging Google's massive footprint for scalability, providing protection across an organization's entire inventory of web applications.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Bigger Truth

The increasingly interconnected nature of technology generally, and applications specifically, is driving a need for a greater level of integration across many types of IT tools. This is especially true in cybersecurity, where attackers rarely focus on a single avenue of compromise but leverage multiple tactics across different vectors as part of a broader campaign. Application security is no different, which has been the genesis of the shift to WAAP-based approaches.

Yet the need for integration must be balanced with the ability of the controls to adequately protect the environment, address the relevant use cases, and enable practitioners to do their jobs more efficiently. Public-facing web applications represent some of the most mission-critical of enterprise resources. The compromise or unavailability of these assets can directly lead to lost revenue and customer dissatisfaction. WAAP solutions generally address the efficiency issue organizations face, but users must ensure strong coverage across all application threat vectors for these implementations to be truly successful.

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, 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 The Enterprise Strategy Group, 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 ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.


www.esg-global.com


contact@esg-global.com


508.482.0188

© 2020 by The Enterprise Strategy Group, Inc. All Rights Reserved.