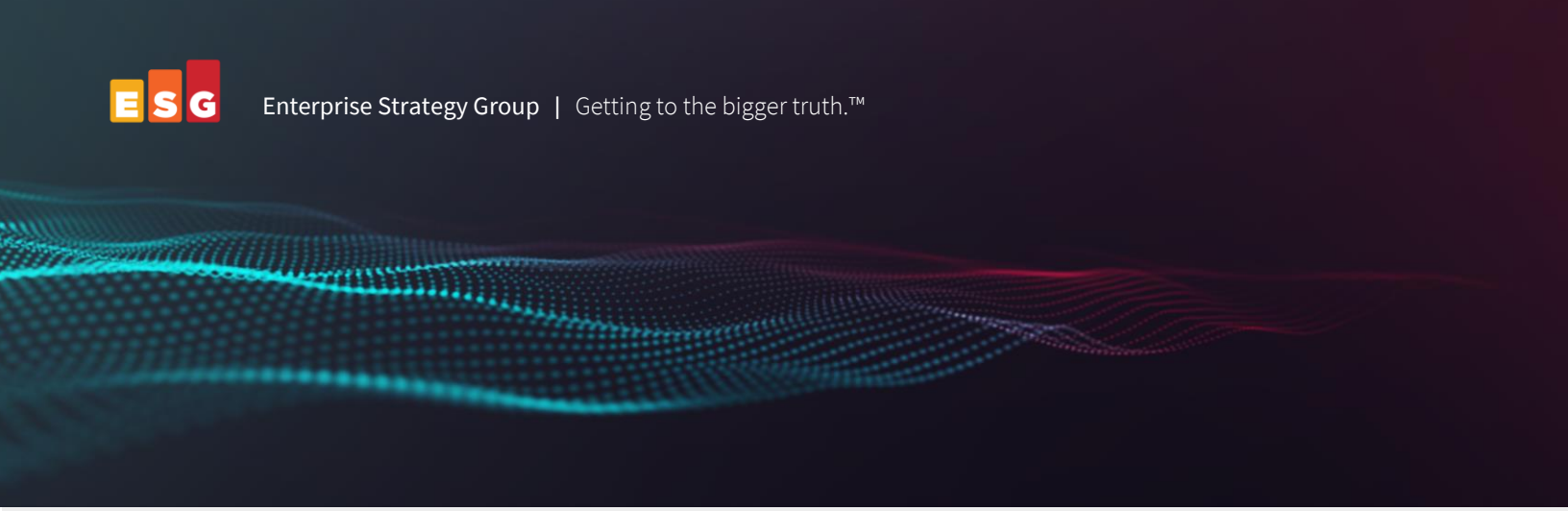


ESG WHITE PAPER

Addressing the Security Gap in High Velocity Modern Application Development Cycles

The Value of Having an Arsenal of Ethical Hackers to Battle-proof Cloud Applications

By Melinda Marks, ESG Senior Analyst

January 2022

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

Contents

Executive Summary

In November and December 2021, ESG interviewed HackerOne customers from three companies. Discussions centered on how they are adapting their application security programs as they undergo business transformation, moving workloads to the cloud for faster development cycles. These interviews of CISOs and security engineers covered the tools and processes they have in place, the effectiveness of their programs, and their strategies for filling in any gaps.

Based upon these interviews, ESG concludes:

- Security teams are under pressure to update security for business transformation supporting remote work and faster development cycles. As organizations increasingly use cloud services and adopt cloud-native application development processes to reach new levels of productivity and innovation, security teams must modernize their security approaches to keep up. Development teams grow while smaller security teams are tasked with ensuring that the applications deployed are tested and secure. Catching any security issues before release is important to preserve brand integrity and to protect keep valuable customer and company data from being vulnerable to attack.

- Organizations are adapting their tools and processes as technology continues to evolve. With dynamic environments and ephemeral resources to protect, security teams face many challenges, including understanding the attack surface, identifying and tracking assets, implementing standardized compliance controls, establishing testing processes, and monitoring for attacks or anomolous behavior. Organizations use some security capabilities from their cloud service providers along with solutions from established security vendors, as well as startup companies who are taking new approaches for cloud-native environments. Organizations are implementing various solutions and processes across the software development lifecycle but realize that securing applications in cloud environments is new territory that is rapidly evolving. So they need additional help to ensure they can find and fix critical security flaws before they release their products.

- HackerOne is a trusted vendor for building an effective cloud application security strategy to ensure quality and trust of their products. The CISOs and security engineers recommended the HackerOne offerings as a way to better assess their attack surface and gain access to world-class security talent to identify security vulnerabilities that may be missed by other tools and processes in place. The HackerOne community of ethical hackers, who are security practitioners and/or security researchers, identify bugs and issues that would have been difficult for internal security teams to find on their own with their current processes and tools. The analysis and reports also provide data to help security leaders make informed strategy decisions.

As organizations move their workloads to the cloud and security teams work to put the right security processes and tools in place, HackerOne strenthens their security capabilities, giving them on-demand access to a global community of security experts to fully test their software before release. This helps them fix vulnerabilities before exposing their products to the the public, where an attacker could target their product and exploit security issues.

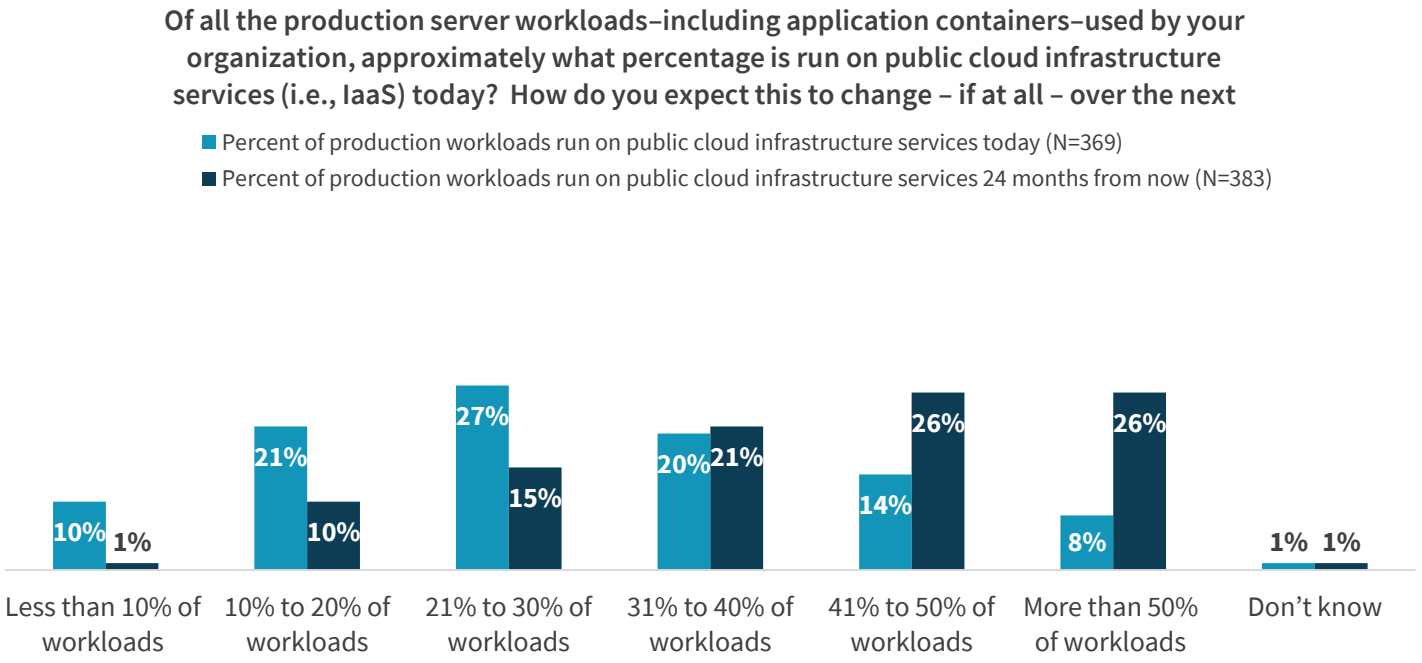
Customers reported the value of having HackerOne solutions identify bugs and issues that they could not have found themselves. They also described how HackerOne services create feedback loops so they can continuously adjust the tools and processes they have in place to more efficiently find and fix security flaws on their own. This helps organizations safely and efficiently move production workloads to the cloud.

Adapting Security for Business Transformation

Organizations are undergoing business transformation, utilizing cloud services to streamline their operations, improve customer outreach, and enable better collaboration among business users. The COVID pandemic has accelerated the move to the cloud, as the ability to adapt to remote work and an increase in online transactions have been crucial to organizations' success and revenue-driving efforts.

In ESG's annual survey of senior IT decision makers, 26% of respondents described their organization's digital transformation initiatives as mature, with several projects implemented and optimized, up from 22% last year. Another 47% are implementing and executing various digital transformation initiatives, with 95% of respondents using public coud services and 44% having a cloud-first policy for deploying new applications.[1] A separate ESG research survey also shows that organizations are increasingly shifting their production workloads to public clouds (see Figure 1).[2]

Figure 1. The Shift of Production Workloads to Public Clouds Continues

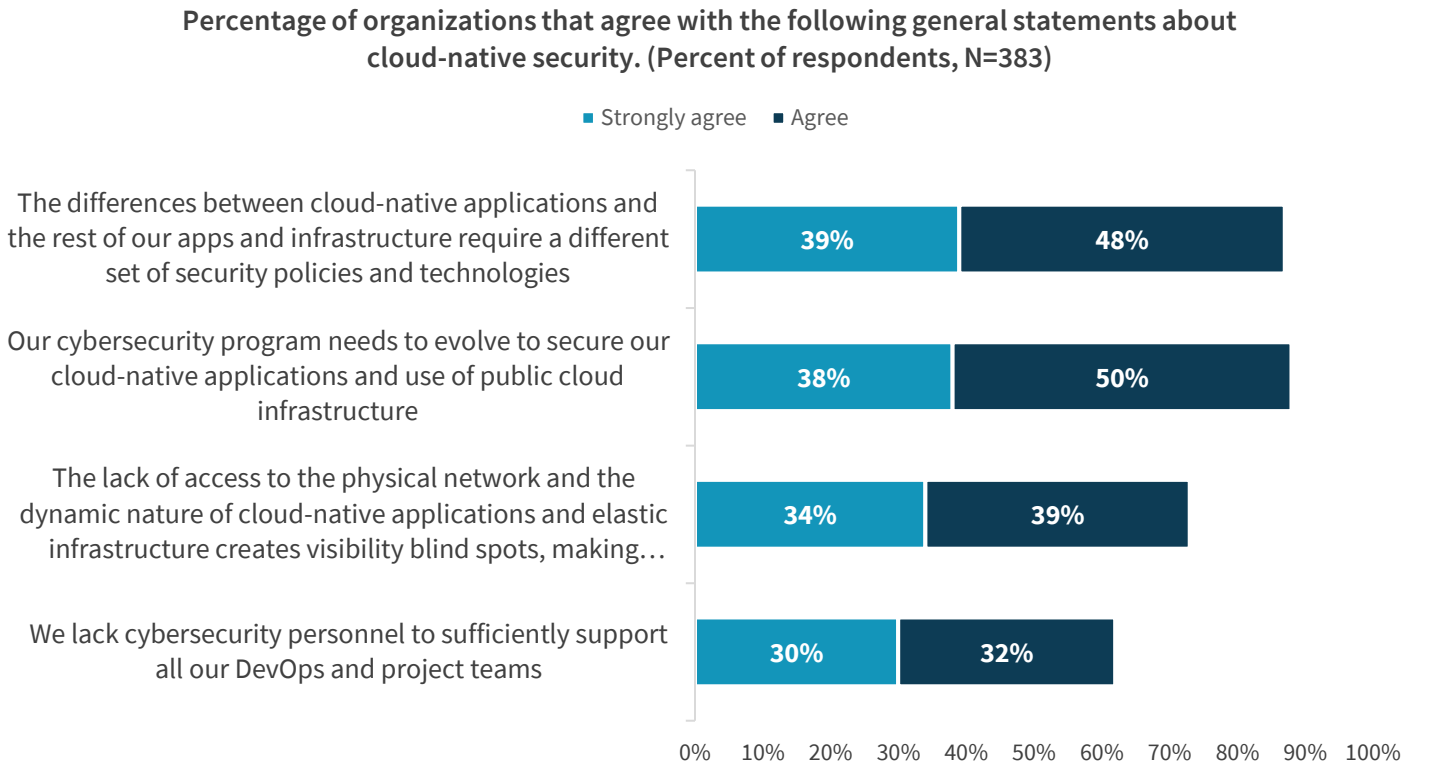


Source: Enterprise Strategy Group

But organizations face challenges adapting their security strategies to faster software development cycles leveraging continuous integration and continuous deployment (CI/CD) processes (see Figure 2).[3] As the development teams grow and scale with rapid product releases, it's difficult to incorporate security across the cloud-native technology stack in ways that don't disrupt CI/CD pipelines.

[1] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.
[2] Source: ESG Research Report, *The Maturation of Cloud-native Security*, May 2021.
[3] Ibid.

Figure 2. Security Needs to Catch Up to Cloud-native on Many Fronts



Source: Enterprise Strategy Group

Implementing Security Tools and Processes for Modern Software Development

The HackerOne customers interviewed by ESG described their approaches to adapting their security programs to deal with the scale and complexity of moving their software applications to the cloud.

- New evolving tech stack and changing attack surface. The microservices architecture for cloud-native applications brings agility because it provides the flexibility to dynamically spin resources up or down on demand as needed. But this also creates challenges for security teams to protect an ever-changing attack surface used by evolving development teams. The miccroservices can be packaged in containers or serverless functions across different architectures of public or private clouds. Immutable infrastructure and infrastructure-as-code (IaC) also add complexity, as the applications can be rapidly built or disassembled by users who may not always be up to speed on security policies.

> **"How cloud development is done is changing with regularity. The need to pivot and change approaches is significant—as we drive work in containers, getting visibility into containers is important. As we get to serverless and IaC, how do you scan IaC for issues? We're also using ML and AI….so it's a moving target."**
>
> - CISO, leading networking company

- Gap between self-sufficient developers and security teams trying to ensure applications are tested. Another advantage of cloud-native software development is that engineers are self sufficient; they don't have to wait for IT or development to set up infrastructure or resources for the applications that they are building. With the available tools and services, they can quickly provision, build, test, and deploy their applications. Newer "shift left" efforts include empowering developers to use security tools to test their applications, but developer knowledge and capabilities vary. While developers have an interest in delivering secure, reliable software, they aren't security experts and would rather focus on coding their applications. So security teams are implementing tools and processes in the CI/CD pipeline to incorporate testing in a way that does not slow development down.

> **"We're focused on shifting QA tests left into development. We have static code testing, application scanning, automatic scanning in the pipeline."**
>
> - Security Engineer, software company

> **"Applications can't move to the cloud unless they meet what we call our toll gates. We have 14 different security controls now that they have to operate within before they're allowed to move. So I'm using the cloud to drive hygiene and governance around following policies and standards."**
>
> - CISO, Global 500 insurance company

- Utilizing policies as guardrails for safe development. As developers are focused on building their code and security doesn't want to interrupt or slow them down, security teams are setting policies as a nondisruptive way to prevent developers from taking unwanted actions as they work. Cloud providers offer sets of policies and frameworks to apply. Additionally, organizations can access open source and vendor tools for setting up and applying policies in the developers' integrated development environment (IDE). This helps ensure proper setup and configuration, putting appropriate processes in place while preventing violations from being deployed.

- Using static application testing without slowing development cycles. Organizations are using a mix of vendor solutions along with some free and/or open source testing tools to help developers perform different types of static testing on their code, including scanning their application code, their open source code and their IaC.

  But they vary in ease of use and setup; if it doesn't work in developer workflows, or if it takes to long to run, developers may want to skip the testing processes. Result quality, including frequency of false positives, also varies, making it frustrating for developers if they need to spend time fixing something that is not a real issue. It can also be difficult to interpret the results or understand what is needed to remediate the detected issues. Another shortcoming is that scanning tools are based on previously discovered vulnerabilities instead of identifying new vulnerabilities, so they can miss critical application flaws.

> **"We try to gather information if we need a vendor tool. We're also big on innovation, so we're creating a lot of our own stuff. We may use some of the open source to provide a data element to a larger technology platform that we're building in house."**
>
> - CISO, Global 500 insurance company

- Catching security issues before deploying them to runtime significantly reduces risk. Security teams are evaluating or using cloud security posture management (CSPM) tools to detect security issues in runtime that expose risk. For example, they can detect misconfigurations, such as an open S3 bucket, or missing encryption at rest, which could expose valuable customer or company data. But if security is only catching these issues in runtime with a monitoring tool, by the time such a tool identifies a problem, the application, and the risk, is already deployed where it can be exploited. It is time consuming for the security team to detect the issue, track it back to the developer owner, and work with them to fix it. It is much more efficient to find and fix the issues as early as possible, especially preventable mistakes, such as misconfigurations. Although CSPM tools can be useful for discovering misconfigurations in runtime, HackerOne customers dicussed how they aim to reduce risk and costs by catching issues earlier in development to prevent them from being deployed in production. Once in production, vulnerabilities can be identified by customers or targeted by bad actors, exposing valuable data.

> **"As the applications are running, the [posture management] tool is something you use to determine if there's a misconfiguration or coding error. We plan on using it [for] real-time monitoring, but also as an enforcement mechanism. Once we operationalize it, we will move to a governance construct."**
>
> - CISO, Global 500 insurance company

> **"How can you consider yourself a prudent security professional in the cloud when the cloud is so new? We've got smart people moving into cloud, but understanding the cloud discipline takes a couple of years."**
>
> - CISO, Global 500 insurance company

- Defensive cloud application skills untested or unavailable. As cloud-native technologies continue to evolve, it can be a challenge to find staff with expertise in new and emerging areas, such as container security, cloud provider security capabilities, Kubernetes, Javascript, IaC (such as Terraform and CloudFormation), custom APIs, managing access and entitlements, and web application security. It can be difficult to recruit and maintain skilled staff across these different areas, as it is difficult to keep them battle-tested as new threats emerge.

Using HackerOne to Ensure Applications Are Safe From Attack

As organizations move their applications to the cloud and are still plugging in the right security processes and solutions across the software development lifecycle, HackerOne services fortify their capabilities to ensure their applications are secure when released. They offer vulnerability disclosure to help developers fix issues early, vulnerability management to help security teams remediate vulnerabilities quickly, bug bounty programs, and penetration testing services to battle test applications. This helps security and product teams fix issues before a malicious attacker can exploit them, which, in turn, helps organizations more quickly and safely undergo business transformation to the cloud, more effectively use their other security solutions, and integrate services in cases where they go through mergers and acquisitions.

Here are the ways that HackerOne customers reported that they are using their services:

- Security Testing and QA. Although these companies are putting security tools and processes in place—such as setting policies, automating testing in development, and monitoring in runtime to detect issues in their digital products—they are using HackerOne services to enhance these processes and to detect critical flaws that their other tools may have missed.

  With HackerOne, they have access to a global community of security experts who can identify security vulnerabilities so issues can be fixed before products are released. HackerOne enables the hacker community to find the vulnerabilities that automated tools often miss but that malicious actors would likely find.

- Staff augmentation. Security teams are vastly outnumbered by growing development teams. As mentioned earlier, companies are challenged recruiting experienced staff members who are skilled with newer technologies and the latest attack methods.

> **"There's no way that we as an individual security team have the same kind of footprint as a worldwide hacker community. It's valuable to use the HackerOne service as a way to bring in hackers to evaluate our products instead of blindly releasing it and hoping that it stays secure."**
>
> - Security Engineering Manager, software company

The CISO of a leading insurance company described how HackerOne provides a valuable service that gives him access to experienced, skilled security practitioners who provide an objective, fresh approach to improving their security posture.

For an innovative software company, the security engineers said that with an expanding portfolio, there's no way that their internal team can scale to match a worldwide hacker community. They said they use the HackerOne community as an extended red team to evaluate security risk in their products. Although they test internally, they find that HackerOne programs can more efficiently detect product security issues, freeing up time and resources for internal staff while effectively preventing cybercriminal exploits.

> **" The HackerOne community brings a diversity of thought and attack that is hard to get internally or by hiring pen testing teams."**
>
> - CISO, leading networking company

- Gaining an assurance partner. The insurance company CISO discussed how it may take a few years to fully understand security for the cloud as new technologies and security solutions continue to emerge. He described how they use some open source tools, some newer solutions from startups, and solutions from established vendors. But he is constantly evaluating their effectiveness and utilization and whether the tools can be more effectively and efficiently used when they are integrated. For example, if you have a vulnerability management solution, you may want to enrich it with threat intelligence.

  So he is using HackerOne as a way to measure the effectiveness of his programs and efforts, including setting policies and integrating testing in development. He also uses HackerOne to validate the security effectiveness of their Web Application Firewalls (WAFs).

> **"My vendors know that if I'm not using your tools 90% or above, you're at risk of being displaced. I will work with teams to make sure we're using the tools at the highest level possible. HackerOne helps us see how well we're doing with everything, so I would call them an assurance partner."**
>
> - CISO, Global 500 insurance company

- Gap analysis for identifying and fixing security program weaknesses. The customers interviewed also described how using HackerOne services provides a feedback loop for program improvements. When the ethical hackers find vulnerabilities and provide their analysis, it gives security teams the information they need to make security program improvements, such as improving scanning tools or modifying threat models to proactively reduce risk. The services help them identify and understand changes that could be made to prevent security incidents, helping them put processes in place that have a high impact on reducing risk.

> **" Subdomain takeovers were the most common issues coming in through bug bounty. We developed tooling to detect unused subdomains. We've cut down the number of issues to about 90% from the last review which we did."**
>
> - Security Engineer Manager, software company

HackerOne helped the software company analyze many of the common vulnerabilities that were discovered and create the right mechanisms to catch and fix those issues themselves. For example, they discovered a common flaw that allowed subdomain takeovers which can lead to significant breaches. The internal team was able to set up automated scans of assets for unused subdomains, helping them drastically reduce their threat risk.

- **Measurable results.** Those interviewed described the value of HackerOne for effectively detecting security issues that they would not be able to find on their own and for providing access to a strong set of global security experts. Adding horsepower to their ability to detect vulnerabilities enables them to remediate issues, saving them the cost of fraud, data loss, and brand mistrust that might have occurred with an attack.

  They also described that the service saves them money by giving them access to an extensive pool of leading pen testers and ethical hackers that regularly battle-test their applications. If a new project comes up, such as the need to test a high risk application, instead of the expense and time of recruiting additional staff, they can work HackerOne for red teaming to assure fast and comprehensive results.

> **"It's something that every organization should have. It gives us assurance of risk identification and prioritization. They are showing real results, demonstrating where I have risks to help me drive decision processes…."**
>
> – CISO, Global 500 insurance company

> **"HackerOne found issues that we had… When the the bug bounty finds stuff, and my team says 'that's brilliant that they found that; I never would have thought of that attack,' that's where the value is."**
>
> – CISO, leading networking company

The CISO for the insurance company also described how the analysis from HackerOne helps him make better security decisions using data from their findings. For example, he has been able to decommission applications or reevaluate how to get more value out of underutilized security tools.

The Bigger Truth

The HackerOne services are helping businesses safely move their applications to the cloud to reach new heights of productivity and scale. As cloud-native technologies and attack methods continue to evolve, security is also evolving to protect these new ephemeral resources and keep up with rapid software development cycles.

As security teams adapt their approaches to fit modern software processes, they face challenges evaluating and deploying the tools to secure applications in cloud environments. Cloud providers are offering some security controls and services traditional security vendors are updating their application security offerings, and startups are introducing new approaches built for cloud-native environments.

HackerOne has been a valuable solution and trusted partner to help companies best use their security tools and ensure their applications are secure with the move to the cloud. The HackerOne platform provides the connective tissue for security across the software development lifecycle. It incorporates human ingenuity, continuous testing, tighter development feedback loops, and direct insight to make the best security decisions that reduce risk.

Security processes and tools, including vulnerability management, policy control, process automation, and the use of ML and AI, are table stakes for security programs to filter out bulk vulnerabilities. HackerOne can fortify an organization's security strategy with targeted security programs and a diverse community of ethical hackers that pinpoint the hard-to-find weaknesses that cyber-criminals could exploit. HackerOne also helps them optimize their solutions and processes to continuously make improvements so they can efficiently find and fix security flaws across their software development lifecycle.

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