



ESG WHITE PAPER

Securing a Remote Workforce with a Zero-trust Strategy

By Doug Cahill, ESG Senior Analyst, and John Grady, ESG Analyst

June 2020

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



Contents

Executive Summary	3
Work-from-home Policies Have Expanded the Identity Perimeter	3
The Identity Perimeter Spans Hybrid, Multi-clouds	3
The Increase in Remote Work Will Transcend the Pandemic	4
VPN Limitations Complicate Secure Access	5
Cyber Adversaries Are Exploiting the COVID-19 Pandemic	6
The Role of Zero-trust as a Strategic Framework	7
The Principles of Zero-trust	7
The Zero-trust Continuous Lifecycle	7
Deliver the Digital Workspace	8
Secure the Devices	9
Secure Access	9
Protect Against Threats and Data Loss	10
Monitor User Activity	10
Recommendations for Getting Started on a Zero-trust Implementation	11
The Bigger Truth	11

Executive Summary

Knowledge worker mobility and the broad adoption of cloud services have challenged traditional “castle and moat” approaches to cybersecurity for some time now. The sudden surge in remote work and the associated direct-to-cloud consumption of SaaS applications have further challenged the role of the physical perimeter in providing secure access to a range of business applications. With users also requiring access to on-premises applications, IT and cybersecurity teams are now charged with providing secure access to resources across a hybrid, multi-cloud environment. This remit necessitates revisiting how we think of the perimeter and reevaluating existing approaches and controls.

Virtual Private Networks (VPNs) have long provided the means of remote access, but the access requirements of today’s remote workforce expose notable limitations. The needs to seamlessly support access to both cloud and on-premises applications, enforce fine-grained policy for users, and incorporate contextual information such as endpoint posture assessment are some of the key reasons why organizations are moving away from VPNs. And because VPNs require, by definition, that endpoints be connected to the corporate network, unmanaged, infected devices represent a risk of introducing threats.

A strategic approach to secure access that meets the requirements of all stakeholders—a frictionless experience for end-users, operational efficiency for IT, centralized policy and distributed enforcement for cybersecurity, and attractive economics for CFOs—is required. Zero-trust as an approach to implementing least privileged access policies is emerging as a foundational cybersecurity construct for securing the modern workplace, and for good reason: Enterprises need a

Zero-trust as an approach to implementing least privileged access policies is emerging as a foundational cybersecurity construct for securing the modern workplace.

strategy to secure the use of both cloud and on-premises applications that enables business agility. Toward that end, zero-trust has a central role in enabling the business outcomes that are top of mind for all IT and cybersecurity leaders: enabling mobility, improving threat detection, and preventing data loss while providing the framework for new initiatives such as data analytics and the use of IoT devices.

However, a lack of prescriptive specificity on implementing a zero-trust program has created confusion. This paper offers a zero-trust framework as a way forward for securing today’s remote workforce while supporting the business workflows that rely on the extensive use of cloud services and collaboration with colleagues and third parties alike.

Work-from-home Policies Have Expanded the Identity Perimeter

The hybrid, multi-cloud composition of the modern data center has made IT more complex. Indeed, nearly two-thirds of IT decision makers believe that IT has gotten more complex over the last two years, and 26% of these respondents attributed this increased complexity to the need to use both on-premises data centers and public cloud providers.¹ But amid such complexity is one constant: the end-user.

The Identity Perimeter Spans Hybrid, Multi-clouds

Many employers have long been supportive of working from home, providing the requisite technology to maximize the productivity of remote employees. An increase in “gig workers” (independent contractors) has contributed to the need for remote access to corporate applications and data. Stay-at-home orders in response to the COVID-19 pandemic have

¹ Source: ESG Master Survey Results, [2020 Technology Spending Intentions Survey](#), January 2020.

resulted in an average of 76% of knowledge workers working from home, creating an overnight requirement to support remote work at scale.²

IT and cybersecurity teams are charged with not only operationalizing this new normal of work, but also securing an expanded perimeter. While remote users are utilizing more cloud apps than ever, those same users need secure access to applications and data within the corporate network. As such,

Today's perimeter is characterized by the identity of the users requiring access to both cloud and on-premises applications and data.

today's perimeter is characterized by the identity of the users requiring access to both cloud and on-premises applications and data. Identity, however, is about more than credentials; it is contextual, based on behavior, device, and the criticality of the application and data being accessed.

The shift to remote work has put a greater emphasis on the device. In fact, 24% of the knowledge workers who participated in a recent study on their experience working from home during the pandemic lockdown shared that they are now using a personal device while working from home, highlighting the role of one's device in establishing identity.³

The Increase in Remote Work Will Transcend the Pandemic

What about the workers themselves? For 75% of the knowledge workers surveyed, the work-from-home transition has been a smooth experience; although many still experience pain points, such as connectivity and access to applications. A quarter shared that connectivity was the area in which their organization was the least prepared to support them working from home. Not surprisingly, an increase in the use of cloud applications is led by a notable uptick in the use of collaboration tools, messaging applications, and online meeting platforms.⁴

Recent research conducted by ESG explored the challenges and go-forward strategies for securing remote workers. Of the IT decision makers (ITDMs) who participated in the study, 29% shared that their organization was underprepared to provide access to the applications used by remote employees. Securing a remote workforce's access to those applications is clearly a concern, with 36% citing increased cybersecurity vulnerabilities resulting from more remote users as one of the biggest challenges supporting those remote users. Two of the top cybersecurity challenges associated with having more employees work from home are directly related to secure access: developing and adjusting security policies (which would include access policies), and scaling up network security controls such as gateways to accommodate the increase in network traffic (see Figure 1).⁵

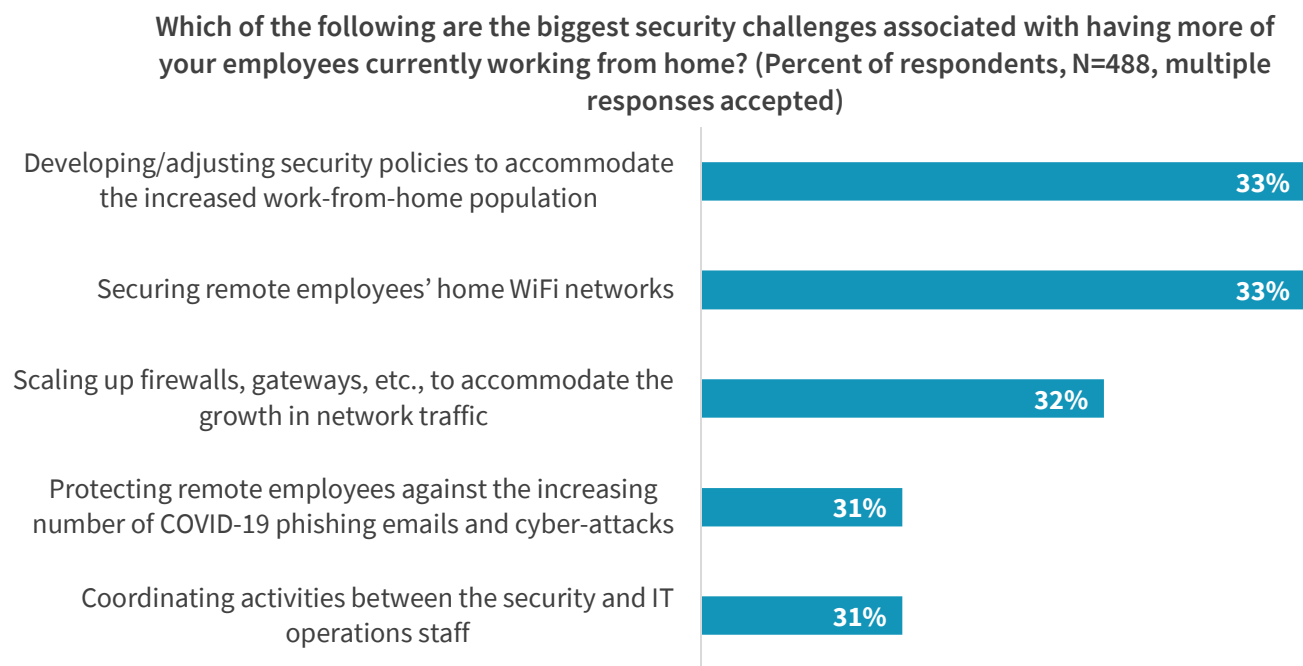
² Source: ESG Master Survey Results, [Technology Impact of COVID-19: IT Decision Maker \(ITDM\) View](#), May 2020.

³ Source: ESG Master Survey Results, [COVID-19 Technology Implications for Knowledge Workers](#), May 2020

⁴ Ibid..

⁵ Source: ESG Master Survey Results, [Technology Impact of COVID-19: IT Decision Maker \(ITDM\) View](#), May 2020.

Figure 1. Top Five Security Challenges with Remote Employees



Source: Enterprise Strategy Group

It is encouraging, however, that employees are staying productive, with more than three-quarters (78%) saying they are as productive if not more so working from home. From a productivity perspective, at least, remote work has been positive, with a notable 57% of knowledge workers saying the experience has taught them that they can do a lot of their job from home and they're interested in doing so more frequently moving forward.⁶ And their IT organizations are supportive, with 79% of IT decision makers saying their organization will be more flexible with work-at-home policies once the pandemic subsides.⁷

VPN Limitations Complicate Secure Access

For most organizations, the corporate VPN remains synonymous with remote access, and is subsequently the main focus of efforts to support expanded work-from-home initiatives. As such, the challenges cited by our research respondents indirectly highlight some of the limitations of current VPN solutions. Even prior to COVID-19, many organizations were beginning to consider alternative solutions that scale elastically with usage and provide more centralized, granular, and contextual control over application access. Some of the specific pain points associated with VPN infrastructure include:

- **Scalability.** VPNs are typically constrained by a ceiling of concurrent sessions, with further capacity requiring the purchase and deployment of additional appliances. As such, a VPN is typically architected for baseline use with no real “burst capacity” available generally, let alone in an on-demand fashion.
- **Cost.** Directly related to scalability is the cost associated with traditional VPNs. As more of the industry shifts to a cloud-delivered, operational expense-based model, VPNs usually require a capital investment in hardware.
- **Complexity.** In addition to the capital cost associated with VPNs, there is also operational cost driven by the complexity of managing silos of VPN infrastructure. Those silos are created by a requirement to support access to

⁶ Source: ESG Master Survey Results, [COVID-19 Technology Implications for Knowledge Workers](#), May 2020.

⁷ Source: ESG Master Survey Results, [Technology Impact of COVID-19: IT Decision Maker \(ITDM\) View](#), May 2020.

applications and data resident across multiple data centers and multiple public clouds via a multitude of VPN appliances that need to be manually configured and updated. This deployment model also creates a policy management challenge; absent a centralized control plane, IT and security teams must replicate policies across VPNs to assure consistency.

- **Policy.** Many VPNs provide only coarse-grained access to the network itself, with limited visibility or control over applications. While secure sockets layer (SSL) VPNs can provide a more application-centric approach, the lack of cloud optimization is a key issue. Ultimately, VPN approaches are not well suited to support a least privileged approach as they cannot employ fine-grained entitlement policies; apply user, device, and other context to inform policy decisions; or provide detailed visibility into user activity relative to applications. The need for more prescriptive policies is even more important when users are accessing applications on unmanaged or personal devices.
- **Performance and end-user experience.** The latency introduced by backhauling VPN traffic from the user's device through the campus data center can negatively impact end-user performance, especially for traffic destined for cloud applications, as well as raise employee privacy concerns around users surfing the internet in their own personal time. Options such as split tunneling to push internet-bound traffic directly to the destination may improve performance and resolve some privacy concerns but limits visibility and control for security enforcement.

In short, VPNs were well designed for the traditional “castle and moat” network architecture, which relied on the implicit distinction of users and entities on the network being trusted. However, in today's decentralized, cloud-centric architecture, the approach can introduce potentially critical security gaps.

Cyber Adversaries Are Exploiting the COVID-19 Pandemic

Ever opportunistic, cyber adversaries are exploiting the pandemic, as evidenced by nearly half of ITDMs who shared their organization has seen an increase of cybersecurity attacks since the COVID-19 quarantine and related work-from-home period started.⁸

Preying on end-user behavior is standard operating procedure for cyber-criminals, and the massive rise in remote users has expanded the set of targets. Of particular note are account take over (ATO) attacks in which a phishing email lures a user to a bogus login page under a false pretense, such as the need to update their password, as a means to steal their credentials. Such credentials are then employed to secure a beachhead and move laterally across a set of connected cloud applications and within on-premises infrastructure from an application to a domain controller or data store.

Preying on end-user behavior is standard operating procedure for cyber-criminals, and the massive rise in remote users has expanded the set of targets.

Nation state actors are also active amid the pandemic. The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) issued a press release⁹ in May warning of activity indicating nation states have been observed targeting personnel and organizations researching the coronavirus in attempts to steal intellectual property related to COVID-19 research.

Given this reality of the threat landscape, knowledge workers and cybersecurity teams will need to be as vigilant as ever. A zero-trust approach should be central to doing so moving forward.

⁸ Source: ESG Master Survey Results, [Technology Impact of COVID-19: IT Decision Maker \(ITDM\) View](#), May 2020.

⁹ FBI National Press Office Press Release, [People's Republic of China \(PRC\) Targeting of COVID-19 Research Organizations](#), May 2020.

The Role of Zero-trust as a Strategic Framework

The notion of zero-trust has cultivated a discussion around a flawed trust model, one based on “trust, but verify” in which many too often establish trust, but don’t verify. Given this shortcoming, zero-trust is meant to convey a “default-deny” approach that assumes everyone and everything is a threat, changing the trust model to one of “never trust, continuously verify.”

While the initial incarnation of zero-trust, going back 8 years, did contemplate knowledge worker mobility, it preceded today’s extensive use of cloud applications. As such, an expanded view of the concept is in order: A zero-trust strategy can serve as a strategic framework to secure access for any user on any device from any location at any time to any application, with fine-grained policies and continuous monitoring.

The Principles of Zero-trust

Zero-trust cannot, of course, be taken literally. After all, users have to be trusted to do their job. The question is about how trust is earned and continuously verified while the privileges associated with granting trust are minimally scoped. As such, the core principles of a zero-trust strategy to secure the identity perimeter include:

- **Frictionless** but deterministic authentication to balance the user experience with strong authentication.
- **Just enough privileges** to perform a given task.
- **Observability** of user behavior and activity.

A zero-trust strategy can serve as a strategic framework to secure access for any user on any device from any location at any time to any application, with fine-grained policies and continuous monitoring.

The Zero-trust Continuous Lifecycle

Zero-trust as a concept was certainly prescient in its applicability as a way forward to secure today’s expanded identity perimeter. To employ zero-trust as a strategic approach to implement least privileged practices, a methodology is in order. As such, the following steps represent such a framework for an identity-centric implementation of zero-trust:

- **Deliver the digital workspace:** The provisioning and unification of secure digital workspaces and applications that include SaaS, web, virtual, traditional 2-tier, and mobile applications as well as remote access to user desktops running on their physical PC in the office.
- **Secure the devices:** Operationalizing the management and security of corporate managed, unmanaged, and employee-owned BYO devices used to access applications and data.
- **Secure access:** Securing access to both cloud and on-premises applications via single sign-on (SSO), software-defined wide-area networks (SD-WANs), multi-factor authentication (MFA), and adaptive authentication.
- **Protect against threats and data loss:** The use of layered threat prevention controls such as web filtering, and remote browser isolation (RBI) as well as data loss prevention controls such as data discovery and classification as the basis for usage policies.
- **Monitor user activity:** Activity monitoring of users and systems to detect anomalous activity.

And because today’s IT environment is constantly changing, trust needs to be continuously vetted without friction. As such, these phases should be thought of as continuous steps (see Figure 2).

Figure 2. The Continuous Steps of an Identity-centric Implementation of Zero-trust



Source: Enterprise Strategy Group

Deliver the Digital Workspace

Irrespective of the device being used, end-users need a fully functional digital workspace to maximize their productivity, including office productivity and collaboration applications used by nearly all businesses as well as those that are industry-specific. As such, businesses using different portals and ways to access their applications, whether they are SaaS, internal web-based, traditional 2-tier, mobile or virtual applications, or other resources like remote access to physical desktops, need to unify access to these resources within the same workspace.

Digital workspaces meet these requirements, providing knowledge workers a VPN-less cloud service to deliver access to a range of applications. Such a unified approach also allows IT teams to centrally manage, configure, and secure these environments, rendering issues such as configuration drift irrelevant.

In addition to providing a frictionless experience for the end-user and operational efficiency for IT teams, a virtualized digital workspace also enables compelling security use cases.

In addition to providing a frictionless experience for end-users and operational efficiency for IT teams, a virtualized digital workspace also enables compelling security use cases. Keystroke loggers, which are more likely to be present on unmanaged and BYO devices, are used by cyber adversaries as a means to capture login credentials to take over accounts. Virtualizing the applications running on a digital workspace obfuscates the end-user keystrokes, rendering the input captured by the keystroke loggers useless. Bad

actors, both insider and external, may also employ screen captures as a means to steal sensitive data. Another benefit of the centralized control of the applications running on digital workspaces is the ability to block the ability to capture screen renderings.

Secure the Devices

The devices used by knowledge workers to access corporate resources should be viewed as a core aspect of their identity. In that context, accessing a diverse portfolio of applications from managed, unmanaged, and bring-your-own (BYO) devices represents both operational challenges and cybersecurity concerns. Unified endpoint management (UEM) solutions should be leveraged for the centralized and consistent management of a diverse range of endpoint devices to assure consistent configurations, and device-level application access and data usage policies.

Given the increase in contractors and remote workers that is resulting in an increase in the use of personal devices, it is important to consider that these unmanaged devices may be infected. To protect the introduction of threats into the enterprise by these devices, organizations should look to sandboxed environments, including remote browser isolation (RBI), as a way to securely allow such devices to connect to corporate applications.

Secure Access

Research conducted by ESG highlights the challenge of providing remote access to applications across a hybrid, multi-cloud environment, with inconsistent management across physical and cloud/virtual environments cited by 44% of respondents as a top access control and management challenge.¹⁰ To address this issue, a unified and adaptive approach to authentication is required, one that spans all of the applications to which a user needs access. Enter the role of a gateway.

A single sign-on (SSO) gateway and web proxy working in concert, deployed in a DMZ or delivered from the cloud, allows for the secure access to and authentication of a range of cloud and on-premises applications. The use of an SSO gateway allows for the centralized control of policies for all security assertion markup language (SAML)-enabled applications. SSO gateways also help prevent lateral movement via stolen credentials by only allowing connections from an SSO gateway, preventing pivoting from one server to another. Elastic cloud gateways (ECGs) are emerging as a compelling evolution of secure web gateways (SWGs). ECGs are cloud-delivered gateways based on a cloud-native architecture that automatically scale, offer centralizes policy management, and provide secure access to a range of applications as well as websites.

Given the increase in contractors and remote workers that is resulting in an increase in the use of personal devices, it is important to consider that these unmanaged devices may be infected.

SSO gateways help prevent lateral movement via stolen credentials by only allowing connections from an SSO gateway, preventing pivoting from one server to another.

Multiple factors should be used as a second challenge to authorize a user to access applications and data sets that an organization deems sensitive or business-critical. Research respondents agree, with 35% citing MFA as a top area in which their company has made or plans to make changes to secure access to certain cloud services.¹¹ The actual types of factors used for primary and secondary authentication are varied and include biometrics, geo

location, and the profile of the user's device, as well as hardware token and SMS texts. In addition to use of MFA for access to critical resources, MFA should be used in an adaptive context such as detecting an anomaly in user behavior.

¹⁰ Source: ESG Research Report, [The State of Network Security: A Market Poised for Transition](#), March 2020.

¹¹ Source: ESG Master Survey Results, [Enterprise-class Cybersecurity Vendor Sentiment](#), March 2020.

Protect Against Threats and Data Loss

Protecting against threats and data loss prevention are, of course, expansive topics, which this section will narrow by offering some considerations as they relate to secure access.

To protect against inbound threats, access to websites should be vetted via both static and dynamic analysis. URL filtering is a fundamental control for preventing access to known malicious websites while remote browser isolation (RBI) as an approach to dynamic analysis can help detect and prevent threats from new and unknown websites.

To protect against inbound threats, access to websites should be vetted via both static and dynamic analysis.

Discovery and visibility are foundational elements for cybersecurity methodologies. As such, discovering and classifying sensitive data serves as the underpinning for data loss prevention (DLP) policies to govern who has access to what data with what privileges. Data classification also enables an adaptive approach to multi-factor authentication in which a second factor of authentication is required for access to applications that hold an organization's most sensitive data.

Monitor User Activity

A core tenet of a zero-trust model is that trust must be continuously verified, which means user activity should be monitored to detect and protect against the 3 types of insider threat:

1. **The unwitting proxy** whose stolen credentials are used in a cybersecurity attack.
2. **The malicious insider** who is exploiting their knowledge or their company's IT environment to steal data or otherwise cause damage.
3. **The inadvertent insider** threat who unknowingly violates a policy, leading to the inappropriate sharing of sensitive data, unauthorized use of cloud apps, and more.

Activity monitoring for anomalous activities that could be indicative of malicious activity by any of these types of insiders include:

- **New geo IP location**, indicating a user's credentials are being used from a new location.
- **Time of day**, indicating a user's credentials are being used during a nonstandard time.
- **Application(s) being accessed**, indicating a user's credentials are being used to access an application they do not normally use.
- **Data being accessed**, indicating a user's credentials are being used to access data they do not need to do their job.
- **Data being downloaded**, indicating a user's credentials are being used to download an inordinate amount of data—a possible indicator of data exfiltration.
- **Use of unauthorized applications**, indicating an attempt to use a user's credentials to access an approved application that the user is not authorized to use, or the use of a shadow IT application that is not approved by the business.

Continuous monitoring also serves as a feedback loop to help organizations tighten up their IAM policies for a zero-trust implementation such as reducing privileges and requiring MFA.

Recommendations for Getting Started on a Zero-trust Implementation

While zero-trust has gained in awareness, there is confusion as to what zero-trust entails and how best to implement a zero-trust approach. In reality, no product singularly provides a zero-trust solution; there are only those that do their part to enable an architecture. With that in mind, it is useful to inventory existing solutions, assess their relevance to a zero-trust approach, and where possible, build off those to achieve quick wins. With a zero-trust framework in mind, organizations can take a series of initial steps to enable such a strategy:

- **Transition from VPNs** by starting to replace traditional VPNs by augmenting them with cloud-delivered gateways.
- **Leverage modern secure web gateways** to gain access to additional capabilities such as remote browser isolation.
- **Unify policies with a converged approach** that consolidates disconnected controls and secures the matrix of any user, any device, any application, at any time.
- **Make third-party integrations a requirement** by seeking solutions that integrate with the other controls in your cybersecurity stack for a defense-in-depth posture.

The Bigger Truth

The COVID-19 pandemic has challenged multiple aspects of IT while also creating new opportunities for cyber adversaries. The shift to an identity-centric perimeter was already underway, a trend accelerated by a surge in remote work. Some organizations were clearly better positioned to support an overnight shift to remote work than others, including those who already had a remote workforce and those with a progressive bring-your-own-device (BYOD) policy. The future of work may have arrived sooner than expected, and under dire circumstances, but silver linings have emerged including pragmatic approaches to zero-trust.

Zero-trust as an approach is a business strategy that enables the workstreams of the modern workplace.

Zero-trust as a framework can serve as a means to secure what has become a new normal: a remote workforce. A mature zero-trust program enables the critical business outcomes of remote work—seamless knowledge worker mobility, improved threat detection by limiting lateral movement, cost reduction by consolidating disparate points tools into converged solutions, data exfiltration

prevention, and more. In fact, a mature zero-trust implementation improves overall security efficacy as well as operational efficiency and supports digital transformation by securely enabling mobility, cloud, and IoT initiatives. As such, zero-trust as an approach is a business strategy that enables the workstreams of the modern workplace.




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