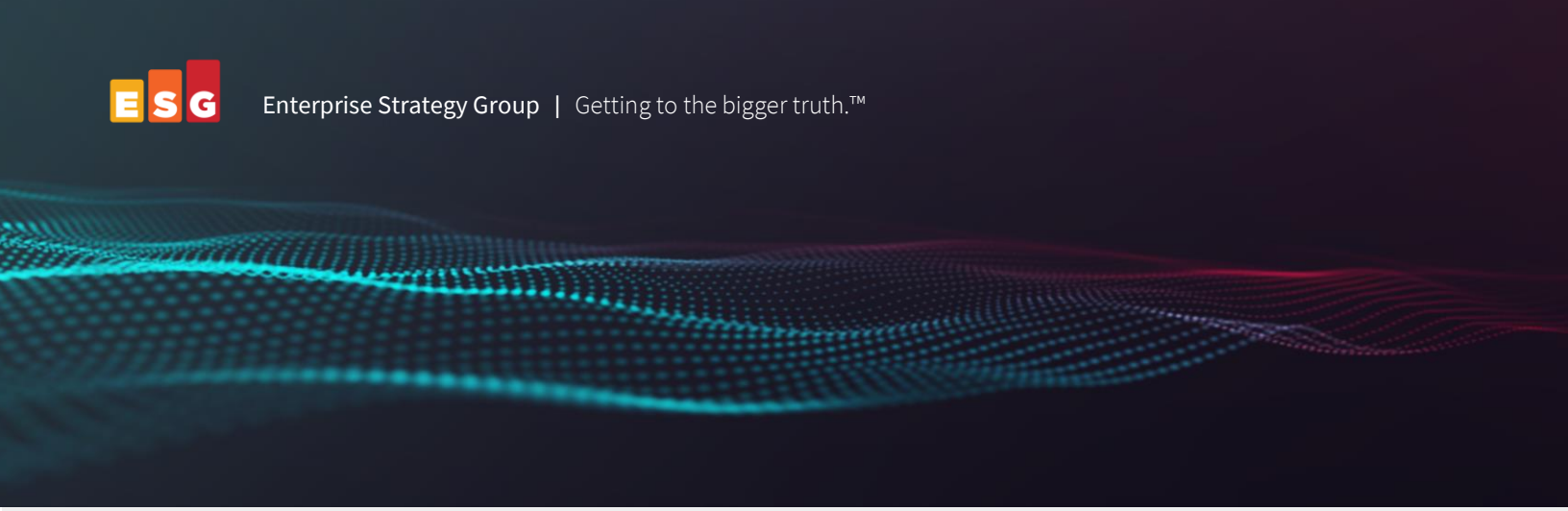


ESG WHITE PAPER

Strategic Zero Trust

Zero Trust Must Include the Workforce, Workloads, AND Workplace

By Jon Oltsik, ESG Senior Principal Analyst and Fellow; and John Grady, ESG Senior Analyst

January 2022

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

Contents

Executive Summary

Zero trust remains one of the hottest topics in IT and cybersecurity and has seen increased attention as organizations struggle to secure increasingly distributed environments. But the question remains: do users really understand zero trust technologies and where they fit? If so, are organizations deploying zero trust technologies and if so, to what end? These issues are explored in the pages that follow and ESG comes to the following conclusions:

- Zero trust remains confusing, and definitions fragmented. Cybersecurity and IT professionals continue to provide different definitions for zero trust, with most pointing directly to tools and technologies rather than a broader strategic approach. While zero trust can be beneficial to improve user access or segment data center traffic, a more comprehensive, strategic approach covering the workforce, workloads, and workplace is required.

- Zero trust can enable the business. Zero trust should start at the business level as a strategy to protect critical business processes. Security teams shouldn't eschew tactical projects but rather make them components of a broader business-centric strategy to protect critical business processes

- Workplace zero trust remains the biggest gap. Organizations are putting their efforts toward zero trust network access (ZTNA) for users or microsegmentation for application workloads while continuing to minimize the need to secure the workplace. While understandable given the acute need to provide secure access to remote users, this narrow approach does not meet the requirements of hybrid work, nor fit with an end-to-end business-driven zero trust strategy. Workplaces should be included to assure that endpoints connecting to the network are properly authenticated, authorization polices are uniformly applied before granting any access, and all devices are regularly monitored for policy compliance and behavioral anomalies. This is especially true for IoT and OT devices that require maximum uptime and performance for achieving business objectives.

The State of Zero Trust

It's important to anchor any discussion of zero trust with a common definition. Rather than create a new one, ESG defers to the NIST Zero Trust Architecture (NIST Special Publication 800-207, August 2020), which defines zero trust as follows:

Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows…Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.

Why the interest in zero trust? Because CISOs need more effective ways to control and protect the rapidly expanding attack surface. Rather than give assets access to the network, zero trust provides the ability to create least privilege trusted relationships between assets. Based upon customized granular policies, users, devices, and applications can gain access to assets they need to communicate with while being blocked from everything else on the network.

According to ESG research, many organizations are moving forward with a zero trust deployment as a means for mitigating cyber-risks. In fact, 46% of ESG research respondents say they have implemented or have begun to implement zero trust across the organizations, 43% report having implemented or begun to implement zero trust for specific use cases, and 10% say they are planning to implement zero trust in the next 12-24 months.[1]

[1] Source: ESG Survey Results, *The State of Zero Trust Strategies,* May 2021. All ESG research references and charts in this white paper have been taken from this survey results set.

While zero trust is garnering lots of new market attention, it's also important to realize that the roots of zero trust are based on many established technologies, like multifactor authentication, network segmentation, and network access control (NAC). It's safe to assume that many zero trust deployments will build upon past security initiatives as organizations move sensitive data to public cloud and SaaS infrastructure or allow access to sensitive applications from mobile devices.

Zero Trust Can Be Confusing

While many organizations are proceeding with zero trust initiatives, there remains some level of disagreement between security and IT professionals about what this concept entails. Zero trust is not a product or tool an organization can buy, but rather a strategy which seeks to remove any implicit trust from the network and incorporate more dynamic, risk-based access policies. Yet while a plurality of ESG research respondents agree that zero trust is a strategic approach, most continue to equate zero trust with tools and technologies for microsegmentation or secure remote access (see Figure 1).

Figure 1. Impressions of Zero Trust

Source: Enterprise Strategy Group

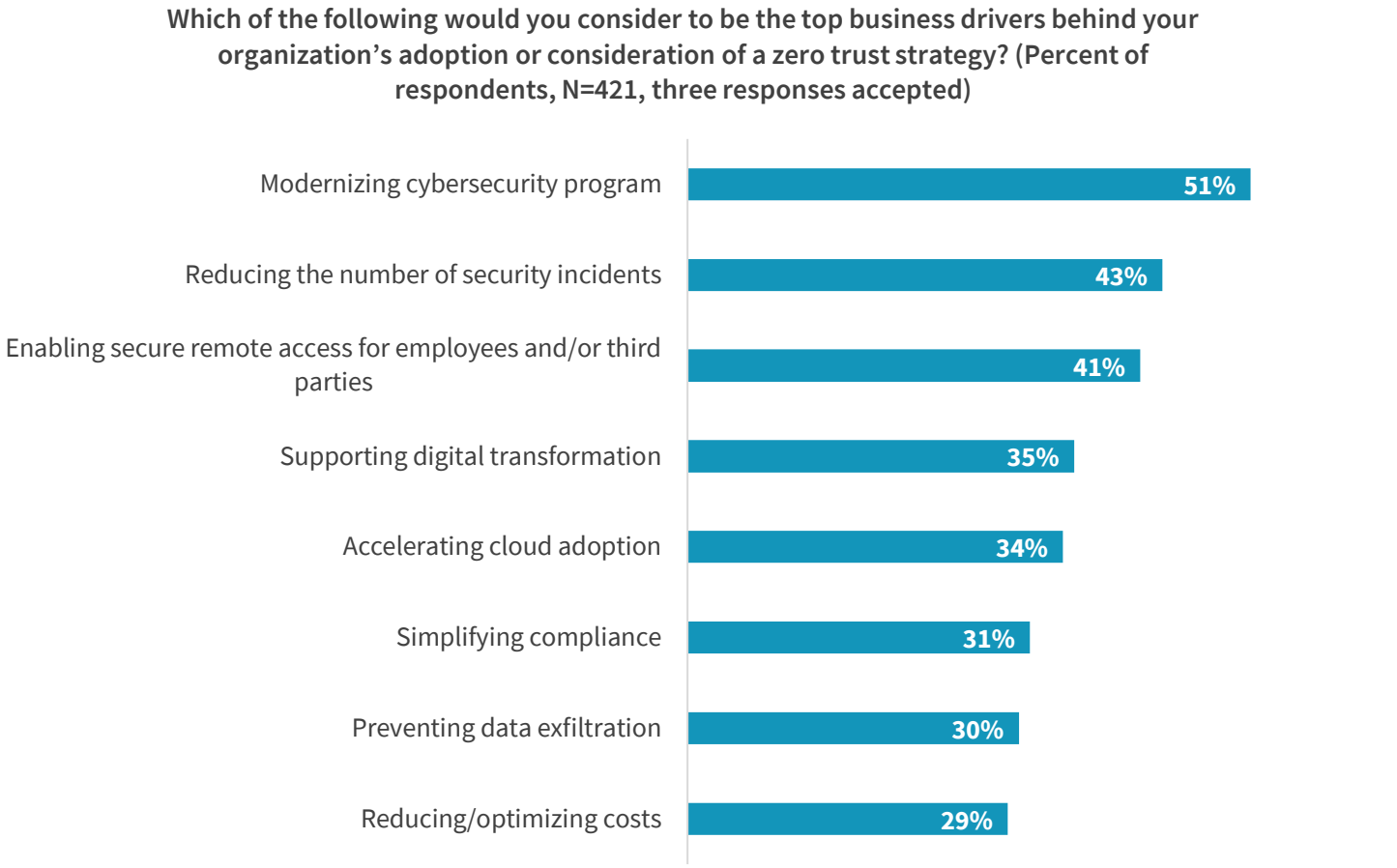
These definitions are important as they likely guide organizations' zero trust initiatives. Certainly, all three definitions are rooted in truth. Yet, because zero trust can be applied to the workforce (i.e., zero trust access), workload (i.e., microsegmentation of east/west traffic), and workplace (i.e., identifying and enforcing policies on every network device), it is helpful to start from a higher level, strategic perspective. Otherwise, a myopic view of zero trust can limit its reach, scope, and ability to help organizations manage the attack surface and mitigate cyber-risk.

Zero Trust Extends Beyond Security to Business Enablement

While the primary focus of zero trust is on security, organizations have begun to understand the positive impact zero trust can have on the business. ESG research has found that the majority of organizations (51%) view zero trust through the lens of modernizing their cybersecurity programs (see Figure 2). Yet while zero trust can be used to mitigate cyber-risk through

better management of the attack surface, there are business considerations as well. Specifically, 35% look at zero trust as a way to support digital transformation, 34% say it can help accelerate cloud adoption, and 29% cite reducing or optimizing costs as a zero trust driver.

Figure 2. Zero Trust Drivers



Source: Enterprise Strategy Group

In addition to supporting these strategic initiatives, zero trust can act as a forcing function to optimize business processes and ultimately reduce risk and improve resilience. Specifically, CISOs should work with business executives on more comprehensive strategies, because zero trust:

- Helps classify IT assets in relation to business criticality. Zero trust provides an opportunity for organizations to discover and classify all assets connected to a network. Armed with this information, CISOs can work with business executives to create a granular classification matrix of IT assets based upon their level of business criticality. These classifications can then be used as input for things like risk assessment, penetration testing focus areas, and security budget allocation. The goal? Prioritize resources, focus, and investments toward the IT assets that drive the business.
- Links network communications with business policies. Building on asset classification, zero trust initiatives force organizations to really examine which users and assets need access to business-critical systems and under what circumstances this access should be permitted. The CFO may need access to payroll information, but should she be permitted to access this data from an open Wi-Fi network on an unmanaged device? Asking questions and then creating and managing these types of access policies can help organizations mitigate cyber-risk and improve business process efficiency simultaneously.

- Aligns with identity governance and regulatory compliance. Zero trust access forces organizations to gain better visibility into users, their needs, and their behaviors. Aside from security, business managers can use this data to assess which assets employees are really using to get their jobs done. Compliance officers can also take advantage of zero trust to define and group users into defined roles, and then use this data to ease compliance reporting.

- Protects critical business processes. Aside from user access, zero trust can be used to discover and identify IoT and OT devices, map out their communications patterns, implement security controls, and monitor network behavior. By doing so, manufacturing companies can mitigate the risk of a disruption to their production lines while healthcare organizations can protect clinical systems used for patient care.

The Three Zero Trust Domains

ESG firmly believes that organizations that approach zero trust from business policy down to technology infrastructure can reap business AND security benefits. To do so, zero trust initiatives should be comprehensive, covering three distinct domains:

- Zero Trust for the workforce. Zero trust access is about providing a secure end-to-end tunnel so a user and/or device can connect directly to the applications and services they need to do their jobs and nothing more. Zero trust access is anchored by technologies like multifactor authentication, DNS, and network encryption. From a business perspective, zero trust access encompasses strict usage policies based upon roles and other factors. Zero trust access then enables good connections while eliminating bad connections.

- Zero Trust for the workload. While zero trust access is about securing north/south traffic, zero trust for workloads focuses on securing east/west traffic between applications, data, and services in a data center. Zero trust for workloads usually includes workload discovery, traffic pattern analysis and mapping, policy suggestions, and then technology controls for policy enforcement. In this way, zero trust for workloads helps organizations better organize and protect business-critical applications.

- Zero Trust for the workplace. While zero trust access and workload security get the majority of headlines, especially due to the focus on remote work and cloud adoption as a result of the pandemic, the shift to hybrid work models and subsequent return to the office only reemphasize the requirement for securing internal network traffic. Zero trust for the workplace also helps extend the workplace by securing trusted connections when remote users connect to internal assets like file servers physically located on corporate LANs. When users do return to corporate offices, they need common policies that consider user location and device type regardless of location. Furthermore, corporate networks are populated by IoT and OT devices like printers, sensors, and industry-specific systems like heart monitors, SCADA systems, and manufacturing robots. Threats to OT and IoT devices have amplified over the past few years, so zero trust for the workplace is increasingly important, driving the need for device authentication and traffic segmentation.

Zero Trust for the Workplace: What's Needed?

ESG has noticed that many organizations have accelerated digital transformation application development as a result of the global pandemic. These initiatives frequently include new types of IoT/OT devices, increasing the urgency of zero trust for the workplace. What's needed to support this? ESG believes that best practices for zero trust for the workplace should include:

- Device discovery, identification, and profiling. To paraphrase an old management adage, "you can't secure what you can't monitor and measure." In other words, zero trust for the workplace starts with an inventory of every device connected to the network. Zero trust technologies should accommodate this requirement by discovering all devices through deep packet inspection and identifying their role (i.e., printers, security cameras, clinical healthcare systems, etc.) by matching these profiles to the characteristics of specific types of network devices. Machine learning and analytics can also be employed here, looking at a multitude of device attributes that can be used for modeling and categorization. Figure 4 shows that 35% of organizations view analytics as a starting point for zero trust. The best technologies for zero trust for the workplace will be able to provide precise device details like device models, manufacturers, software levels, patches, and operating systems.

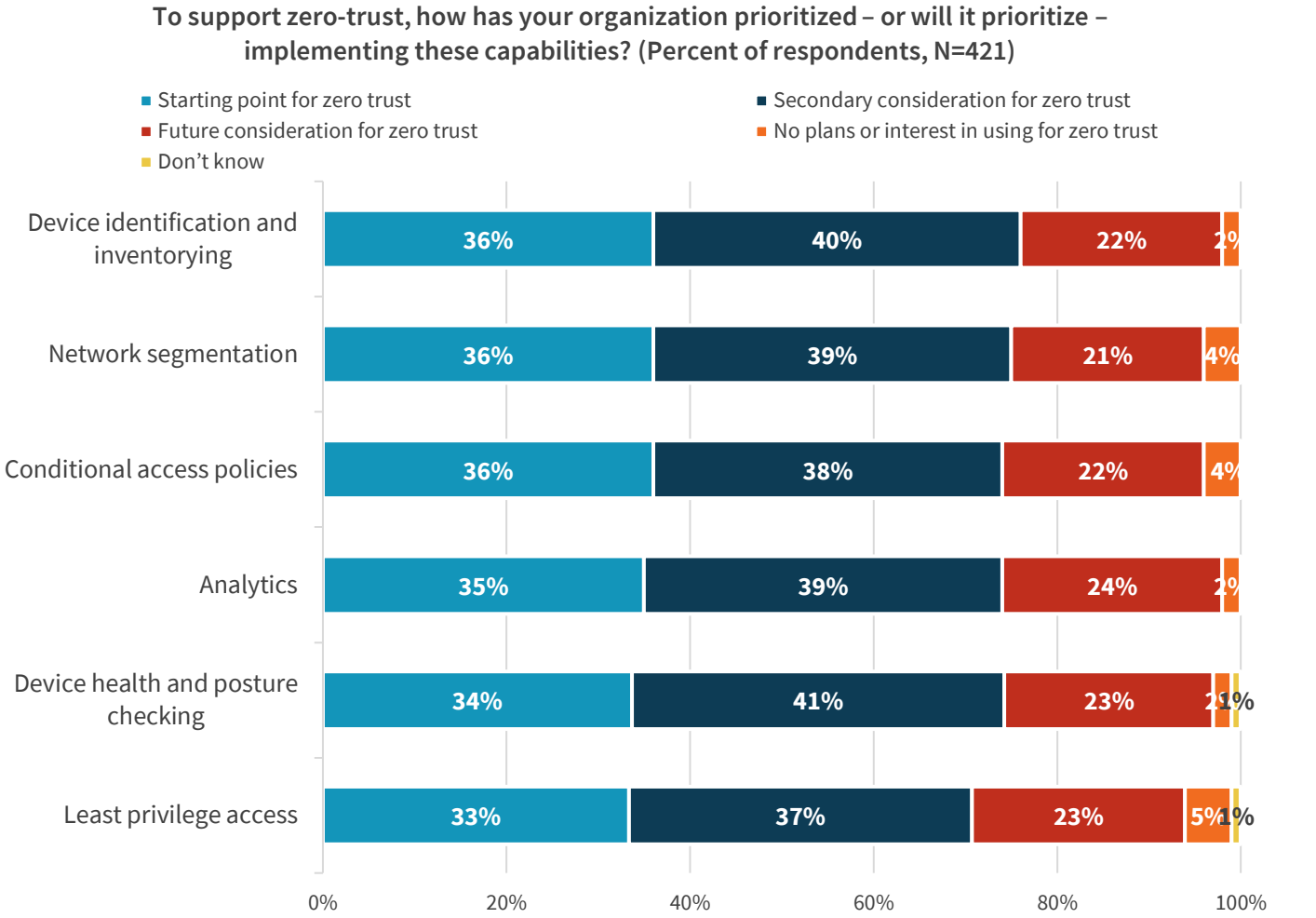
- Device classification and grouping. Armed with specific information about each device, zero trust technologies can classify and group devices based upon device type and traffic patterns. In this way, organizations will have an inventory of all devices, their location, and status. IT and security teams can then manage devices as groups (i.e., all HP model X printers, all Siemens CT scanners, etc.) rather than on an individual basis. When a vulnerability is discovered, security, IT, and OT operations personnel have an up-to-date list of devices to check for software levels and configuration status. ESG research found that 36% organizations agree that device identification and inventorying is a starting point for zero trust.

- Continuous authentication. Each device must be instrumented with strong authentication technology (i.e., PKI, digital certificates, FIDO token, etc.) to establish a trust relationship for network access. To maintain trust levels after authentication, zero trust for the workplace technology must constantly analyze devices, looking for changes in device profile or behavior. Along these lines, 34% of ESG research respondents view device health and posture checking as a zero trust starting point, Suspicious changes should lead to immediate alerts and, in extreme cases, trigger automatic actions like device quarantining and the creation of a high priority trouble ticket.

- Authorization. This covers what each device can do, and when they can do it. It's important to understand the role of each device as it relates to business processes. This can help organizations create the right policies for device communications and least privilege rules. One-third of ESG research respondents agree that least privilege is a starting point for their zero trust plans.

- Trusted network segmentation. Upon policy creation, zero trust for the workplace is then tasked with policy enforcement. This involves microsegmentation of device traffic between devices, to internal applications, and to cloud-based systems. A manufacturing robot should be able to communicate with a SCADA system but shouldn't be allowed to beacon out to a known bad IP address in Ukraine. This will never happen if organizations employ the right policies and microsegmentation across networks. All network traffic should also be encrypted from end to end to preclude man-in-the-middle attacks. ESG found that 36% of organizations agreed with this view and identified network segmentation as a zero trust starting point.

Figure 3. Zero Trust for the Workplace Capabilities



Source: Enterprise Strategy Group

Applying zero trust for the workplace best practices can provide business AND security benefits. From a business perspective, zero trust for the workplace helps organizations align network assets with business processes so they can fine tune them for performance and availability. This can lead to things like production line efficiency or real-time monitoring of critical care patients in a hospital. On the security side, zero trust for the workplace can help organizations decrease their attack surface, helping to mitigate risks. When problems do occur, security operations teams can better pinpoint root causes of problems and make faster informed decisions for incident response.

Cisco for the Zero Trust Workplace

As previously mentioned, zero trust initiatives should be business-driven and comprehensive. While this seems like it could be a big endeavor, most organizations already have some zero trust technology elements in place. CISOs should start by taking an inventory of their existing network security technologies, leverage what's available, and build toward a comprehensive infrastructure from there.

Not surprisingly, many organizations have numerous Cisco networking and security technologies in place that can be used as part of an end-to-end zero trust deployment. For example, the anchor of zero trust for the workplace is Cisco Identity Services Engine (ISE). ISE can create a dynamic and automated approach to device discovery, profiling, policy creation, and

enforcement (via Cisco Group Based Policy [formerly TrustSec]). This leads to software-defined access and microsegmentation for workplace-based IT and operational technology.

Aside from this workplace role, ISE also integrates with numerous other Cisco networking and security technologies to form a zero trust infrastructure that can span the extended enterprise. For example, ISE can integrate with Cisco AI Endpoint Analytics, which applies machine learning algorithms to monitor endpoint behavior, group assets, and detect anomalous behavior. With context sharing via the pxGrid ecosystem, ISE integrates with services such as those provided by Cisco Secure Endpoint (formerly Advanced Malware Protection (AMP) for Endpoints) and Cisco Secure Network Analytics (formerly Stealthwatch Enterprise) to continually authenticate the endpoint and protect the network from cyber-attacks. Any anomalies in behavior can trigger a new policy and enable rapid threat-containment to ensure trust and access levels are maintained throughout the entire session. Aside from Cisco products, ISE also integrates with third-party products like Check Point, F5, Fortinet, McAfee, Microsoft, Splunk, and Symantec. To gain added assurance, ISE integrates with Cisco Duo, adding multifactor authentication for users.

The Bigger Truth

Zero trust is timely concept—especially in response to a global pandemic and WFH requirements. Unfortunately, zero trust remains nebulous, and those that understand zero trust tend to approach it myopically. These limitations are unfortunate. Rather than manage zero trust tactically, CISOs, CIOs, and business executives should create a strategy that balances business and security needs. The goal should be comprehensive zero trust coverage across the workforce, workloads, and workplace.

Of these three areas, ESG research indicates that efforts are really skewed toward the workforce and workloads. While this is understandable due to growth in remote workers connecting to new cloud-based applications, CISOs shouldn't ignore the workplace—especially those working at organizations with aggressive digital transformation plans. This is especially true for organizations in industries like energy, healthcare, logistics, and manufacturing, with significant investments in and plans for IoT and OT device deployment.

This paper outlined what's needed for zero trust for the workplace best practices. CISOs looking for solutions here may benefit by examining how Cisco can help.

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