

WHITE PAPER

Making Zero Trust a Priority for Your Cybersecurity Strategy

By John Grady, Enterprise Strategy Group Senior Analyst

January 2023

This Enterprise Strategy Group White Paper was commissioned by Akamai and is distributed under license from TechTarget, Inc.

Contents

Executive Summary	3
Complexity Reigns in the Modern Enterprise	3
Zero Trust Has Gained Traction, But Key Issues Remain	5
Establishing Zero Trust Priorities	6
Akamai’s Approach to Zero Trust.....	8
The Bigger Truth	9

Executive Summary

When it comes to cybersecurity, there is an uncomfortable but essential fact that must be acknowledged: Too many organizations place too much implicit trust in what takes place in their systems, on their networks, and in their policies and practice. In cybersecurity, there is no place for implicit trust; in essence, it creates an untenable extent and depth of risk for organizations.

The development of zero trust into a vital cybersecurity practice has been more than a decade in the making and is now an increasingly strategic and essential part of any organization's cybersecurity defense framework.

Making it the linchpin of an organization's ability to thwart the increasingly higher number and sophistication of threats is smart business, not just smart technical practice. Preventing the impact of those threats by limiting possible access to only those required for the business to function is the new best practice. In doing so, organizations cut off threat actors from options to infiltrate systems, deploy malware or ransomware, and exfiltrate data.

By erecting a bulwark against potential threats, zero trust is the smart, efficient, and effective way organizations can better protect their digital assets by minimizing the damage should a breach occur.

Complexity Reigns in the Modern Enterprise

Nearly all organizations—even many small ones that rely on technology as a business differentiator—face a more daunting and onerous cybersecurity landscape. Attacks are up, as are the economic, regulatory, legal, operational, and brand-related costs of those attacks.

Cybersecurity defenses must be modernized against a more persistent and sophisticated group of attackers, many of which are collaborating to leverage their respective knowledge, including using technologies such as artificial intelligence and machine learning to execute their attacks faster, more often, and with greater precision. Organizations are becoming increasingly aware of the attackers' innovation and perseverance, but the growing complexity of their infrastructure, architecture, data models, and digital business practices means cybersecurity strategies must be taken to an even higher level.

At the core of modern cybersecurity strategy is understanding and planning for this increased digital complexity. There are a number of reasons why this complexity is on the rise, including:

- Applications are proliferating, both on-premises and in the cloud, creating more data, more targets, and more potential network entry points.
- Device and data source expansion also is accelerating, thus expanding threat vectors and new potential points of entry for cyber thieves. This often includes unmanaged and unsecured personal devices that may be accessed on networks outside the organization's physical facilities, as well as network-connected devices not properly controlled by security policy.
- The inexorable swing toward remote work and hybrid work has further intensified security complexity, as have the rapid uptake in SaaS applications, cloud services purchased and used at home, and the potential for "rogue IT."

The growing groundswell of cloud adoption by organizations is a huge issue that increases complexity. Certainly, cloud is an important part of most organizations' IT strategy and increasingly is at the heart of modern IT architectures. Multi-cloud and hybrid cloud are standard for most organizations, many of which have adopted a cloud-first or cloud-native mentality.

But many organizations have yet to pay suitable attention to cloud security, opening up new avenues of incursion for cyber-attackers.

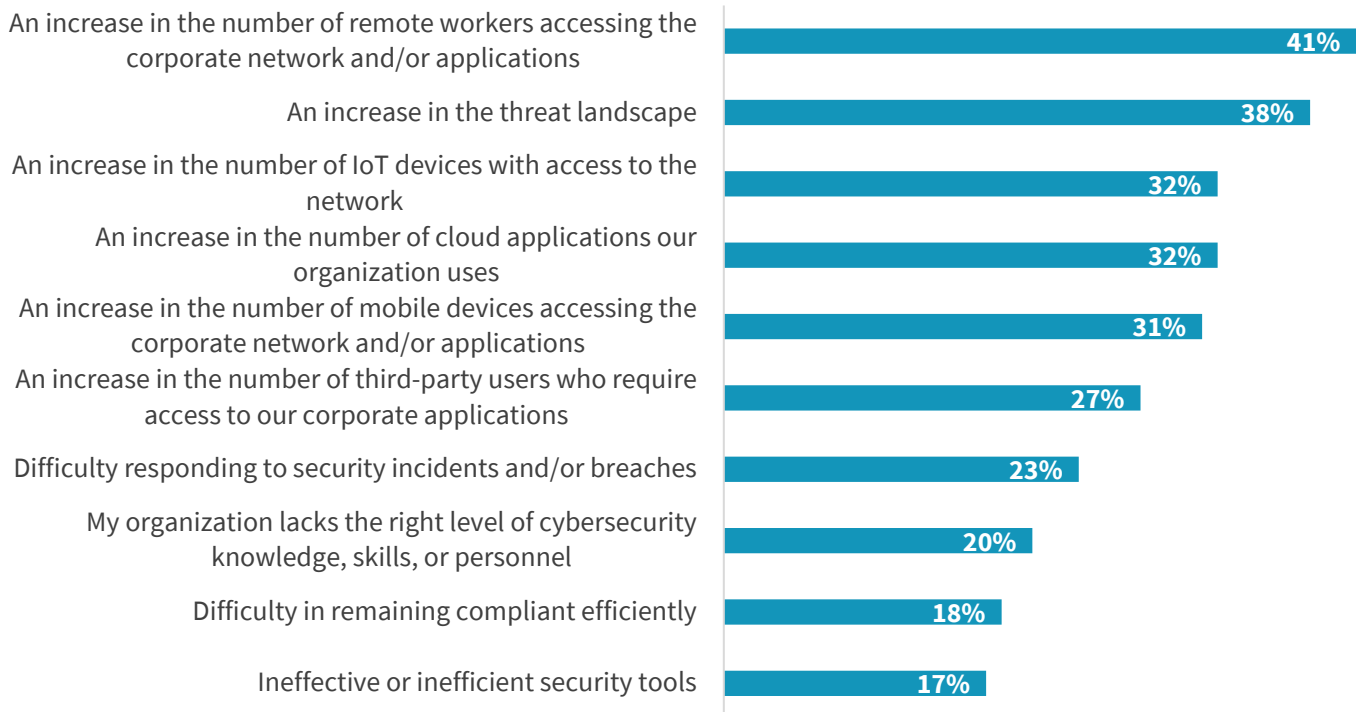
The end result: It is harder than ever to fully and efficiently protect data, applications, identities, credentials, and intellectual property. Traditional security approaches can't keep pace since most were designed in an area where on-premises was the predominant infrastructure approach and when the number and types of devices were limited.

The stakes are higher, too. The cost of a data breach grows every year, and the regulatory and governance implications of inadequate security are more onerous every day.

The net result is that cybersecurity continues to become more difficult and, thus, more challenging to do fully and properly. Research from TechTarget's Enterprise Strategy Group (ESG) points out that 59% of organizations agree that cybersecurity has become more difficult in the past two years. The two most-cited reasons for this are an increase in the number of remote workers accessing the corporate network and/or applications (41%) and an increase in the threat landscape (38%, see Figure 1). ESG's research cites a number of other risk factors that are likely to become more prevalent in the near future, such as the growing number of Internet of Things (IoT) devices accessing the network (32%), the growing number of cloud applications used by the organization (32%), and the continued proliferation of mobile devices being used to access the network and/or applications (31%).¹

Figure 1. Reasons Cybersecurity Has Become More Difficult

In your opinion, which of the following factors have been most responsible for making cybersecurity management and operations more difficult? (Percent of respondents, N=249, three responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

¹ Source: Enterprise Strategy Group Survey Results, [The State of Zero Trust Security Strategies](#), May 2021. All Enterprise Strategy Group research references and charts in this white paper are from this survey results set.

It is essential for organizations to recognize these and other sources of complexity and risk and to take decisive steps to make zero trust a high priority within their overall cybersecurity strategy. While zero trust certainly won't totally eradicate these risks, it will help put organizations on a stronger, more secure footing in protecting digital assets and in instilling a stronger commitment to modernized cyber hygiene.

Zero Trust Has Gained Traction, But Key Issues Remain

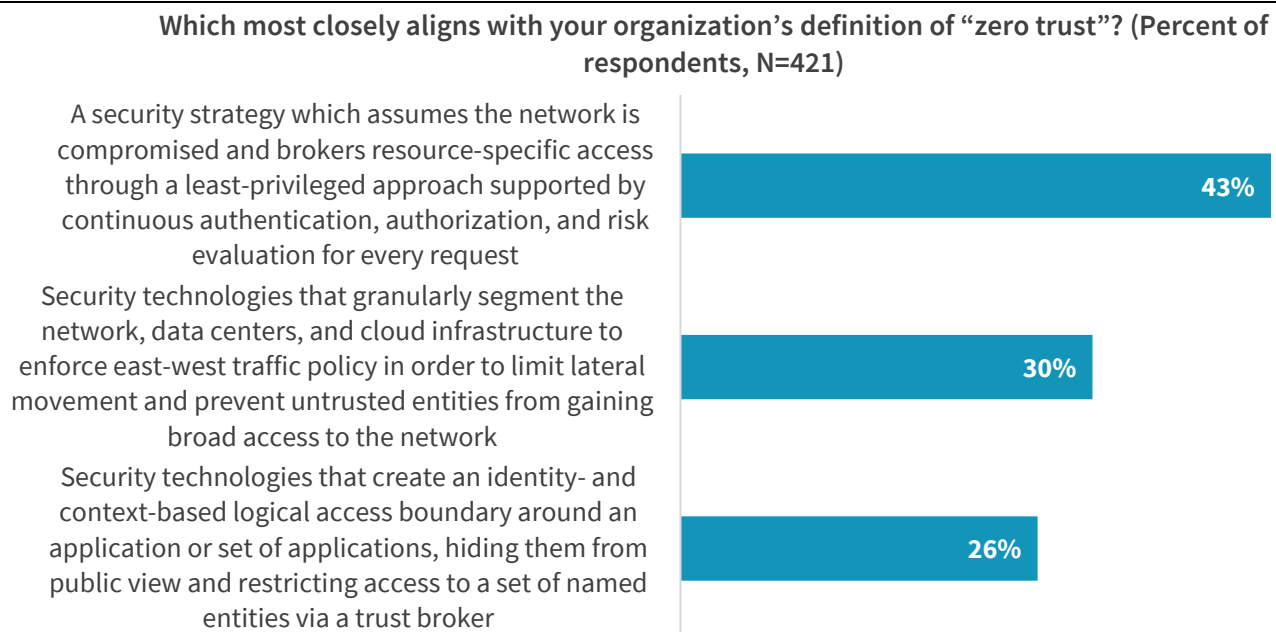
As important and strategic as cloud computing has become, its prominence makes it the bullseye of most organizations' cyber-risk equations. As cloud computing has become central to modern IT strategies, so has the principle of zero trust. Organizations and their cloud service partners must have a clear, universally understood, and equally supported approach on roles and responsibilities for cybersecurity in and out of the cloud. This collaboration is essential in order for organizations to optimize their ability to enjoy the benefits of a zero trust model because it limits—or, ideally, eliminates—risks created by potential policy enforcement gaps.

Zero trust's acceptance has grown significantly in recent years, and that adoption is likely to become near-universal over the next several years. For instance, 46% of respondents to Enterprise Strategy Group (ESG) research inquiries say they've implemented or begun to implement zero trust across their organization, while 43% say they've implemented or begun to implement it for specific use cases.

Still, one major challenge is the fact that many organizations still have imprecise, or even misplaced, understandings of what zero trust is and what it is designed to do.

There still are fundamental differences among organizations in how to define zero trust. For instance, ESG research notes that organizations are close to split on whether zero trust is a collection of cybersecurity tools or an overarching strategy. When asked about their organization's definition of zero trust, 43% of respondents said it is a security strategy, while 56% said it is most associated with security technologies and tools (see Figure 2). While this kind of dichotomy of how organizations view emerging trends and practices such as zero trust is not unusual, it does point to a source of confusion and potential inefficiency in how zero trust has been deployed to date.

Figure 2. Definitions of Zero Trust Vary



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Despite this lingering confusion, there is good news and a promising near-term future for zero trust. One of the most reliable ways to determine what the future is likely to hold for technology trends like zero trust adoption is to see how strongly organizations feel about what they’ve been able to accomplish to date with a zero trust model.

Fortunately, many organizations tell ESG that they are seeing success with their initial implementations of zero trust. The even better news is that organizations note that they are experiencing both security and business benefits derived from their move to a zero trust mindset. For instance, nearly half of organizations say they are benefitting from zero trust in numerous ways, including reducing the number of cyber incidents (43%), improving the efficiency of their in-house security operations center (43%), simplifying their compliance efforts (41%), and reducing the number of data breaches (41%, see Figure 3).

Figure 3. Benefits Seen from Zero Trust



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Although many initial zero trust deployments were targeted at specific use cases, systems, departments, and applications, positive results are likely to spur even broader utilization and adoption. Initial success stories also are likely to breed further interest in, and acceptance of, zero trust models across a wider range of organizational departments, functions, and geographies.

Establishing Zero Trust Priorities

Committing to a zero trust strategy is an important and necessary first step, and it clearly is a positive development that more and more organizations are making that commitment. But actually implementing a comprehensive zero trust

initiative is a significant undertaking, requiring organizations to do a thorough analysis and evaluation of how to prioritize their implementation steps.

It touches a variety of cybersecurity segments, and there are many technologies that can help support zero trust strategies. That makes it essential to properly plan and prioritize the areas to focus on and tools to deploy initially to make the biggest impact in the shortest amount of time.

While there's no single path toward zero trust, a few tools, technologies, and techniques do stand above the rest in their relevance to zero trust.

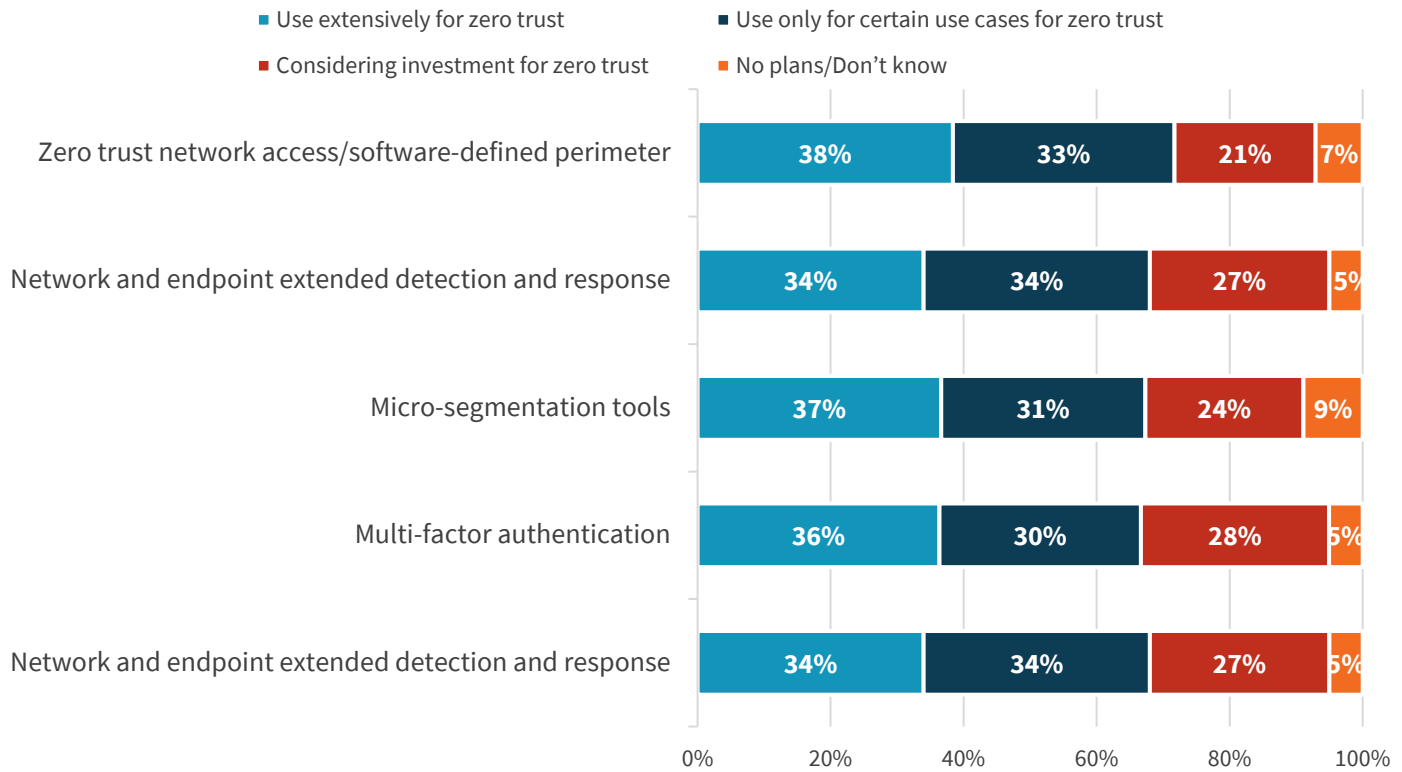
These include:

- **Segmentation and microsegmentation.** At its core, zero trust is about ensuring that entities are only allowed to communicate with one another when dictated by policy. Coarse-grain segmentation can begin to limit what parts of the environment users and devices are able to access. For example, organizations can ensure that connected medical devices cannot access the same network on which finance applications sit. However, this does not provide the level of granularity required for a true zero trust approach. As a result, microsegmentation has seen increasing interest to more specifically create policies at the workload level and to prevent lateral movement by attackers.
- **Identity strategies, including multifactor authentication and password/passwordless identity frameworks.** With identity theft becoming a larger and more insidious threat to organizational cybersecurity, using zero trust principles to clamp down on sources of identity theft both outside and inside the organization is essential—and smart.
- **Zero trust network access (ZTNA).** Traditional approaches to providing remote access to applications, such as VPNs, actually provide users with network-level access. Attackers who gain unauthorized access are able to move laterally through the network. By contrast, ZTNA enables application access based on identity and reduces the potential for lateral movement.
- **Detection and response.** Organizations must understand and react quickly when actions occur outside of a “trusted” policy. It is widely accepted that “alert fatigue” is a growing problem for cybersecurity organizations, and a more granular and contextually aware approach to flagging anomalous behavior and potential threats is necessary. Putting a trust-based policy in place helps to make detection and response more efficient and effective.

Enterprise Strategy Group (ESG) research highlights the importance of those and other priorities for actually implementing a zero trust framework. For instance, most organizations use ZTNA as part of their zero trust model either extensively or for specific use cases (71%). Other technologies and services used as part of organizations' zero trust model include network and endpoint EDR (68%), microsegmentation tools (68%), and multifactor authentication (66%, see Figure 4).

Figure 4. Technologies Used to Support Zero Trust

Please indicate your organization’s usage of or planned usage for the following types of technologies and services specifically in support of a zero-trust strategy. (Percent of respondents)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Akamai’s Approach to Zero Trust

Akamai is well known for its track record in helping organizations effectively deliver and protect their applications to end-users. However, Akamai has been steadily adding enterprise security capabilities for a number of years and now boasts a [number of products](#) that can help organizations begin to build toward a zero trust security posture across people, things, and identities.

Through its acquisition of Guardicore, Akamai offers [host-based microsegmentation](#) to ensure the communication between workloads and applications is denied by default unless expressly permitted by policy. The solution helps customers to reduce their attack surface, prevent lateral movement, secure their critical assets from ransomware, and automate zero trust policies across all environments (on-premises, cloud, and IoT/OT).

Akamai Hunt is a managed threat detection service that discovers and alerts customers on adversary actions such as lateral movement, malware execution, communication to Command & Control servers, user and network anomalies, and more. By leveraging a team of expert researchers, customers receive only high-priority alerts on security risks, including mitigation recommendations.

Akamai’s Enterprise Application Access is a cloud-based zero trust network access solution that applies granular, least-privilege access policies to private applications based on strong authentication and context.

Akamai MFA is a phishing-proof MFA service based on FIDO2 that delivers strong user authentication. It can help prevent employee account takeovers. It is a frictionless authentication solution that can help organizations begin to layer

additional identity verification mechanisms into their security policies and to support the evolution to passwordless authentication.

Finally, Akamai's Secure Internet Access is a secure web gateway that protects users and devices accessing internet-based resources from malware, ransomware, and other threats. Further, it can help ensure that acceptable use policies are followed and that sensitive data is not inadvertently or maliciously uploaded to external sites and applications.

This breadth of capabilities makes Akamai an attractive partner for any organization, whether it is at the beginning of its zero trust journey or has already begun down the path.

The Bigger Truth

Cybersecurity will only become more difficult and complex as organizations, industries, and societies become more digitized. As a result, the impact of breaches, incursions, data loss, and digital asset compromises will become bigger, broader, and more problematic.

Zero trust must be at the heart of every organization's cybersecurity strategy, and microservices and other enabling technologies must inform, shape, and influence how, when, and where zero trust is deployed.

Akamai's approach to zero trust and microservices takes an expansive, forward-looking, and innovative look at cybersecurity strategies that help organizations defend digital assets in an increasingly cloud-centric landscape.

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


This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.



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

 www.esg-global.com

 contact@esg-global.com

 508.482.0188