Osterman Research
WHITE PAPER

**White Paper** by Osterman Research
Published **November 2021**
Sponsored by **BIO-key International**

# Why Zero Trust is Important

# Executive Summary

Zero trust offers a modern approach for security to meet modern work designs and tackle the cybersecurity challenges facing organizations. The rise in remote work, the relentless waves of ransomware and other cybersecurity attacks, and the need to redress fundamental weaknesses in perimeter-based security have coalesced to drive interest and uptake in zero trust architectures. First touted in 2004, organizations are progressing with zero trust designs to increase the efficacy of cybersecurity protections and build a stronger foundation to address the new challenges of hybrid work, data protection, and security. Organizations view strengthening identity and access management as the key design modification for zero trust initiatives, and confidential files the most important data source to protect. Most organizations expect to be fully deployed with a zero trust architecture within two years.

This white paper reports on how organizations are deploying and planning to deploy a zero trust architecture. It offers direction to decision-makers and influencers on best practices and solutions to support the move to zero trust.

*Zero trust offers a modern approach for security to meet modern work designs and tackle the cybersecurity challenges facing organizations.*

## KEY TAKEAWAYS

- **Zero trust offers a new approach to cybersecurity**
  Earlier security approaches assumed people and devices within the network were trustworthy. Zero trust approaches do not rest on this assumption, requiring instead the ongoing verification of trustworthiness.

- **Mitigating trends, increasing efficacy, and strengthening cybersecurity protections are the key drivers of zero trust**
  Organizations are deploying zero trust to mitigate the threat of current trends (e.g., high-profile ransomware incidents and pandemic-induced remote working), double the average efficacy of cybersecurity protections (e.g., against data breaches), and strengthen current protections (e.g., identity and access management). Organizations are putting high emphasis on protecting key data sources, with confidential files viewed as the most important data source to include in a zero trust architecture. Cloud migration has made the identification and protection of sensitive data more complex.

- **Organizations face a journey to implement zero trust architectures**
  Most organizations expect to be able to fully deploy a zero trust architecture in two years or less. Initial steps include improving identity and access management, strengthening application access management, and increasing protections for external parties, such as customers and supply chain partners.

- **Technical and resourcing barriers to zero trust currently rate highly**
  Organizations must deal with a set of barriers to deploying zero trust successfully. The current top-rated barriers deal with technical (e.g., dealing with limitations in legacy systems) and resourcing (e.g., obtaining appropriate financial and staffing resources to do zero trust properly) issues.

- **Zero trust architectures leverage multiple types of cybersecurity solutions**
  No single product alone delivers a zero trust architecture. Organizations must deploy and integrate a combination of solutions that enhance identity and access management, access controls, and protections for sensitive data, among others.

### ABOUT THIS WHITE PAPER

This white paper was sponsored by BIO-key International. Information about BIO-key International is provided at the end of this paper. This paper references data from an in-depth survey of 125 IT and security decision-makers in mid-sized and large organizations (average employees 11,992, median employees 1,500), all of whom are knowledgeable about how their organization was using or planning to use a zero trust architecture, or why their organization had intentionally chosen not to do so.

## What is Zero Trust?

Zero trust architectures address a fundamental shortcoming in how many organizations have traditionally approached security: namely, that people and devices inside the network or a given security perimeter are assumed to be trustworthy. If an authenticated user wants access to data, they get it. If a corporate device is connected to the network, it is treated as a trusted entity. The cybersecurity approach in such situations is to build strong defenses that keep the bad out and let the good in. Over the past several decades, this model has proven to be flawed due to emerging cybersecurity threats, the desire for more convenient ways of digitally interacting with organizations, the recent rapid shift to remote work, and the rise of hybrid deployment models.

> ***Zero trust architectures address a fundamental shortcoming in traditional security models: that people and devices inside the network are assumed to be trustworthy.***

Threats, trends, and current issues elevating the need for zero trust include:

- **Insiders represent a significant threat to organizations**
  People inside the network accidentally expose data to unauthorized individuals by misdirecting an email message, falling for phishing campaigns, or using unsanctioned cloud services (e.g., a personal Dropbox account) to speed up a business process or get around IT security policies but failing to secure confidential corporate data when doing so. Other people inside the network act stealthily with malicious intent to steal corporate intellectual property, share confidential data with outsiders, or help cybercriminals to compromise the organization by acting as an accomplice.

- **Compromised devices threaten security posture**
  Corporate devices become compromised through malware, keyloggers, unpatched applications, early-stage ransomware infiltrations, viruses, and other pernicious activity. Left unchecked, such devices can spread infections and vulnerabilities within the corporate network or become a channel through which corporate data is surreptitiously exfiltrated. Device threats are amplified when IT does not control the environment, such as with bring-your-own-device strategies or the use of personal devices with the pivot to remote working.

- **Employees are using compromised networks to connect to corporate data**
  Even before the pandemic of 2020 forced a rapid rethink in work location and the devices used to access work resources for many people, remote access to support mobile workers, ad hoc telecommuting, and work-from-home arrangements had increased. Employees on the road leveraged free Wi-Fi networks in coffee shops and airports, and those working from home relied on consumer-grade Wi-Fi routers to establish connectivity with the corporate office, raising the specter of breached data through network sniffing, malicious hotspots, remote access vulnerabilities, and other forms of surveillance.

- **Cloud-only, multi-cloud, and hybrid infrastructures are on the rise**
  Few organizations retain an on-premises deployment model alone. Most rely on multiple cloud services in conjunction with a decreasing footprint of on-premises capabilities. A zero trust architecture that span on-premises and multiple cloud services enables organizations to provide secure access across a changing deployment model.

## TRUST NOTHING BY DEFAULT

Zero trust is an alternative security framework that was initially developed by the Jericho Forum, an international group formed in 2004 to address the rising interest in cloud computing and other data-level security issues.[1] More recent work on zero trust was conducted at Forrester Research starting in 2010.[2]

The basic principle of zero trust is that no user or device is trusted by default. Instead, every user or device is considered a potential threat until proven otherwise. Being proven otherwise is not a one-time event. The basic principle of zero trust is continually tested and enforced to limit the possibility that once-trusted users or devices become compromised and transition to an active threat status. Verification happens in real-time whenever a user or device requests access to new resources, rather than on a periodic basis, e.g., every several days; access grants also time out forcing re-verification. Zero trust and the principle of least privilege are tightly linked, so that only the access privileges required for a given user, device, or application are granted. Users, groups, and departments with no valid business need to access certain applications or data sources cannot do so.

*Trust nothing by default.*

## THE CONCEPT OF MICRO-SEGMENTATION

Segmentation provides a structured approach to giving access rights to the correct people and ensuring no one else has access. In its most rudimentary form, all systems or applications have two segmentation policies: access is granted, or access is not granted. Security architectures based on authenticated network access grant access to everyone who can authenticate using a valid identity and disallow access for anyone else.

A zero trust architecture takes the first of these two policies and enumerates many variations based on identifiable characteristics of the individual, the device, the type of network connection, the user's location, and time of day, among others. For example, identifiable characteristics include:

- **User characteristics**
  Who is making the access request? Are they an employee, manager, executive, or someone external to the organization, such as a business partner? For internal users, have they been newly hired or been recently evidencing disgruntled behavior? Are they following a normal pattern of behavior or is this access request an aberration? For people external to the organization, are they a prospect, customer, or from a third-party vendor?
- **Device characteristics**
  Which device is being used to request access? Is it a corporate-issued device, a previously seen employee-owned device, or a never-seen-before device in an Internet café? Is it a laptop, Android or Apple smartphone, tablet? Is the device compliant with the organization's baseline security policy? Are there any applications that are not up to date with patching against known vulnerabilities on the device?

- **Type of network connection**
  What type of network connection and IP address ranges are being used to make the connection attempt? Is the network known and trusted, and do the IP addresses have the reputation of being clean? Or are connections coming from free Wi-Fi networks, low-reputation IP address ranges, or even dark web networks, such as Tor?
- **User location**
  From what geographical location is the access request coming? The office buildings for the organization? Countries in which the organization is not operating and where no employees are based or are currently traveling? Known hotspots for cybercriminal activity?
- **Time of day**
  When is the access request being made? During business hours? In the early evening? At 2:00am when the network is not being actively monitored?
- **Presence of confidential data**
  Is the requested data considered sensitive or confidential to the organization or a client? Does it contain personally identifiable information or personal health data covered by general and specific data protection and privacy regulations?

## EXAMPLES OF DIFFERENTIAL ACCESS BASED ON CONTEXTUAL FACTORS

Zero trust uses pre-defined micro-segmentation policies to enforce differential access based on an assessment across the characteristics and criteria above—and relative to user's needs for productivity, increased complexity with work from home arrangements, and collaboration across global teams. Access may be denied completely, enabled completely, or offered in a limited form. For example:

- **Executive access to a cloud system**
  An executive requesting access to a cloud system from the corporate network using a company-controlled device will be handled using a different micro-segmentation policy than when she connects from an open Wi-Fi network at a hotel in a foreign country using her personal tablet. In the second case, for example, she may be given only read access to the cloud system, additional step-up authentication challenges, or more questions to answer to verify her identity. The first scenario has fewer risk signals than the second.
- **Employee access to the corporate file share**
  An employee connecting to the corporate file share from his personal computer at 2:00am in the morning over his home wireless network will be handled using a different micro-segmentation policy than when requesting the same access during business hours at the office using his corporate device. The first scenario has many more risky signals than the latter one, meaning the employee may be denied access entirely at 2:00am, given read-only access, or be prevented from downloading any documents.
- **Salesperson requesting access to a new customer in the CRM**
  A salesperson has been browsing the list of her current customers in the firm's Customer Relationship Management (CRM) system while connected from outside the corporate network on a personal device. When she tries to open the details of a customer account outside of her territory, an additional multi-factor authentication challenge is presented. She must pass this step-up challenge before being providing with read-only access to limited parts of the customer record.

> ***Zero trust uses micro-segmentation policies to enforce differential access based on an assessment across multiple characteristics and criteria.***

- **Security by design for sensitive customer data**
  When a customer places an order on the corporate web site, details of the customer and their order are stored in the e-commerce application for the firm. To minimize the potential of data theft by malicious insiders and external threat actors, credit card numbers and other identifying details of customers are automatically replaced with pseudonymized placeholders. By default, therefore, a data breach from outside will not reveal any usable data, and access by authorized employees will only show the core data required to fulfil the ordering process. If an employee needs access to a credit card number, social security number, or the customer's phone number, a higher level of access can be requested by the employee—which must be approved, verified, and logged for reporting purposes.

- **Employee access to incorrectly filed confidential data in SharePoint**
  An employee requests access to a document library in SharePoint from a corporate-managed device during standard working hours. The document library is supposed to only contain files that do not include confidential data, but some files have been uploaded that do. When the employee tries to open one of the files that includes confidential data, added restrictions are imposed on his request, such as step-up authentication or read-only access. If the employee had requested access from a non-managed device, a corporate device used from home, or from any device outside of normal working hours, access to the file would have been blocked entirely.

- **Employee moving to a new role**
  An employee moving to a new role in a different department is a major event in the lifecycle of an employee and their digital identity. The mix of applications, systems, and data they are permitted to access changes when they make the transition to their new role. Access rights that went with the previous job role should be revoked. The access rights required for the new role should be enabled.

- **Employee offboarding**
  When an employee is terminated or departs to work for the competition—another major event in the lifecycle of an employee—their employment status and access rights both change. Their user account and any devices used to connect to the network and cloud resources should be immediately blocked to reflect the potential for data theft.

- **Customer access to business applications**
  A customer requesting access to an application containing their data from a registered smartphone is given a different set of access rights than when accessing the application from an unknown device. The lack of a device fingerprint for the unknown device means a step-up authentication requirement must be met before private information is disclosed to the customer.

## UNDERSTANDING USER NEEDS FOR PRODUCTIVITY

Organizations face a perpetual struggle between security and productivity—between ensuring confidential data and processes are kept secure while not dampening the ability of employees to be productive. Irrespective of whether restrictions are necessary, when the practical implementation of any security process is too severe, employees usually revolt and find workarounds that have fewer restrictions. Deploying zero trust may work technically without reference to employees but cannot succeed organizationally without it.

> ***Deploying zero trust may work technically without reference to employees but cannot succeed organizationally without it.***

Wider success with zero trust relies on a contextual understanding of how potential zero trust designs affect the ability for people to work. This understanding must be included in the initial design phase and ongoing administration of zero trust, along with efforts to help employees understand the need for zero trust and how they can get help when micro-segmentation policies block productive working rhythms. Zero trust deployments that are approached as security projects without reference to a wider group of executives and employees from across the organization will never achieve their potential or expected benefits.

## ZERO TRUST IS ONLY PART OF THE CYBERSECURITY EQUATION

A zero trust architecture is only one part of a complete cybersecurity strategy, not the entire answer. Several threat vectors and areas of vulnerability are not addressed by fully embracing a zero trust approach, including:

- **Vulnerability and patch management of applications**
  Zero trust can ensure that a user or device is authorized to access data in a particular application, but does nothing to assure that the application itself is secure, free from vulnerabilities, patched, and not a vector for any other threat types. Offering assurance for these concerns is the responsibility of vulnerability and patch management solutions, not zero trust ones.

- **Digital transformation to replace legacy applications**
  The selection of the correct micro-segmentation policy to apply to any given access request relies on the ability to detect and utilize nuanced differences across users, devices, network connections, and more. Legacy applications that lack granularity hamper zero trust efforts, because the constructs to offer granular rights do not exist. For example, legacy applications that only support read-write access to an authenticated user cannot by design support micro-segmentation policies that want to offer read-only access when certain attributes trigger a higher risk profile. In parallel with moving to a zero trust architecture, therefore, organizations need to embark on a program of digital transformation to upgrade or replace current legacy applications that prevent full adoption of zero trust.

- **Security status of hardware**
  Insecure device hardware can be compromised by vulnerabilities and attacks that sidestep zero trust policies. Endpoint protection, detection and response, and vulnerability analysis is a needed complement to zero trust to prevent attacks that start with compromised hardware.

- **Warnings of supply chain and nation state attacks**
  Credential and account compromise at partner firms—particularly cloud service providers—as part of advanced supply chain and nation-state attacks may not be identified by zero trust architectures. When an organization approves delegated access permissions for service providers, any upstream compromise at the service provider may be invisible to an organization because the full background and contextual characteristics of an access or resource request is hidden behind layers of obfuscation. Zero trust architectures may lack the ability to capture and identify the underlying characteristics of a malicious access request when it is routed through a trusted partner. Our understanding of the complexities and nuances of supply chain attacks is still in its early days.

> ***A zero trust architecture is only one part of a complete cybersecurity strategy, not the entire answer.***

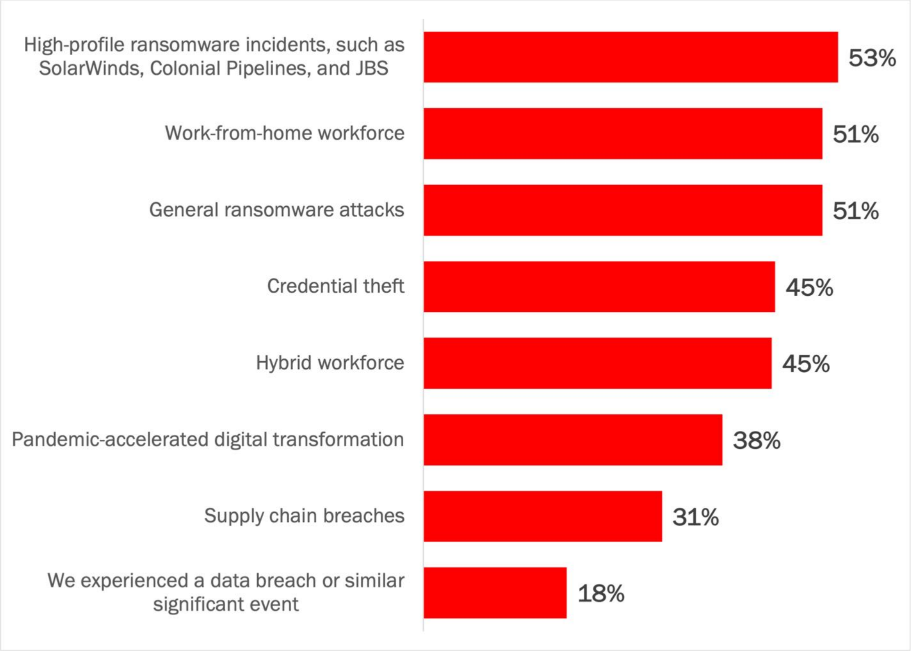
# Key Drivers for Zero Trust Architecture

Embracing a zero trust architecture requires rethinking approaches covering identity and access management, application access, and data, among others. It is a significant undertaking for organizations. In this section, we look at the key drivers for deploying a zero trust architecture.

## MITIGATING CURRENT TRENDS, THREATS, AND RISKS

Several current trends have impacted the decision to embrace a zero trust architecture, led by high profile ransomware incidents, adapting to a work-from-home workforce, and mitigating general ransomware attacks. Over half of respondents indicated these three trends were highly or extremely impactful on their decision-making process. See Figure 1.

**Figure 1**
**Trends That Impacted the Decision to Embrace a Zero Trust Architecture**
Percentage of respondents indicating "highly impactful" or "extremely impactful"



*Source: Osterman Research (2021)*

**53%**

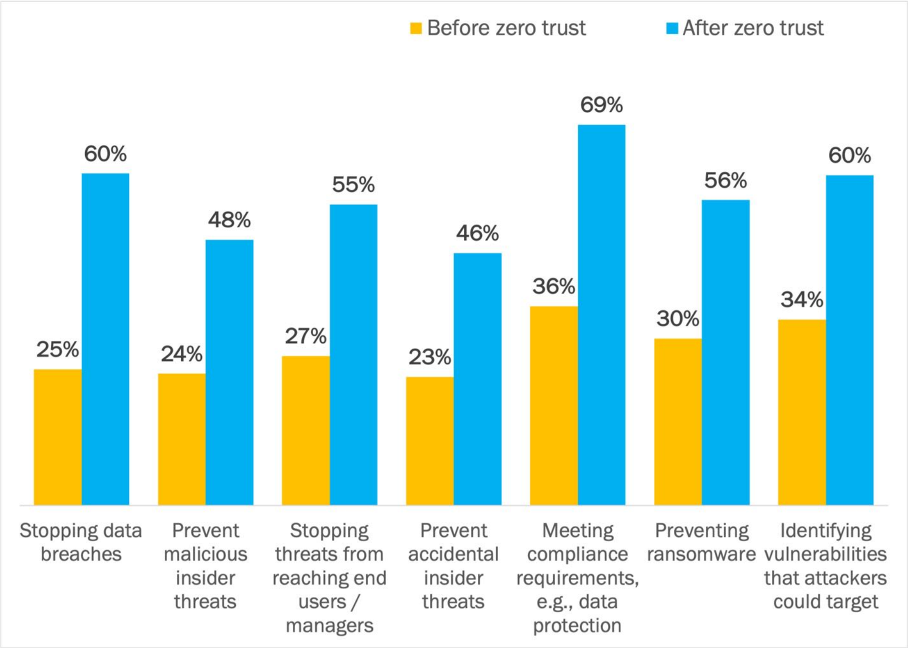
***Respondents who say high-profile ransomware incidents is the trend having the largest impact on the decision to embrace zero trust.***

The two ransomware trends in the three top drivers represent unquantified threats external to the organization, as opposed to actual events an organization has experienced. The impact of these significant, potential external threats is more than two and a half times higher than seeking to prevent a reoccurrence of a cybersecurity incident that has already happened. For example, only 18% of respondents said that a previous data breach or similar significant event was highly or extremely impactful. The fear of unquantified but potentially catastrophic consequences is a much stronger driver for adopting zero trust than addressing something that has already been experienced.

## ACHIEVING SIGNIFICANT UPLIFT IN CYBERSECURITY EFFICACY

A zero trust architecture is expected to double the average efficacy of cybersecurity protections against a range of threats and incident types. The highest anticipated increase is in the ability to stop data breaches—with a 144% increase in anticipated efficacy from the assessment of efficacy before zero trust (25%) to the assessment after zero trust (60%). The two benefits with the lowest anticipated increases are preventing ransomware (83% increase) and identifying vulnerabilities that attackers could target (78% increase), although these are still significant increases nonetheless. See Figure 2.

**Figure 2**
**Confidence in Cybersecurity Protections to Achieve Key Outcomes**
Percentage of respondents indicating “confident” or “highly confident”



*Source: Osterman Research (2021)*

**2X**

***Zero trust is expected to double the average efficacy of cybersecurity protections against a range of threats and incident types.***

In looking at the data:

- **Significant uplift but a wide threat scope remains**
  Respondents expect zero trust to have a significant impact on the efficacy of their cybersecurity protections, but deploying zero trust is not viewed as the complete answer to elevate efficacy to 100% for any of the threat types above. On average, there is still a 40% to 50% gap left between the anticipated future state with zero trust and a robust set of complete cybersecurity protections. Respondents expect zero trust to make a significant contribution to reducing the scope of threats (as it should), but do not expect it to completely mitigate every threat alone (as it cannot).

- **Stopping data breaches—and reducing the cost of a breach**
  Zero trust is expected to deliver the largest increase in efficacy for its ability to stop data breaches. This will be of critical importance for many organizations. One study found that while data breaches still occur at organizations with mature zero trust deployments, the average cost of rectification was 35% lower than at organizations without zero trust.[3]

- **High expectations around insider threats**
  Insiders—i.e., employees, managers, and executives—are implicated in many cybersecurity incidents. Most insider incidents are accidental while some are malicious. Accidental insider incidents include sending sensitive data to the wrong recipient, falling for a phishing campaign that captures account credentials, and losing an unencrypted thumb drive containing confidential data. Malicious insider threats include deliberate theft and sharing of data. By limiting insiders' scope of access to corporate data and enforcing restrictive policies on access rights that are granted based on contextual factors, recipients expect the efficacy of their protections against both types of insider threats to double.

- **Data breaches and ransomware now usually go together**
  Respondents ranked ransomware threats as two of the three highest rated trends impacting the decision to implement zero trust, and the impact of an actual data breach as the least impactful trend (see Figure 1 above). In terms of impact on the efficacy of cybersecurity protections, however, zero trust is anticipated to have a much greater impact on the ability to stop data breaches (144% increased efficacy) than preventing ransomware (83% increased efficacy). With ransomware gangs increasingly using multi-level extortion tactics predicated on data exfiltration, the difference between the two is shrinking. Ransomware attacks are increasingly linked with data breaches.[4] Dealing holistically with both ransomware and data breaches requires cybersecurity education and awareness training so employees and executives complement technology solutions rather than undermining them.

*Ransomware gangs combine unwanted encryption with data breaches for multi-level extortion.*

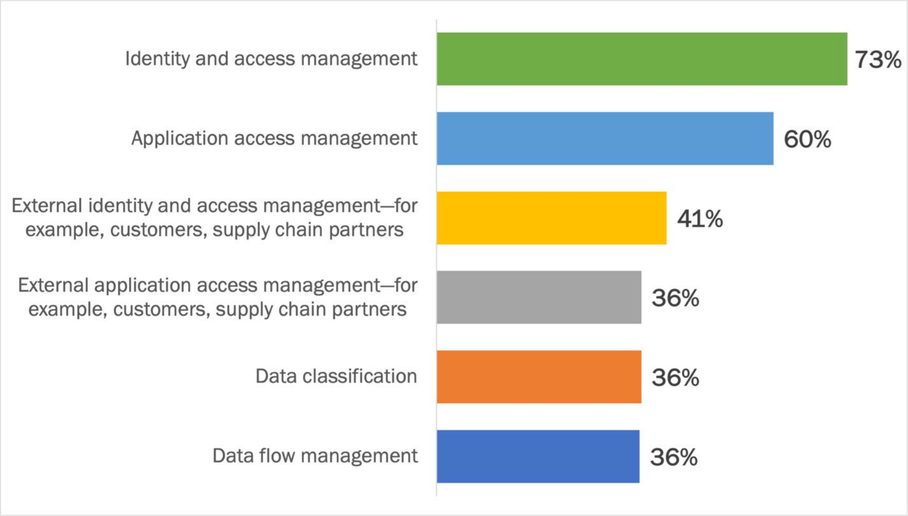
- **Efficacy for compliance higher than efficacy for security concerns**
  The ability for cybersecurity protections to meet compliance requirements after the deployment of zero trust is ranked the highest of all outcomes (69%). All the security outcomes receive lower ratings than the compliance one after the deployment of zero trust. While meeting compliance requirements is important, strengthening core security protections has direct impacts on the compliance agenda too. Cybersecurity efficacy to avoid a compliance compromise is a lower standard than avoiding a security compromise.

- **The higher efficacy for identifying vulnerabilities that attackers could target is surprising**
  Zero trust architectures do not address the need to identify vulnerabilities that attackers could target. Unlike their name, zero trust approaches assume that applications are trustworthy. We are concerned that respondents are expecting increased efficacy in this area that is not addressed by zero trust.

## STRENGTHENING CYBERSECURITY PROTECTIONS

Organizations see zero trust approaches as enabling design modifications to strengthen cybersecurity protections primarily focused on internal matters—that is, identity and access management and application access management for employees and internally-facing applications whether hosted internally or as cloud workloads. Fewer organizations are initially focused on strengthening external access, addressing data classification, and managing data flow. See Figure 3.

**Figure 3**
**Where Organizations are Focusing Design Modifications for Zero Trust**
Percentage of respondents indicating "highly focused" and "extremely focused"



*Source: Osterman Research (2021)*

Addressing the internally-facing identity and access management concerns for employees and internal applications is viewed as almost twice as important as the same concerns for external participants, such as supply chain partners. Every organization must start somewhere with zero trust, and strengthening internal issues is critical to get right. We hope that organizations do not neglect the other issues above as their internal strategies mature, because the external threats—including supply chain attacks—are increasingly significant.

Knowing which data sources include sensitive and confidential data is a core aspect of instantiating the correct access policy in response to a user or system request. When this awareness is based on point-in-time audits, data drifting between systems and repositories decreases the ability to identify the correct access policy and increases the risk of data breaches. Solutions that automate the continual classification of data and manage data flows across systems and repositories enable organizations to move away from point-in-time audits to real-time assessments, thus decreasing the likelihood of data breaches. Even data that is held authoritatively in structured data systems is at risk of drift, as people copy and paste data into files or use export functionality to move data into Excel or CSV files for specific purposes. When these files are emailed to other people inside or outside the organization, additional copies of such data are created beyond the tight access controls of structured data systems. Organizations appear to be placing insufficient focus on the core disciplines of data classification and data flow management across both structured and unstructured data systems.

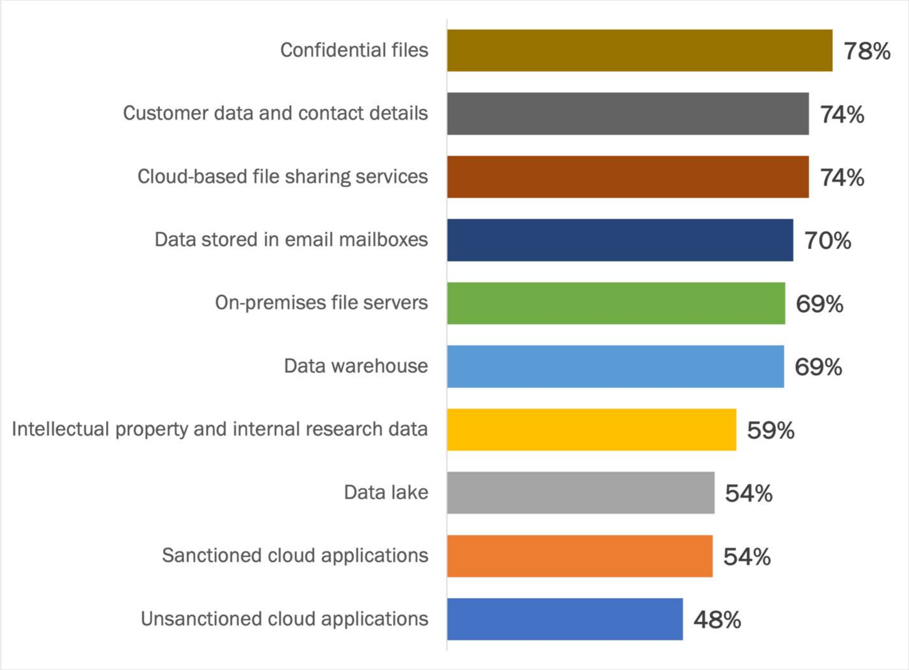
**73%**

***Respondents focused on identity and access management for employees as the key design modification for zero trust.***

## SAFEGUARDING A RANGE OF DATA SOURCES

Organizations have many data sources, repositories, and content types containing data that requires protection. Respondents view confidential files—holding secret, sensitive, and other protected information inside—as the most important data source to include in a zero trust architecture, followed by customer data and contact details. Sanctioned and unsanctioned cloud applications are the two data sources viewed as being least important to address. See Figure 4.

**Figure 4**
**Data Sources Important to Include in a Zero Trust Architecture**
Percentage of respondents indicating "highly" or "extremely important"



***Source: Osterman Research (2021)***

**78%**

***Respondents viewing confidential files—holding secret, sensitive, and other protected information inside—as the most important data source to include in zero trust initiatives.***

Organizations need to ensure their zero trust deployments protect the locations where confidential and sensitive data is stored. Key areas include:

- **Files contain sought-after data**
  Files stored in corporate file shares, cloud services, thumb drives, and as attachments in email accounts are a highly sought-after container of confidential and sensitive data, information and records. Much of this data is stored in loosely controlled Microsoft Office documents. An individual file can relate to a single individual (e.g., a contract for service) or thousands of employees or customers (e.g., an Excel spreadsheet with payroll details for employees, purchase history for customers, or an export of customer details for an email marketing campaign). Files are under threat from multiple directions, such as cybercriminals who want access to mine files for personally identifiable information that can be used in attacks against individuals, as well as accidental insider incidents where sensitive data attached to an email is misdirected. Misdirected emails are a growing problem in organizations; one study found an average of 800 misdirected emails per year for an organization with 1,000 employees.[5] In the United Kingdom, misdirected emails were more commonly implicated in data breaches than phishing campaigns in 3Q 2021.[6] In

multi-level ransomware attacks, cybercriminals have started using breached data to extort individual customers for ransom payments.[7] The net implication of these types of incidents is that confidential files require heightened protection—wherever they are stored and whenever they leave the organization through email or another channel.

- **Data stored in email accounts is highly valued**
  Cybercriminals seek access to email accounts through phishing campaigns, malware, and brute-force password attacks, among others. A compromised email account enables hijacking of the victim's reputation—including the reputation of the associated brand and email infrastructure—for use in subsequent internal and broadcast phishing campaigns and with access to unprotected documents stored in Sent, inbox, and project folders. Cloud providers offer email accounts with storage limits of 100GB or more, which represents a goldmine of sensitive communications and confidential files that inform attacks, invoice and payroll fraud attempts, and impersonation. Data breaches are generally not identified promptly. The timeframe between the incident occurring, being detected, and being fully rectified is measured in hundreds of days rather than minutes.[8]

- **Recent data protection and data privacy regulations have upped the game with customer data and contact details**
  Protecting customer data and contact details used to be about keeping details of key accounts away from competitors. However, recent data protection and data privacy regulations—led by the European-wide General Data Protection Regulation (GDPR) and followed quickly by other countries and emerging localized approaches in the United States—have transformed this issue into a completely different topic for organizations in all industries. Some industries, such as healthcare in the United States, were early adopters of a broader definition of privacy. Breached customer data and contact details now carry significant regulatory penalties, mandated breach notifications, and degraded market performance irrespective of whether competitors gain access to customer lists. In addition, many organizations face a new set of requirements to ensure data subjects gain rights of access, rectification, and deletion over their data, heightened restrictions on what data can be collected and processed, and the need to support secure transfer of data to another organization if a data subject wants to move to another provider.

*Recent data protection and data privacy regulations have upped the game with customer data and contact details.*

- **The lower importance of cloud applications is concerning**
  Organizations across all sectors are embracing cloud infrastructure, but the increased speed to market for new service offerings does not negate the need to utilize appropriate cloud security strategies too. If zero trust initiatives do not encompass sanctioned and unsanctioned cloud services, the greater risk of cyber exposure negates any benefits gained by moving to the cloud. In addition, cloud providers generally have internal drivers and metrics around increasing usage and simplifying sharing settings to lower barriers for users, many of which compromise and undermine the security efforts of the organization, such as when sharing options are activated by default. Organizations need to pay attention to the ever-changing strategies of cloud providers to drive usage with tactics that undermine security.

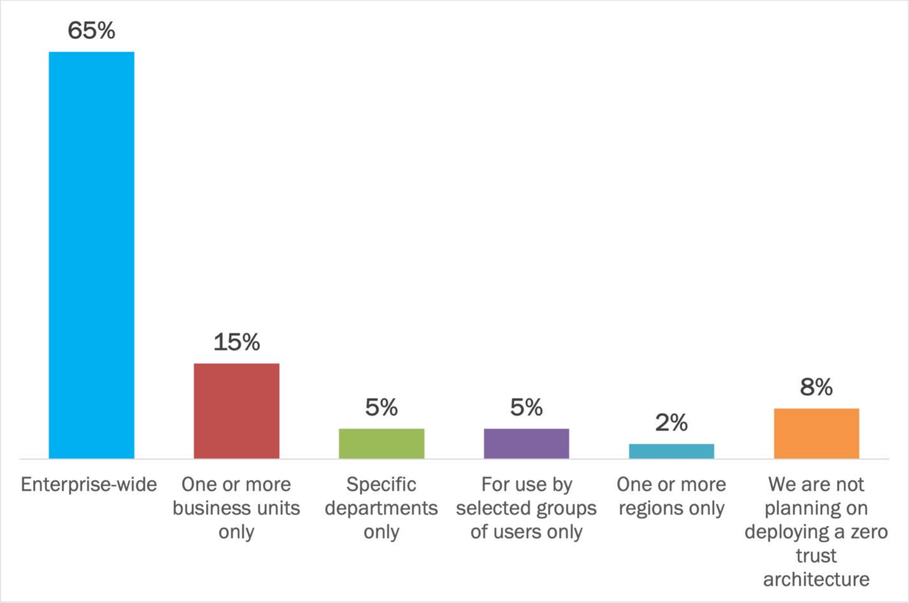
# Deployment Scope, Cadence, and Plans

Organizations are deploying a zero trust architecture to mitigate the threat of current trends and increase the efficacy of cybersecurity protections. In this section, we look at deployment specifics, such as scope, priority, cadence, and budget.

### SCOPE IS ENTERPRISE-WIDE OR MULTIPLE BUSINESS UNITS

Two out of three organizations are planning an enterprise-wide scope of deployment for a zero trust architecture. Excluding the 8% of organizations that are not planning to deploy zero trust at all, the remainder are planning to limit the scope of deployment to subsets of the organization based on business unit (15%), department (5%), group (5%), or region (2%). See Figure 5.

**Figure 5**
**Planned Scope of Deployment of a Zero Trust Architecture**
Percentage of respondents



***Source: Osterman Research (2021)***

*Creating threat susceptibility by safeguarding less than 100% of the enterprise with zero trust protections is not a strong cybersecurity strategy.*

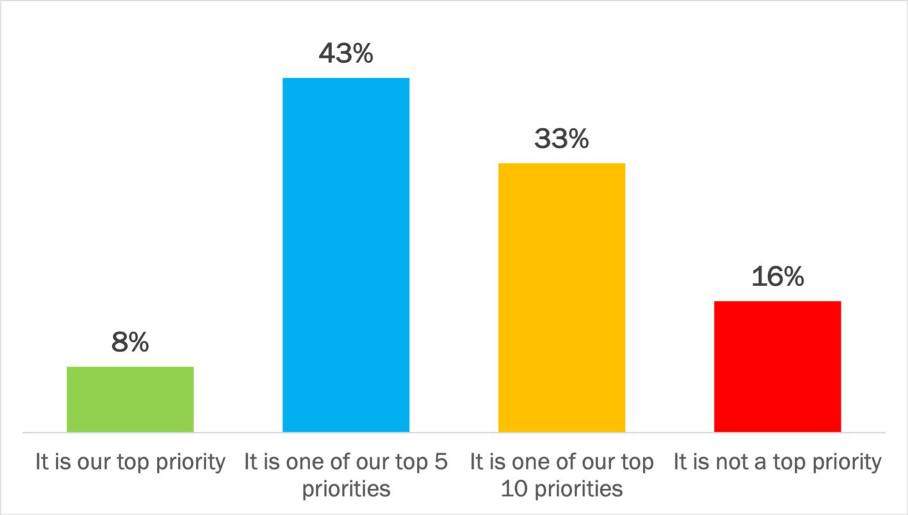
Organizations are not viewing zero trust as an "all-or-nothing" approach. We were surprised that only 65% of organizations have set an enterprise-wide scope for zero trust; we thought it would be much higher. Creating threat susceptibility by safeguarding less than 100% of the enterprise with zero trust protections is not a strong cybersecurity strategy. We expect to see those organizations initially limiting their deployment scope moving to full enterprise-wide deployment as they reap the initial wave of benefits and gain expertise with zero trust.

Eight percent of total respondents said they are not planning on deploying a zero trust architecture, but over half have allocated a budget for zero trust initiatives over the next two years. The 8% figure, therefore, indicates respondents with no plans to deploy zero trust this year—rather than respondents with no plans to deploy zero trust ever.

## MOVING TO ZERO TRUST IS A HIGH PRIORITY

Implementing a zero trust architecture is one of the top five security priorities at more than half of organizations. Overall, implementing zero trust is the top priority for 8% of organizations. See Figure 6.

**Figure 6**
**Priority of Implementing Zero Trust Relative to all Security Priorities**
Percentage of respondents



***Source: Osterman Research (2021)***

**51%**

***Organizations where implementing a zero trust architecture is a top-5 priority.***

In looking at the data:

- **The matrix of benefits to realize and risks to mitigate supports high prioritization of zero trust initiatives**
  An earlier section in this report highlighted four drivers for deploying a zero trust architecture: mitigating current trends and threats, achieving higher cybersecurity efficacy, strengthening protections, and safeguarding data sources. These drivers cover both benefits to realize and risks to mitigate, and on balance, present a compelling case for zero trust. Expectations around outcomes support the prioritization of zero trust initiatives.

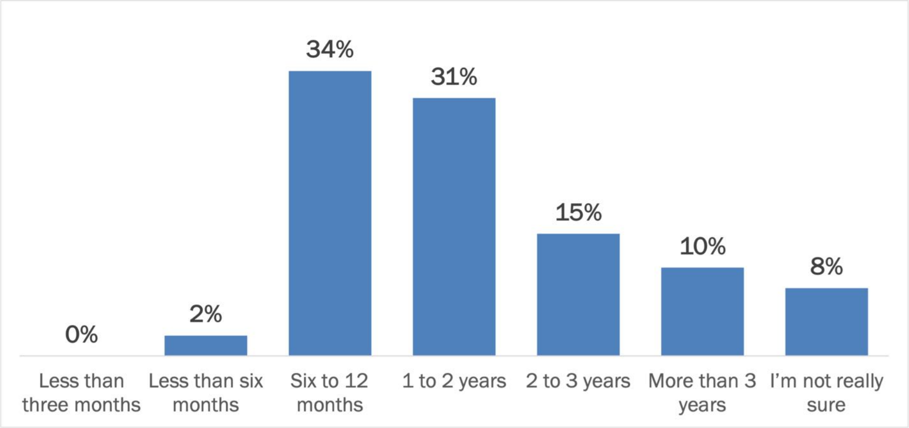
- **Alignment with our other research on priority initiatives**
  In other recent surveys by Osterman Research, respondents have assigned high priority to initiatives that complement zero trust approaches, including discovering sensitive data,[9] preventing data exfiltration,[10] and assessing the extended cybersecurity threat surface for organizations with subsidiaries.[11] Across multiple separate surveys, therefore, respondents are indicating heightened focus on initiatives to improve baseline cybersecurity protections.

- **Half of organizations where zero trust is not a top priority do not plan on implementing zero trust**
  Eight percent of survey respondents indicated their organization is not planning on implementing zero trust (see Figure 5 above). All these respondents also said that zero trust is not a top priority in Figure 6. This represents one half of the 16% group.

## FULL DEPLOYMENT IS EXPECTED TO TAKE LESS THAN TWO YEARS

Two out of three organizations expect to achieve full deployment of a zero trust architecture in a timeframe ranging from three months to two years. One in 10 organizations expect it to take more than three years, and slightly less than this are not sure how long deployment will take. See Figure 7.

**Figure 7**
**Expected Timeframe to Fully Deploy a Zero Trust Architecture**
Percentage of respondents



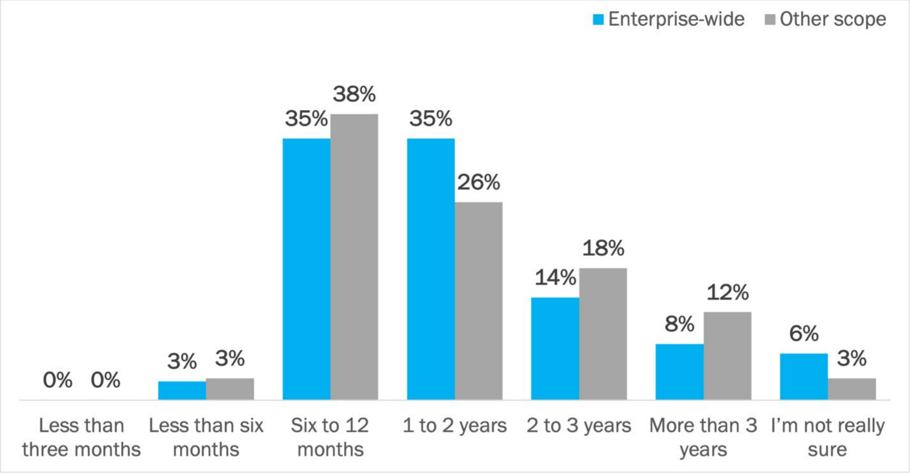
*Source: Osterman Research (2021)*

## DEPLOYMENT SCOPE DOES NOT SIGNIFICANTLY IMPACT TIMEFRAME

The intended scope of deployment—enterprise-wide compared with the more limited scopes (e.g., business unit, department, group, region)—does not have a significant impact on the expected deployment timeframe. Although slightly more organizations with one of the limited scopes expect to be at full deployment within six to 12 months, more organizations with a limited scope than the enterprise-wide deployment scope expect it to take two years or longer. See Figure 8.

*Organizations deploying zero trust with a more limited scope do not expect to see a significantly faster deployment timeframe.*

**Figure 8**
**Timeframe for Deployment Based on Deployment Scope**
Percentage of respondents

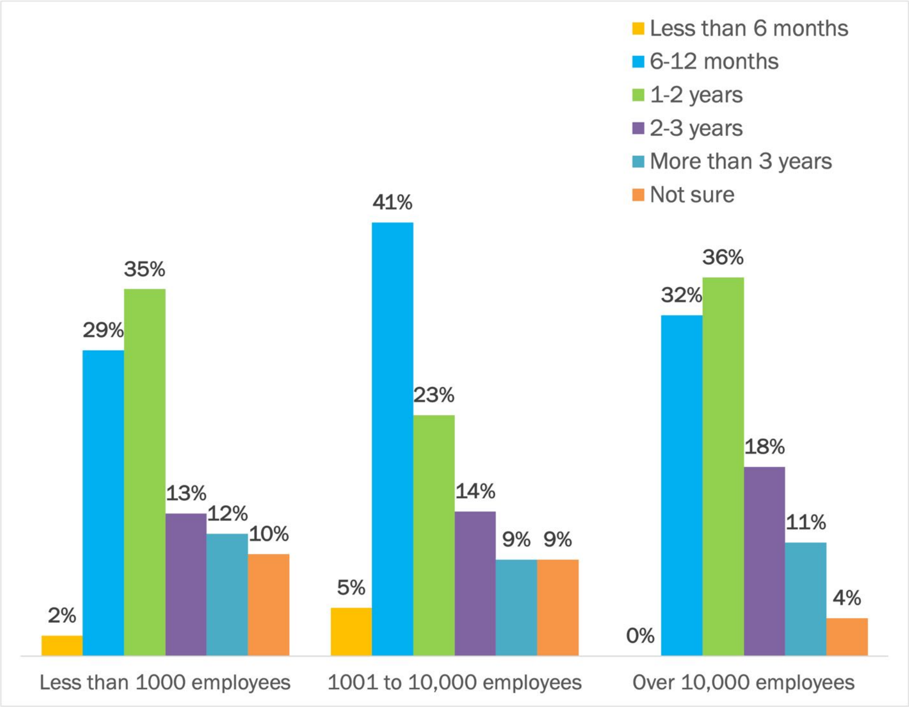


*Source: Osterman Research (2021)*

## LARGER ORGANIZATIONS EXPECT TO DEPLOY FASTER

Larger organizations expect to achieve full deployment faster than smaller organizations. For example, 46% of organizations with between 1,001 and 10,000 employees expect to achieve full deployment of a zero trust architecture in one year or less, compared with only 31% of organizations with 1,000 employees or fewer. Smaller organizations are the most likely of the three groupings to take more than three years to achieve full deployment or not know how long deployment will take. See Figure 9.

**Figure 9**
**Timeframe for Deployment Based on Organizational Size**
Percentage of respondents



*Source: Osterman Research (2021)*

*Larger organizations expect to achieve full deployment faster than smaller organizations.*

Larger organizations can deploy technologies such as zero trust faster than smaller organizations for several reasons:

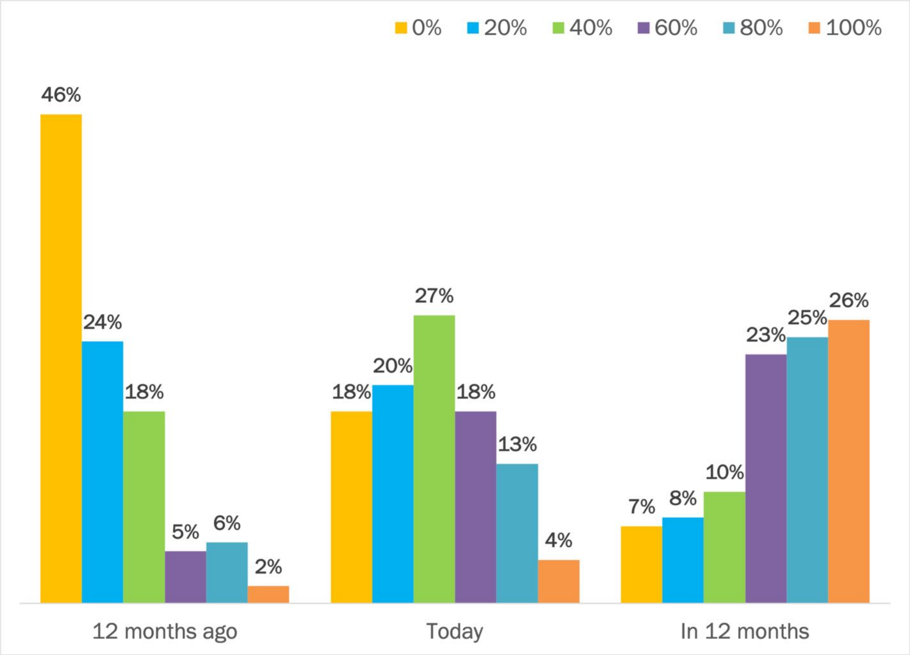
- **Better resourcing due to access to more full-time IT staff**
  Larger organizations are more likely to have cybersecurity and IT security professionals on staff, thus simplifying access to people with the required skills and enabling concentrated effort to deploy new technology. While the deployment scope covers many more people, professionals are available to fast-track the deployment cadence.

- **Higher urgency due to reputational and financial damage**
  The risk of reputational damage, regulatory fines, and other financial penalties to larger organisations is often higher and more significant than for smaller firms. There is a greater sense of urgency, therefore, to decrease the attack surface, shore up cybersecurity protections, and be seen to be utilizing the best technical and organizational approaches against cybersecurity threats.

## RAPID SWING TOWARDS HIGHER DEPLOYMENT

Organizations are rapidly swinging towards full deployment of a zero trust architecture, with 26% of organizations expecting to be fully deployed in 12 months time. See Figure 10.

**Figure 10**
**Completeness of the Move to a Zero Trust Architecture Over Three Years**
Percentage of respondents (sums to 101%, 100%, and 99% due to rounding )



*Source: Osterman Research (2021)*

The swing towards higher deployment over an average of two years is consistent with the general timeframe for deployment in the earlier Figure 7:

- **From low deployment to high deployment**
  Twelve months ago, 70% of organizations were 20% or less complete in the move to zero trust. Today, 65% of organizations are between 20% and 60% complete. In 12 months, it is expected that 74% will be between 60% and 100% complete (including 26% at full deployment).

- **The next 12 months is critical for zero trust initiatives**
  Organizations will want to start reaping the early benefits from shifting to zero trust architectures over the next 12 months. Early successes in reducing the incidence of data breaches, insider threats, and ransomware attacks will fuel the organizational willingness to complete and extend currently planned zero trust deployments.

- **One quarter at only 40% or less in 12 months**
  Although there is a strong swing towards higher deployment rates, one quarter of respondents anticipate still being only 40% or less deployed in 12 months. Some of these are organizations who are only just beginning their zero trust journey in 2021, or are not starting with zero trust until 2022 or later.

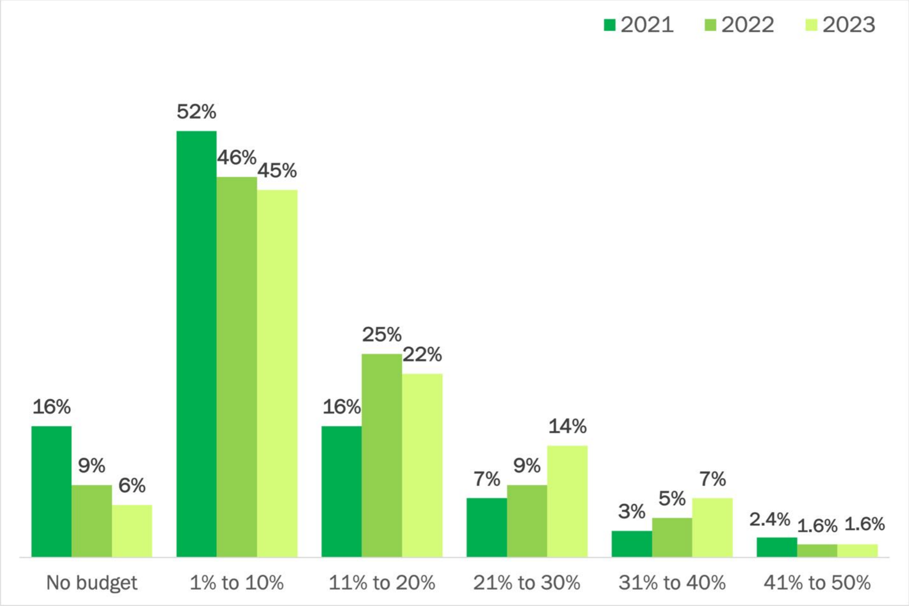
***2 years***

***Anticipated maximum deployment timeframe for most organizations.***

## MORE BUDGET IS ALLOCATED FOR ZERO TRUST INITIATIVES

The percentage of the total IT budget allocated to zero trust initiatives varies significantly between organizations. For 2021, over half of organizations have allocated between 1% and 10% of their total IT budget for zero trust initiatives, and a further 16% have allocated 11% to 20%. In 2022 and 2023, fewer organizations are allocating 1% to 10% and more are allocating 11% to 20% of their total IT budget. Over the next two years, an increasing number of organizations are allocating more than 20% of their total IT budget for zero trust initiatives. Organizations indicating they were not deploying zero trust in any of the three years were removed from this data. See Figure 11.

**Figure 11**
**Bands of Total IT Budget Allocated for Zero Trust Initiatives by Year**
Percentage of respondents



*Source: Osterman Research (2021)*

*Organizations are allocating more of their IT budget to zero trust initiatives year on year.*

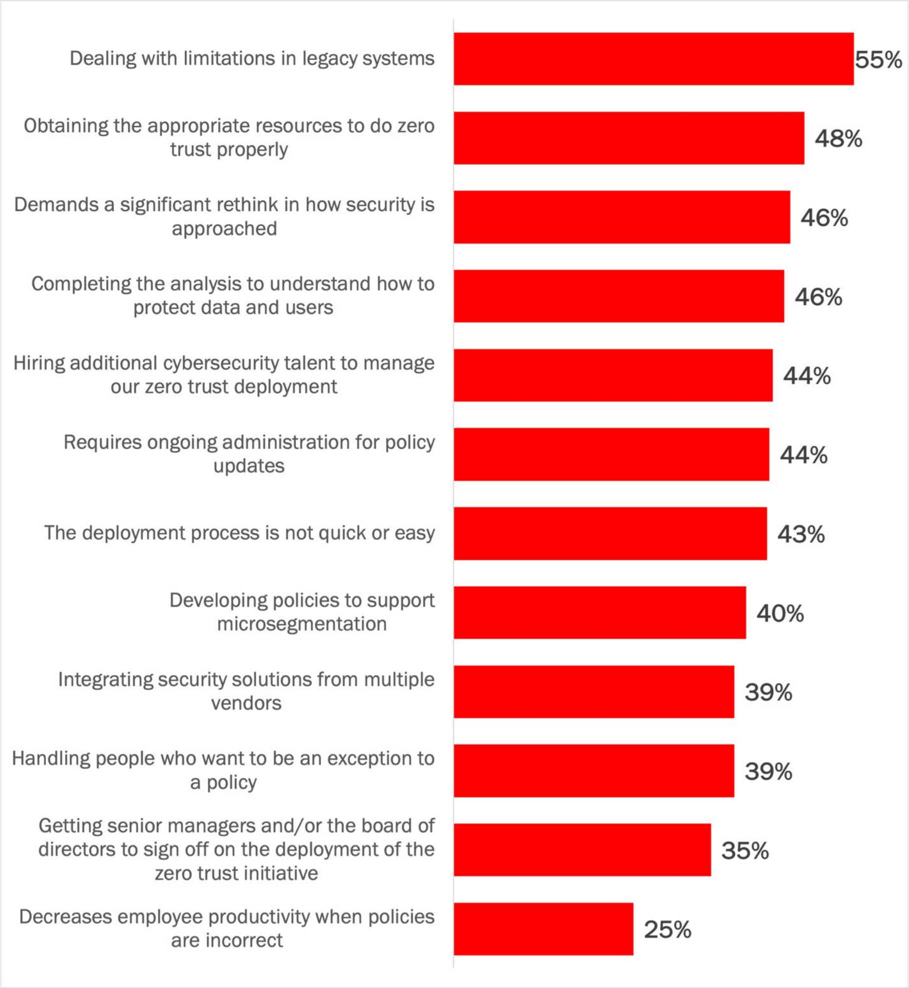
Fewer organizations year on year are allocating no budget to zero trust initiatives. More than half of the organizations indicating they had no plans to deploy zero trust in 2021 (and therefore did not allocate budget) have actually allocated budget to zero trust beginning in 2022 and/or 2023. This accounts for most of the reduction in the "no budget" band above.

Many of the budgeted expenditures that currently fall under a zero trust umbrella deliver benefits beyond zero trust initiatives exclusively. Solutions for improving identity and access management, for example, may have been reallocated under the zero trust category in the IT budget this year, but deliver wider benefits for other budget categories too.

## ORGANIZATIONS HAVE BARRIERS TO OVERCOME

Zero trust initiatives can be derailed, delayed, or undermined when potential barriers are ignored. Respondents ranked the significance of 12 potential barriers to zero trust. The top-ranked barrier is dealing with limitations in legacy systems—such as the inability to leverage contextual signals to determine which micro-segmentation policy is most appropriate. See Figure 12.

**Figure 12**
**Key Barriers to Embracing Zero Trust**
Percentage of respondents indicating barriers were "highly" or "extremely" significant



*Source: Osterman Research (2021)*

> *Organizations face a set of barriers to overcome when deploying a zero trust architecture.*

In looking at Figure 12, we draw the following conclusions:

- **It is still early days for many organizations with zero trust**
  The rank ordering of the barriers reflects that many organizations are still in the early days of zero trust, they are just starting, or they are yet to start. The five top-rated barriers—three technical and two resourcing ones—are critically important in the initial stages of deploying zero trust but should become less of a barrier as organizations get further along with zero trust.

- **The current lowest-ranked organizational barrier will become critically important over time**
  The current lowest ranked barrier is an organizational one: employee productivity is decreased when policies are incorrect. Over time, we expect this barrier to become the critical pivot for the success or failure of zero trust. For example, if micro-segmentation policies do not keep up when employees change jobs, productivity will take a hit. Required files and applications will be inaccessible, which may lead to unsanctioned services being used to get around outdated micro-segmentation policies. Alternatively, if an executive is denied access to a critical resource while traveling that results in the business losing a significant client opportunity, zero trust approaches may carry the blame.

- **Dealing with limitations in legacy systems**
  Systems developed before the principles of zero trust became commonly accepted lack the programming hooks, APIs, and design models to leverage contextual signals to determine which micro-segmentation policy is most appropriate for a specific authentication event and data request. Organizations with a stable of older systems must either decrease the planned scope of deployment by using generalized rather than specific micro-segmentation policies, redevelop legacy systems to support zero trust (which may be impossible), or migrate to newer modern systems that support zero trust principles by design. For core business applications that are not zero trust–aware, migrating to a modern platform is a significant undertaking with costs and implications that reach far beyond zero trust alone.

- **Integrating security solutions from multiple vendors**
  Two out of five respondents see integrating security solutions from multiple vendors as a highly or extremely significant barrier to success with zero trust. Organizations with legacy security solutions will struggle with making zero trust work just as much as organizations with legacy business applications that do not support zero trust approaches. The challenge of integration will be even greater if hardware and software vendors embrace a slower approach to supporting zero trust than what organizations would prefer in order to meet their internal deployment timeframes.

- **Data security in the cloud is the new frontier**
  Safeguarding data in the cloud is the new frontier as organizations increase their use of cloud services. Widespread adoption of the cloud has led to significant cybersecurity incidents, including massive data breaches, misconfigured security rights, and targeted attacks to steal cloud credentials. Getting data security right for sanctioned cloud services is enough of a challenge for organizations, but almost all also have a whole suite of unsanctioned services in use by employees that fall outside of accepted controls.

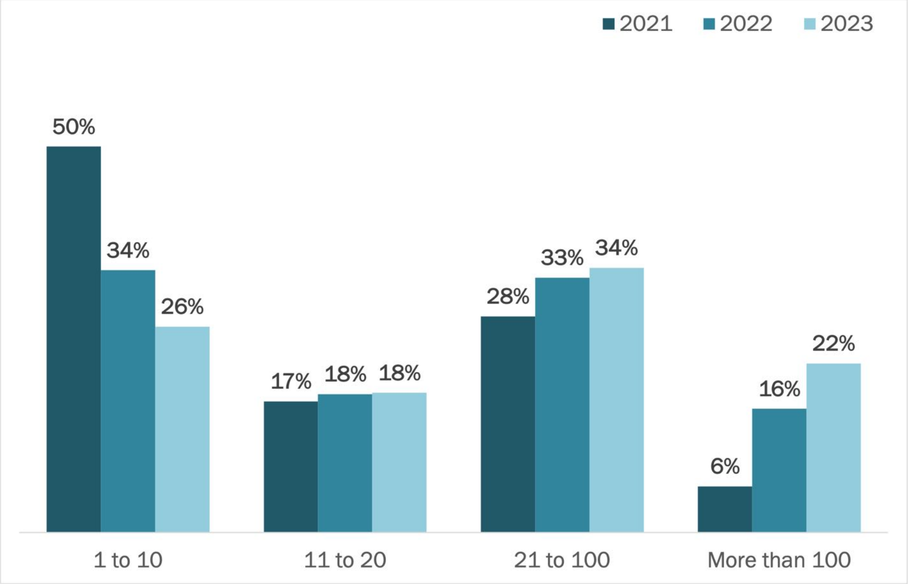
- **Zero trust requires a new mindset—for IT professionals and everyone else too**
  Security used to mean keeping the inside safe from the outside. Zero trust removes the concept of sides entirely—there is no inside or outside as elemental divisions—and replaces sides with a set of assessment criteria that must be weighed each time a resource is requested. IT professionals must embrace this new mindset when architecting a coherent set of solutions that combine to meet the design goals of zero trust, as must everyone else in the organization in relation to the removal of standing access rights to resources. Understanding how zero trust changes security is key to minimizing unreasonable demands by people who want to be an exception to a policy.

> ***After initial technical barriers to deployment are resolved, we expect the impact of zero trust on employee productivity to become the critical issue.***

## THE NUMBER OF POLICIES IS EXPECTED TO INCREASE

Most organizations deploying zero trust expect to see annual increases in the number of micro-segmentation policies used. The number of organizations using ten or fewer policies is expected to drop by 50% over the next three years, and the number using more than 100 separate micro-segmentation policies is expected to increase by almost four times. See Figure 13.

**Figure 13**
**Expected Number of Separate Micro-segmentation Policies**
Percentage of respondents by band by year



***Source: Osterman Research (2021)***

*Most organizations deploying zero trust expect to see annual increases in the number of micro-segmentation policies used.*

In looking at the underlying data, we found:

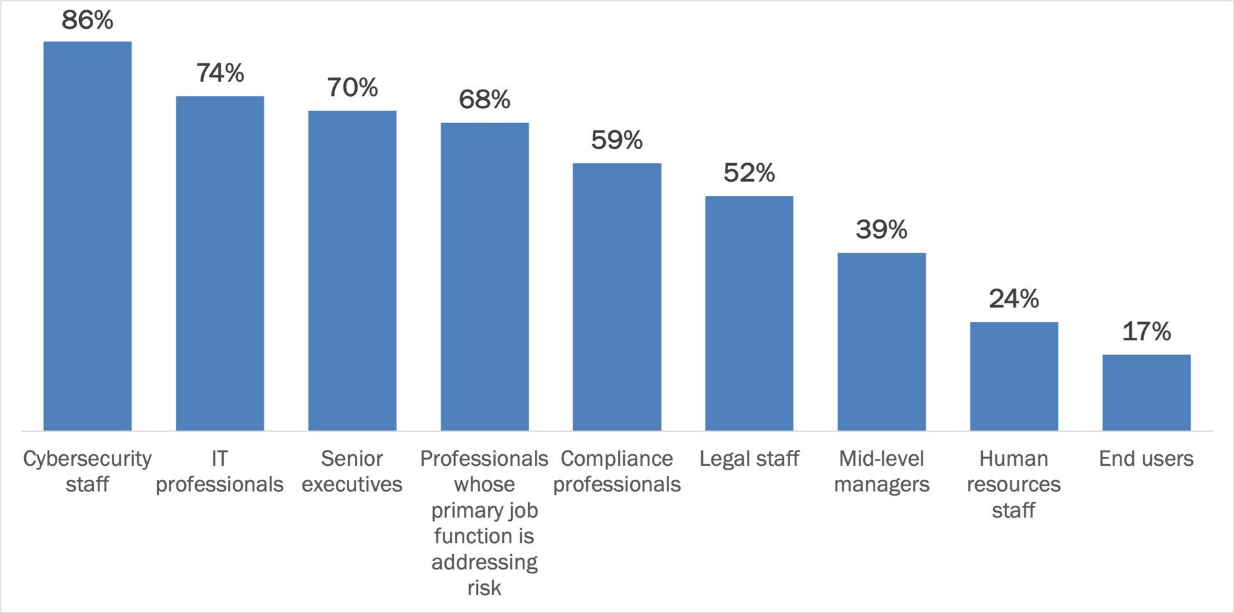
- **Three patterns in the number of micro-segmentation policies**
  Just under three out of five organizations expect the number of policies to increase year on year over the next three years, one fifth expect the number of policies to remain unchanged each year, and the remainder expect some other pattern of variation, e.g., the number of the policies increases from 2021 to 2022 and then decreases in 2023.

- **Larger organizations expect to have more policies**
  The larger the organization, the more micro-segmentation policies are expected. Among organizations with fewer than 1,000 employees, only 9% expect to have more than 100 policies by 2023. Among organizations with 10,000 or more employees, 39% expect the same.

## GROUPS INVOLVED IN DEFINING THE REQUIREMENTS FOR ZERO TRUST

Respondents indicate that cybersecurity staff, IT professionals, and senior executives are the three groups with the highest levels of influence for defining the requirements for zero trust. Risk, compliance, and legal professionals are in the middle of the pack for levels of influence, and end users are viewed as having the least influence on the decision-making process even though they are potentially most impacted daily, notably when micro-segmentation policies get in the way of productive work. See Figure 14.

**Figure 14**
**Influence of Groups in Zero Trust Initiatives**
Percentage of respondents indicating high levels of influence



*Source: Osterman Research (2021)*

A common challenge with projects that include a high technical component is that they are either driven by the IT department without consultation with other parts of the organization (the IT-led project type) or are assumed to be an IT project only and left to the IT department by default (the disinterested business project type). In both cases, projects that are deemed a technical success can fail organizationally. In a technical project we would expect to see high levels of influence by cybersecurity staff and IT professionals, but in a project with a broader business-led mandate, we would want to see higher levels of involvement from the other groups in Figure 14 above. In the best-case interpretation, the influence ratings above reflect that zero trust is still in its early days for many organizations and therefore currently has high technical demands, but that once technical implementation decisions are finalized, wider business involvement is expected or planned. In the worst-case interpretation, technologists are again imposing heightened security restrictions without business buy-in. To avoid the outcome of a perfect technical solution that fails organizationally, every organization must explicitly make the decision whether zero trust is a technical or a business project and staff it accordingly.

> ***Is zero trust a technical project or a business one? Every organization needs to make an explicit decision and staff the project accordingly.***

## Solutions for Zero Trust

We have explored the findings from our recent survey in this white paper. In this section, we present an overall sense of the types of solutions required for making zero trust work.

- **Continuous verification of identity**
  Knowing with precision and certainty the identity of every given person and device on a continuous basis as they access various resources and applications is a critical part of zero trust. Without it, inappropriate levels of access to data and systems will be offered if the identity is not continuously verified, or when an incorrect micro-segmentation policy is triggered. Solutions to investigate include stronger forms of multi-factor authentication, contextual and step-up authentication, and for most deployments, centralized biometric authentication, which offers the only way of uniquely identify a person rather than a device, phone, or security token. Ultimately, stronger authentication approaches beyond a username and password must be used in all situations.

- **Replacing top-level admin access rights with tighter controls**
  For many years, IT administrators have had top-level admin access rights to data in core business systems, along with the expectation of not abusing that trusted position. This historical approach is incompatible with zero trust. Access by IT administrators must be managed, curated, limited, scoped, and audited. Solutions that deliver these capabilities fall under the privileged access management moniker.

- **Detecting characteristics in devices, networks, and geographical locations**
  Micro-segmentation policies rely on the ability to differentiate certain attributes in devices, networks, and geographical locations, among others. Solutions are required that can reliably identify the type of device being used in an access request, whether it is a managed or unmanaged device, the network type and address range, and geospatial indicators to plot the access request in physical space. These discernable attributes need to be available immediately for use in policy selection.

- **Detecting the presence of sensitive and confidential data**
  Micro-segmentation policies can be configured to protect data in pre-defined systems, but they risk being too brittle when files containing sensitive and confidential data are stored in places that was not foreseen. The ability to detect sensitive and confidential data in files, cloud data stores, structured data systems, and emerging user-generated data systems (e.g., Microsoft Teams, Slack) will be key to ensuring that the protections of the most appropriate policy are applied.

- **Establishing resource-constrained connections**
  Solutions that enable software-defined perimeters (SDPs) are a key networking enabler for zero trust. SDP solutions bring together the verified user identity and validated device status to provide a unique and time-limited connection to the resources required by the user.

> ***Zero trust architectures leverage solutions that deal with identities, access controls, and protections for sensitive data, among others.***

- **Selecting modern applications designed to safeguard data**
  Data is compromised when systems are breached through stolen credentials, backdoors, and unpatched vulnerabilities. Compromised email accounts are an especially attractive target for cybercriminals, because they usually contain sensitive and confidential files in addition to communication chains and patterns. Sensitive and confidential files can be used to undermine the organization, extort customers, and steal intellectual property. Deploying new solutions that offer modern ways of securely transferring data between people, processes, and organizations reduces the attack scope against email accounts, removes sensitive and confidential files from unmanaged repositories, and enforces strong security over data in transit and data at rest.

- **Identifying gaps in micro-segmentation policies that create vulnerabilities**
  No selection of micro-segmentation policies will be perfect on their first iteration. Policies will have to change over time as more is learnt about supporting both security and employee productivity. New threat vectors will demand the creation of new policies to address unforeseen situations. New applications and ways of working will require ongoing administration to ensure the current set of policies enforces appropriate protections. As policies are created, modified, and deleted, organizations risk exposing applications and data through unintentional gaps in policies. Organizations will require solutions that uncover policy gaps based on recursive analysis of policy chains as well as monitored events that fall outside of the intent of current policies.

- **Finding complementary solutions to address vulnerabilities in applications**
  Vulnerabilities in business applications and cloud services provide alternate ways of accessing business data that bypass zero trust controls. Organizations need to ensure ongoing integrity in their applications and cloud services through methods such as vulnerability management, patching, and virtual isolation.

- **Embarking on a complementary program to mitigate limitations in legacy applications**
  Legacy applications that do not support zero trust approaches will hamper or derail zero trust initiatives. Address technical debt through a complementary program to resolve current limitations in legacy applications by upgrading to newer versions. Where that is not an option or not strategically aligned with the direction of your organization, replace legacy applications with modern alternatives. Digital transformation is a significant undertaking for organizations and such initiatives will have their own timeframes that unlock added value from a zero trust architecture over time.

*Zero trust is the security architecture for the new world of work.*

## Conclusions and Next Actions

The world has changed with relentless cyberattacks, the adoption of cloud services, and new work-from-home and hybrid working models. Security architectures predicated on people and devices being inside the corporate network do not work in this changed world. Many organizations have already started the journey to using zero trust design principles and approaches to rearchitect security for the modern age. Those who have not already started need to get going.

# Sponsored by BIO-key International

BIO-key is a trusted provider of Identity and Access Management (IAM) and Identity-Bound Biometric solutions that offer an easy and secure way to authenticate the identity of employees, customers, and suppliers while managing their access across devices and applications.

Over 1,000 global customers, including the federal government and 200+ higher education institutions, trust BIO-key PortalGuard IDaaS, an award-winning IAM platform, to reduce password-related help desk calls by up to 95%, eliminate passwords, secure remote access, prevent phishing attacks, and improve productivity for the IT team. PortalGuard provides the simplicity and flexibility required to secure the modern digital experience with options for single sign-on, self-service password reset, and over 16 multi-factor authentication methods, and is the only IAM platform to offer Identity-Bound Biometrics.

Backed by decades of expertise, BIO-key has a proven track record of successful IAM project delivery and strong customer relationships.

Learn more at www.BIO-key.com.

BIO-key®

www.BIO-key.com

info@BIO-key.com

+1 732 359 1100

Osterman Research does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

[1] Linda Rosencrance, History and evolution of zero trust security, June 2021, at https://whatis.techtarget.com/feature/History-and-evolution-of-zero-trust-security

[2] Doug Barney, Three Keys To Healthcare IT: HIPAA, Zero Trust, and Ensuring File Transfers Are Secure, August 2021, at https://blog.ipswitch.com/three-keys-to-healthcare-it

[3] IBM Security, Cost of a Data Breach Report 2021, June 2021, at https://www.ibm.com/security/data-breach

[4] Threatpost, What's Next for Ransomware?, December 2020, at https://threatpost.com/webinars/whats-next-for-ransomware/

[5] Tessian, Why DLP Has Failed and What the Future Looks Like, December 2020, at https://www.tessian.com/research/the-state-of-data-loss-prevention-2020/

[6] ICO, Data security incident trends: Q2 2021-22, October 2021, at https://ico.org.uk/action-weve-taken/data-security-incident-trends/

[7] BlackFog, The Shift from Ransomware to Data Theft Extortion, May 2021, at https://www.blackfog.com/shift-from-ransomware-to-data-theft-extortion/

[8] IBM Security, Cost of a Data Breach Report 2021, June 2021, at https://www.ibm.com/security/data-breach

[9] Osterman Research, Sensitive Data Discovery Rises as a Top Concern for Organizations, September 2021, at https://ostermanresearch.com/2021/09/22/activenav-sensitive-data-discovery/

[10] Osterman Research, Preventing Data Exfiltration: Introducing Anti-Data Exfiltration (ADX), October 2021, at https://ostermanresearch.com/2021/10/26/orwp_0347/

[11] Osterman Research, Managing Risk from Subsidiaries: Goals, Friction, and Failure, September 2021, at https://ostermanresearch.com/2021/09/23/cycognito-subsidiary-risk/