DARKReading RESEARCH

OCTOBER 2022

State Of Zero Trust in The Enterprise: Shift To Identity-Powered Security

NetIQ

Executive Summary

Cybersecurity has changed. The attack surface has expanded, thanks to the rapid adoption of cloud applications and services, shift to remote work, and proliferation of mobile devices. Having enterprise systems, applications, and data in one location and relying on layers of security tools and controls to keep attackers out, is no longer sufficient when the bulk of data and workloads now live outside the traditional network. Attackers are also increasingly targeting credentials to appear as legitimate users.

This rising menace is why enterprises are increasingly embracing zero trust as a necessary strategy for securing the business and proactively managing risk. Defenders understand that identity and privilege access management are critical first steps to zero trust, but many of them have not gotten further than implementing multi-factor authentication. Privilege management and identity governance are emerging as a bigger focus for organizations, but defenders are still figuring out how to stay ahead of the rapidly changing digital landscape and all its threats.

A new study commissioned by NetIQ at Micro Focus, and conducted by Dark Reading, indicates that organizations are on a maturity journey to protect their network environment. They are now moving beyond the limitations of network and endpoint controls and are looking to deploy more dynamic and adaptive security management throughout the user session. Specifically, while many organizations have enabled multi-factor authentication, research results make a strong case that they are increasingly exploring a more comprehensive approach that integrates identity management and privileges management across zero trust environments.

Top Findings

Accepting Zero Trust: Of the 104 security practitioners polled, 87% said they were on the zero trust journey — having already rolled out zero trust or making plans for implementation. Organizations not implementing zero trust are hampered by limited budgets and resources, not lack of interest.

MFA for Some: Respondents recognize that multifactor authentication is critical, as 61% said they have already implemented it for employees, and 33% have plans to implement it at some point over the next 12 months. However, only 38% have extended MFA for external users accessing their applications, and 47% have plans to do so over the next 12 months.

Privileges and APIs Aren't the Focus: Defenders are overly focused on MFA and aren't addressing other components of the zero trust strategy, including privilege access management and API security. Just 36% said they are securing access to APIs, 44% said they have plans to in the next year, and 33% said they implemented privileged access to cloud infrastructure **(Figure 1).**

Securing Endpoints: Respondents are still thinking in terms of endpoints. Two-fifths of respondents (40%) said it was most important to integrate endpoint protection with identity and access management to support zero trust **(Figure 2)**. Just about a third of respondents named identity governance (36%) and privileged access management (32%).

Protecting Against Credentials Theft: Defenders are more confident in their organization's ability to manage risk and protect account credentials than they are in securing cloud platforms. Eighty-one percent rated their organization's management of risks associated with account credentials as excellent or good. Two-thirds (66%) said the same about cloud platforms and infrastructure, and for cloud applications it was 65% who gave themselves an excellent or good rating.

Figure 1.

Zero Trust Implementation

Where is your organization in your zero trust journey?

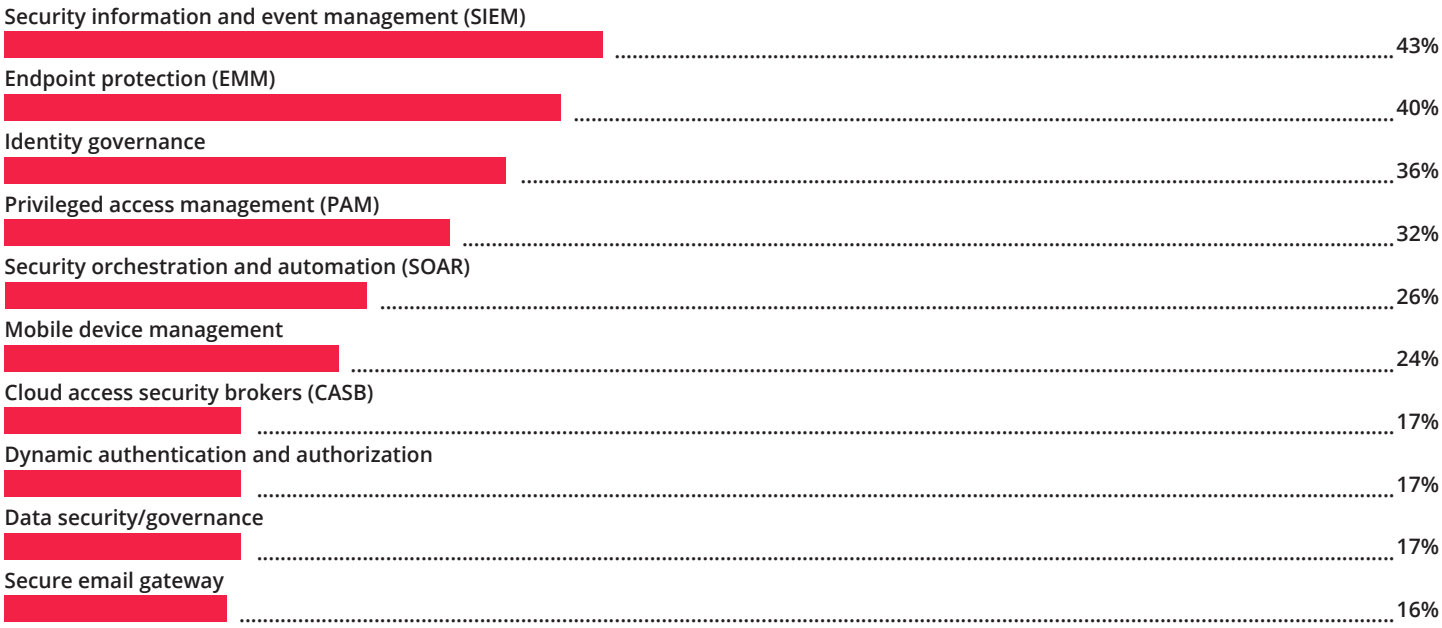
	Already implemented today	Will be implemented in the next 6 months	Priority in the next 12 months	Priority in the next 18 months	N/A
MFA for employees	61%	17%	16%	5%	1%
Single sign-on for employees	57%	20%	12%	6%	5%
Employee directory is connected to cloud apps	44%	17%	21%	11%	7%
MFA for external users	38%	26%	21%	8%	7%
Securing access to APIs	36%	21%	23%	12%	8%
Identity governance	36%	24%	20%	12%	8%
Privileged access to cloud infrastructure	33%	27%	25%	9%	6%
Single sign-on for external users	32%	25%	18%	8%	17%
Automated provisioning/deprovisioning for employees	31%	21%	22%	12%	14%
Data governance	30%	30%	20%	12%	8%
Deploying multiple factors across user groups	29%	31%	25%	8%	7%
Automated provisioning/deprovisioning for external users	23%	24%	21%	11%	21%
Context-based access policies	21%	24%	29%	11%	15%
Passwordless access	12%	20%	20%	20%	28%

Base: 90 respondents who have implemented, are in the process of implementing, or actively considering implementing zero trust by next year
Data: Dark Reading survey of 104 cybersecurity and IT professionals at companies with 100 or more employees, May 2022

Figure 2.

Important Factors to Integrate with IAM

Which of the following do you consider most important to integrate with IAM to support zero trust?



Note: Maximum of three responses allowed
Base: 90 respondents who have implemented, are in the process of implementing, or actively considering implementing zero trust by next year
Data: Dark Reading survey of 104 cybersecurity and IT professionals at companies with 100 or more employees, May 2022

Zero Trust: A Framework for Resilience

Traditional enterprise security was based on the assumption that all applications, systems, and data were stored in one physical location, usually where the organization maintained its offices. Putting up a moat around the network in the form of different types of security tools and controls made sense when attackers were outside the organization. The modern IT environment — with cloud-based infrastructure, platforms, and software; proliferation of mobile devices and personal devices; new web-based services and applications; and a distributed workforce connecting from different networks — has expanded the organization's attack surface and introduced unprecedented exposure to risk of cyberattacks and data loss.

According to the most recent "Data Breach Investigations Report" from Verizon, some 80% of data breaches are caused by external threat actors. However, as the DBIR notes, use of stolen credentials and phishing are the two most common methods attackers utilize, as they were used in around two-thirds of all data breaches. Criminal actors are increasingly focusing their efforts to steal credentials because it is far easier to just sign into the system or application remotely than to try to exploit a vulnerability or rely on malware backdoors to gain access. The latest IBM Research shows the average total cost of a data breach increased by nearly 10% year over year, the largest single year cost increase in the last seven years. The report concurs with the DBIR, noting that compromised credentials has been the most common initial attack vector, responsible for 20% of breaches. The DBIR also notes that 82% of data breaches involved the human element, which includes stolen credentials, phishing, misuse, or error — underscoring the fact that organizations have to consider every user, device, and service that requires access as potentially hostile, even if it's a known and approved entity.

That is where zero trust comes in. Zero trust is not a single piece of software. Rather, it's a strategic framework for resilience — one that provides organizations with an integrated plan to withstand attacks while continuing to provide critical business functions. The key components for a zero trust architecture include least privilege access, micro-segmentation, multifactor authentication, API control and monitoring, and adaptive authentication.

Zero trust implementation hinges upon recognizing who is trying to access the enterprise resource, and whether or not they should be allowed to access it. For organizations, this goal requires maintaining strict controls at every point of access and focusing on the identity as being the differentiator (instead of location, as in a perimeter defense). To understand the framework better, it is helpful to think of it in four integrated concepts or directives.

1. Don't assume trust. This means maintaining strict controls at every point of access, and not trusting anyone or anything by default.
2. Follow the philosophy of least privilege. Grant access to only what is needed; nothing more, nothing less.
3. Break the environment down into smaller security zones. This minimizes the possible damage by slowing down the progress of a potential attack.
4. Verify identity at every step. Guarantee a high level of assurance between security zones.

The foundation, or architecture, of the zero trust framework rests on the concept of Least Privilege Access, or granting only as much access as necessary, and equally, only the minimum permissions for the shortest duration required. Other tactical components include organizing the environment using micro-segmentation to limit the scope of access by breaking the environment down into smaller security zones and maintaining separate security controls for each compartment; requiring multifactor authentication (MFA), so that two or more verification factors are needed in order to gain access to a resource; securing and monitoring APIs by tightly governing how many different devices and APIs can access resources; and cultivating an adaptive environment and approach, where access is dynamically determined based on the current state and past activity.

Adaptive access management is the crucial ingredient in zero trust. Static configuration measures depend on simple criteria — whether the user is remote or the device is already known. Unfortunately, this approach falls short if the known device has been compromised since the last time it was assessed or the user's behavior has changed since the initial login.

With adaptive access management, neither the user's device nor the origin of the request automatically grants access to services. Instead, continuous authentication repeatedly gathers access metrics and recalculates risk. This control across each session, along with the extending monitoring and control throughout the session, empowers the capacity for:

- Detecting when the risk level has changed since the start of the session and then initiating an authentication request.
- Tuning (reducing or increasing) the authorization level based on the identified risk and available identity verification.

Raising access security to a zero trust level leverages this adaptive or continuous analysis and control.

Our research shows that mid-to-large organizations (organizations with 100 or more employees) are beginning their zero trust journey, but most are still in the early stages. While many of the organizations have made some progress towards multifactor authentication, and applying identity and access management to the network, they also are still relying on traditional security defenses such as virtual private network (VPN) solutions. The findings demonstrate that defenders are beginning to realize that privileges and identity governance are critical for zero trust deployments, but they still face challenges integrating identity access management into their environment to support zero trust architecture.

How Organizations Are Thinking About ZT and IAM

Of the 104 IT and security professionals in the survey, 87% had already implemented, or were in the process of implementing or planning to implement, zero trust architecture in their environment. When this group was asked what words came to mind when they thought of zero trust, several of the responses spoke to the underlying concepts, such as "identity access management," "segmentation," "limit access," and "least privileged access."

Among the small group of IT and security professionals who said they currently had no zero trust plans, the barrier to adoption appears to be more along the lines of competing priorities and limited budget and resources, not that they are satisfied with their existing state of security and identity management. In fact, this group noted that training users to protect account credentials, password management, and privilege management are among their top identity and access management challenges.

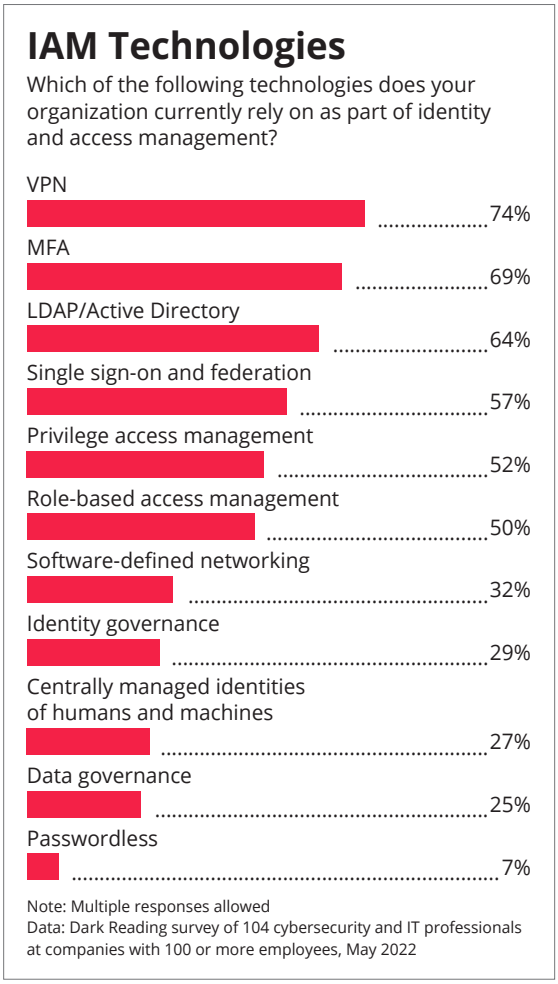
With the increased usage of cloud-based services and personal devices, organizations have to consider where services are located, who controls them, and how they are used. To understand what activities organizations are emphasizing in their current or planned zero trust environments, respondents on the zero trust journey were asked to identify three components they consider the most important to integrate with Identity Access Management (IAM) to support zero trust. The top four selections were security information and event management (43%), endpoint protection (40%), identity governance (36%), and privileged access management (32%). Endpoint protection, identity governance, and privilege access are all expected components of zero trust architectures.

The fact that organizations are prioritizing integrating their SIEM stack with IAM, highlights the role SIEM plays in effective threat detection and response. One of the biggest challenges with SIEM is to filter out false positives (alerts that don't indicate actual threats) and zoom in on issues that require some kind of action. By integrating IAM with SIEM, security teams can enhance the intelligence threat hunters are relying on as they search for that needle in the haystack.

Tools and Best Practices in Play

How organizations implement zero trust depends a lot on what tools they use. The top five technologies in use by organizations already using or considering zero trust were VPN (74%), Multifactor Authentication (69%), LDAP/Active Directory (64%), Single sign-on and federation (57%), and Privilege Access Management (52%) **(Figure 3)**.

Figure 3.



Many organizations are still relying on virtual private network (VPN) solutions to manage remote access to the enterprise, but the shift to remote work is making VPN untenable due to the massive increase in workloads and traffic.

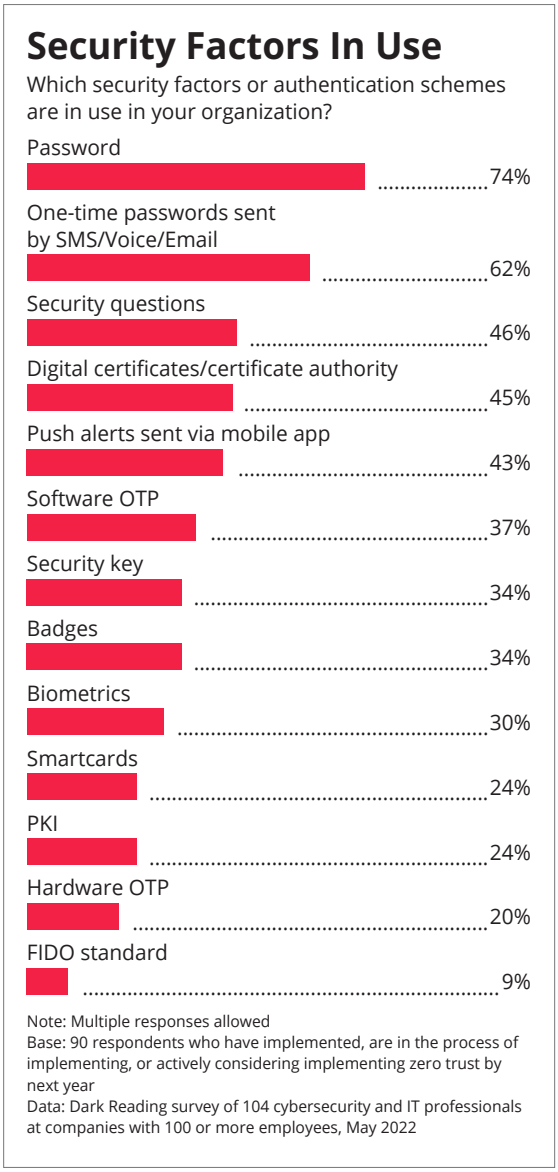
Organizations are lagging on role-based access management (50%) and identity governance (29%), suggesting that security teams are still missing some of the core elements of zero trust. Only 7% indicated they were relying on a passwordless sign-on solution.

When asked about security factors and authentication schemes currently in use in their organization, 74% reported using passwords or one-time passwords (62%) sent by SMS, voice, or email. Other top selections included security questions (46%), digital certificates or certificate authority (45%), push alerts sent via mobile app (43%) **(Figure 4)**. Only 9% selected using the FIDO standard.

When asked which specific tools and technologies respondents had already integrated with IAM, the five leading responses were endpoint protection (54%), security email gateway (52%), security information management (46%), mobile device management (40%), and privileged access management (36%) **(Figure 5)**. More notably, more than half of respondents indicated they were planning to make those integrations across the board within the next 12 months, suggesting high intent among organizations to improve how they use identity and access management within their environment.

To understand how organizations were using single sign-on and multifactor authentication technologies, respondents were asked which systems and resources had been set up or were planned for. Many of the respondents said single sign-on and multifactor authentication have been set up for internal applications (61%) **(Figure 6)**. A little less than half of the respondents said they have been set up for endpoints, such as laptops and desktops (49%), servers (48%), and databases (45%). Considering how frequently attackers target these types of systems, security teams are exposing their organizations to high risk.

Figure 4.



However, about 40% (give or take a few) of respondents appear to recognize the risk and are planning to set up single-sign or multifactor authentication for these three types of systems within the next 12 months.

While API security is an important component of zero trust architecture, less than a third of respondents indicated they have set up single sign-on and multifactor authentication for APIs (31%). There is a silver lining, though, as 46% indicated they plan to implement them for APIs within the next 12

Figure 5.

Technologies Integrated with IAM

Which tools and technologies will your organization integrate (or plan to integrate) with identity and access management?

	Already implemented today	Will be implemented in the next 6 months	Priority in the next 12 months	Priority in the next 18 months	N/A
Endpoint protection (EMM)	54%	24%	11%	5%	6%
Secure email gateway	52%	20%	15%	6%	7%
Security information and event management (SIEM)	46%	28%	16%	6%	4%
Mobile device management	40%	27%	15%	10%	8%
Privileged access management (PAM)	36%	29%	23%	8%	4%
Identity governance	36%	27%	20%	14%	3%
Dynamic authentication and authorization	31%	25%	19%	10%	15%
Data security/governance	29%	34%	18%	13%	6%
Cloud access security brokers (CASB)	24%	36%	19%	10%	11%
Security orchestration and automation (SOAR)	21%	45%	19%	6%	9%

Base: 90 respondents who have implemented, are in the process of implementing, or actively considering implementing zero trust by next year
Data: Dark Reading survey of 104 cybersecurity and IT professionals at companies with 100 or more employees, May 2022

Figure 6.

Systems for Single Sign On and MFA

Specifically to single sign on and multifactor-authentication, which systems and resources have been set up?

	Already implemented today	Will be implemented in the next 6 months	Priority in the next 12 months	Priority in the next 18 months	N/A
Internal applications	61%	15%	11%	7%	6%
Endpoints	49%	28%	12%	6%	5%
Servers	48%	25%	17%	5%	5%
Databases	45%	23%	16%	5%	11%
SaaS applications	44%	29%	13%	8%	6%
Cloud systems/servers (IaaS, PaaS)	42%	32%	11%	11%	4%
Mobile devices	36%	27%	13%	11%	13%
APIs	31%	29%	17%	11%	12%
Other types of endpoints	17%	24%	15%	10%	34%

Base: 90 respondents who have implemented, are in the process of implementing, or actively considering implementing zero trust by next year
Data: Dark Reading survey of 104 cybersecurity and IT professionals at companies with 100 or more employees, May 2022

months, which is a larger group than for other categories. This suggests security teams are aware of how important it is to secure the API against modern threats.

Level of Experience and Confidence

Experience and confidence with the zero trust framework and related tools and components can go a long way towards successful outcomes. When asked to rate their level of zero trust maturity, it was clear that zero trust implementation is very much a work in progress outside of identity. Many of the respondents rated their organizations as mature or very mature for network (45%), identity (44%), and policy (41%). Respondents said they were not mature in terms of zero trust for user behavior (37%), network (27%), and data (26%).

Other factors reveal that organizations are still in the early stages of their zero trust journey. Specifically, organizations indicated they have already implemented multifactor authentication (61%); single sign-on for employees (57%); and connecting the employee directory to cloud applications (44%). The numbers drop off for implementing MFA for external users (38%), identity governance (36%), securing access to APIs (36%), and privileged access to cloud infrastructure at (33%). The findings indicate that organizations have prioritized zero trust activities for internal applications and employees. But their goals and objectives suggest a forward momentum on the zero trust journey, as respondents indicated plans within the next 12 months to implement multifactor authentication across user groups (56%), context-based access policies (53%), data governance (50%), MFA for external users (47%), and automated provisioning/deprovisioning of external users (45%).

Balancing Challenges and Opportunities

Managing a secure environment can typically involve juggling disparate obstacles and wrangling crucial resources while keeping an eye out for ways to achieve better outcomes. Respondents on the zero trust journey were asked about critical factors when controlling and approving access to internal resources. The top four answers were the device is verified and healthy (60%), user group or privileged access user (48%), physical location/known IP or geography (43%), and the device is managed (40%).

When asked about their biggest zero trust challenges, respondents cited other high priority initiatives (55%), difficulty integrating technologies (50%), and not enough budget or resources (49%) **(Figure 7)**.

Figure 7.

The responses suggest there are two major challenges for zero trust — technical challenges around implementation, and resources. The pattern of responses echoes the answers given by the small group of respondents who said they were not implementing zero trust because of limited budget and resources and competing priorities.

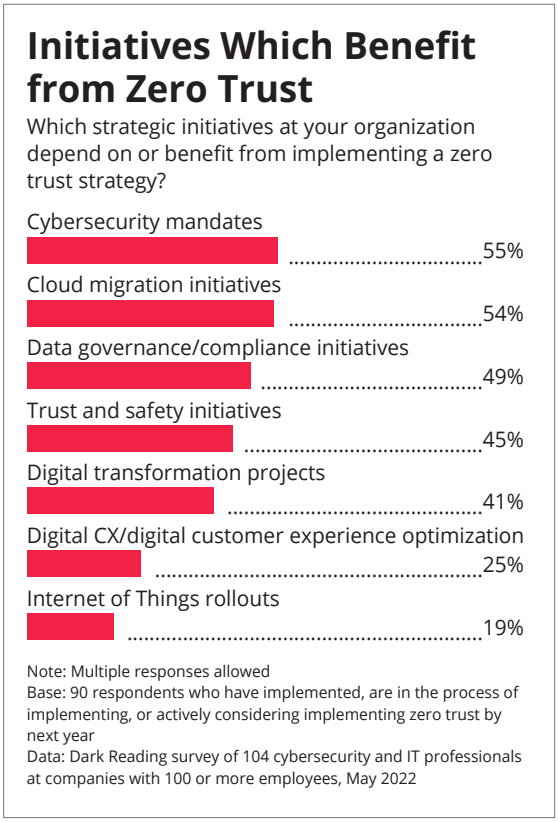
Impact on Business Areas and Strategic Objectives

Zero trust can help organizations achieve a variety of business benefits that advance business strategy and objects. Organizations must recognize that if they are targeted, they can eventually be compromised, and they need to integrate this possibility into their cyber risk management plans. Fundamentally, zero trust is an integral part of organizational risk management that can help safeguard sensitive business information and, thereby, brand reputation. To understand how zero trust may integrate into an overall IT risk management strategy, respondents were asked to rate their organization's management of risks associated with certain technologies. Most received majority rankings for good or excellent (with exception as indicated below).

- Account credentials (81%)
- Cloud platforms and infrastructure (66%)
- Cloud-based applications (65%)
- Websites and web apps (63%)
- Third-party access (56%)
- API access (55%)
- AppDev resources, e.g. code libraries, frameworks, etc. (54%)
- Social media accounts (43%)

A variety of strategic business initiatives can depend on or benefit from implementing a zero trust strategy. The majority of participants cited cybersecurity mandates (55%) and cloud migration initiatives (54%) (**Figure 8)**. Other leading responses included data governance/compliance initiatives (49%), trust and safety initiatives (45%), and digital transformation projects 41%.

Figure 8.



The new reality of a hybrid workforce and cloud-based computing can offer potential attackers with a broader attack surface. Zero trust can help organizations protect their business while adapting to the ever-changing security landscape and retaining the benefits of digital transformation.

Respondents were asked to rank a list of identity management and identity security topics to shed light on how organizations were prioritizing these topics. The top five

were understanding risk across the enterprise, managing/governing data, implementing MFA and passwordless authentication, building the "identity security" foundation for zero trust, and updating IAM for cloud and hybrid services.

We asked participants implementing, planning, or considering zero trust how it ranked among all of the organization's security initiatives for the coming year. It ranked among the top three or higher for 44% of respondents, and fell in at least the top five for 84%.

We looked at spending plans of all participants to glean deeper insight into how strategic priorities might ultimately play out. About 73% of respondents revealed their spending on information security was on track to grow this year, compared to last year. We also learned, from further questioning, that 70% of organizations were planning to devote at least 5% of their overall IT budget to credentials management, zero trust, or other identity related initiatives. About 37% of respondents reported plans to dedicate more than 10% of their IT budget.

Conclusion

IT departments can find creating layers of security and protection for sensitive data a challenge with cloud-based services, especially as more organizational work is happening remotely and on personal (non-company) devices. To remain competitive, many organizations are adjusting their business models and providing new digital experiences. They are also increasingly enabling a global hybrid workforce as recent events, such as the COVID-19 pandemic, have accelerated this transformation.

As a result, IT security teams are seeking greater control to decide what resources, data, and activity are required for the organization's security strategy. They are also looking to nail down breachers faster and better by harnessing the potential of identity access management along capturing precise data regarding the time, location, and application involved in each access request.

As a zero trust environment can enable these abilities, many organizations have already started on their journey of implementation. This reality will continue to drive IT spending priorities and use of credential access management technologies.

About NetIQ

NetIQ offers modern IGA and adaptive access to help organizations progress on their zero trust journey. NetIQ Identity and Access Management provides comprehensive workforce and customer identity solutions to enterprise scale organizations – leveraging Identity to provide secure access, effective governance, scalable automation, actionable analysis and insight across their Cloud, Mobile, & Data platforms.

NetIQ is part of CyberRes, a Micro Focus line of business.

Survey Methodology

Dark Reading conducted a survey in May 2022, on behalf of the NetIQ line of business at Micro Focus, exploring the current cybersecurity landscape and enterprises who are embracing zero trust as a strategy to proactively manage cyber risk. The final data set from this research is made up of 104 IT cybersecurity and IT professionals at organizations with 100 or more employees.

Nearly one-quarter of respondents (23%) are security or IT director or head of the department, such as fraud detection or risk management. Twenty-two percent are executive level titles such as CSO/CISO, chief of threat intelligence, CIO/CTO or VP of IT or cybersecurity, and 26% are information security department manager or staff. Rounding out other survey respondent titles are network administrator, engineer, cloud architect, security architect, and other line of business or corporate job titles. Twenty percent of respondents work at companies with 100 to 499 employees, 35% are at companies with 500 to 4,999 employees, and 45% work at companies with 5,000 or more employees. Respondents work in more than 20 industries concentrated mostly in North America.

The survey was conducted online. Respondents were recruited via email invitations containing an embedded link to the survey. The emails were sent to a select group of Informa Tech's qualified database; Informa Tech is the parent company of Dark Reading. Informa Tech was responsible for all survey design, survey administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

248-000009-001 | 05/24 | © 2024 OpenText