CYBERARK®

2022 IDENTITY SECURITY THREAT LANDSCAPE REPORT

Table of Contents

Executive Summary

The CyberArk 2022 Identity Security Threat Landscape Report represents the findings of a worldwide survey of 1,750 IT security decision makers[1], highlighting their experiences over the past year in supporting their organizations' expanding digital initiatives.

These senior security professionals overwhelmingly (79%) agree that security has taken a back seat to maintaining business operations, with organizations prioritizing IT and digital initiative investments.

These initiatives — especially those prioritizing remote/hybrid working, new digital services for customers and citizens, and increased outsourcing of remote vendors/suppliers — have created an explosion of human and machine identities, often running into the hundreds of thousands per organization.

This has driven a buildup of identity-related cybersecurity "debt": organizations are now facing the consequences of insecure digital acceleration, including greater risk exposure to ransomware threats and vulnerabilities across the software supply chain.

This report shines a spotlight on a rapidly expanding identity problem and explores perspectives on the evolving threat landscape. It also shows a direct connection between rampant cybersecurity debt and imbalanced investment decisions that emphasized digital projects over robust security measures. We believe this gap is a significant issue for organizations in 2022: identities are a prime attack vector and waiting to apply security controls after an attack is not a responsible security policy.

Did You Know?

- Credential access seen as the number one risk factor for organizations
- Machine identities now outnumber human ones in the average organization by a factor of 45x
- 64% of security leaders admit an attack on their organization originating from a compromised software supplier could not be stopped

[1] Respondents were based in the US, UK, France, Germany, Japan, Italy, Spain, Brazil, Mexico, Israel, Singapore and Australia, working for organizations with at least 500 employees across all private and public sectors (excluding consumer services). 65% represented companies of 3,000 employees or more. The majority of respondents (94%) surveyed were manager level or above. Of these, 25% were C-level executives. All respondents were interviewed online using a rigorous, multi-level screening process to ensure that only suitable candidates took part. All participants were prescreened for having experience with Identity Security before being invited to participate.

A Growing Identities Problem

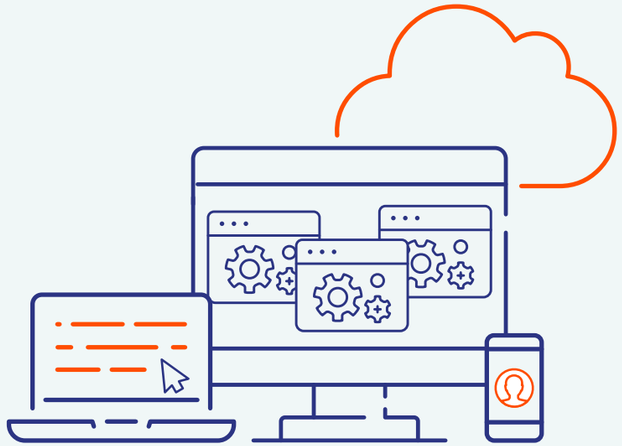
The Digital Sprint Leaves a Deluge of Uncontrolled Identities Behind.

Nearly all (99%) of organizations surveyed had fast-tracked the adoption of at least one business/IT initiative over the last 12 months. This was no surprise: digital acceleration initiatives aren't only essential for staying competitive; they're the key to an enterprise's resilience in times of volatility.

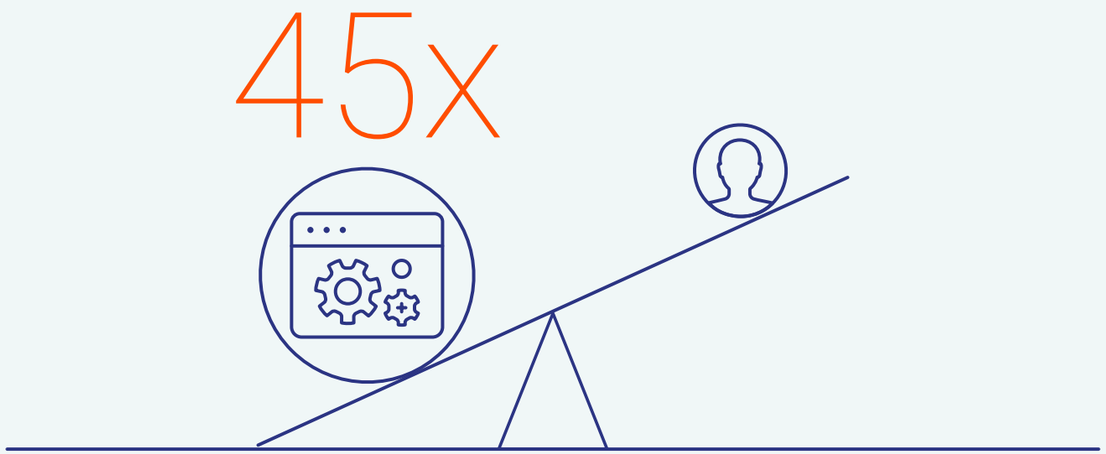
Every major IT-related initiative — from enabling hybrid work to introducing new digital services for customers or citizens — results in more digital interactions between people, applications and processes. Each connection point requires a digital identity to authenticate the human or machine involved. For instance, an individual's unique logon to Microsoft Outlook is a digital identity, as is a secret used by a DevOps tool to access code repositories or manage cloud resources.

According to survey results, the number of digital identities in organizations is already remarkably high — and will continue to grow in parallel with high-priority initiative rollouts. In a typical enterprise today:

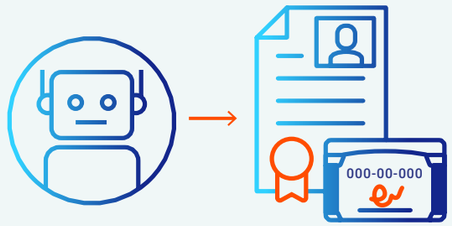
- The average staff member accesses more than 30 applications and accounts
- Machine identities outnumber human identities by a factor of 45x



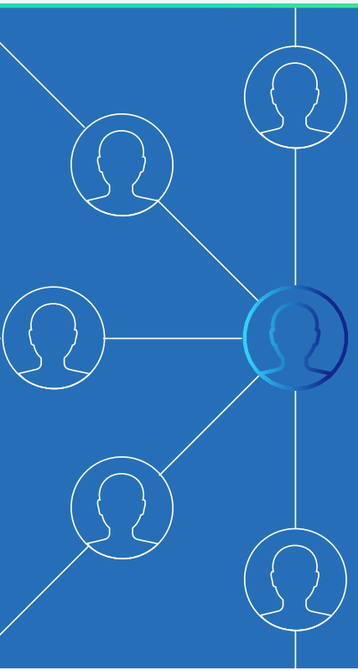
The average staff member accesses more than 30 applications and accounts



Machine identities outnumber human identities by a factor of 45x



68% of non-humans or bots have access to sensitive data and assets



52% of organizations' workforces have access to sensitive corporate data

Some identities provide direct, privileged access to sensitive data and assets, so people and machines can perform their jobs or functions. ***All identities*** can become privileged under certain conditions, based on the systems, environments, applications or data they are accessing, or the types of operations they are performing. This is why it's critical to manage and secure all identities — and why it can be difficult to do so as new ones are generated rapidly.

In most organizations, the number of people and machines with access to sensitive data is already high:

- More than half (52%) of organizations' workforces have access to sensitive corporate data on average
- 68% of non-humans or bots have access to sensitive data and assets

It takes just one compromised identity for an external or inside threat actor to start an attack chain. The acceleration of digital initiatives and resulting surge in digital identities feed into an expanding attack surface.

The 2022 Attack Surface

Cyber Attacks are a Past, Present and Future Reality. Yet Organizations Remain Unprepared.

Survey participants' organizations were, like many others, targets of cyber attacks over the past 12 months. A high percentage of respondents reported frequency of two types of attacks in particular:

- **Ransomware.** More than 70% of organizations have experienced ransomware attacks in the past year — two each on average, with healthcare organizations averaging two or more. Privilege escalation was the number one attack vector of risk for healthcare organizations.
- **Software supply chain attacks.** 71% of organizations suffered a successful software supply chain-related attack that resulted in data loss or asset compromise. Energy and utilities companies were particularly targeted: 88% experienced a successful software supply chain-related attack.

Participants identified the kinds of IT and digital initiatives that were the biggest potential source of cyber risk:

- Hybrid working (86%)
- Introducing new digital services for customers or citizens (84%)
- Increased outsourcing of remote vendors / suppliers (84%)

71% of organizations suffered a successful software supply chain-related attack that resulted in data loss or asset compromise.

MITRE | ATT&CK™

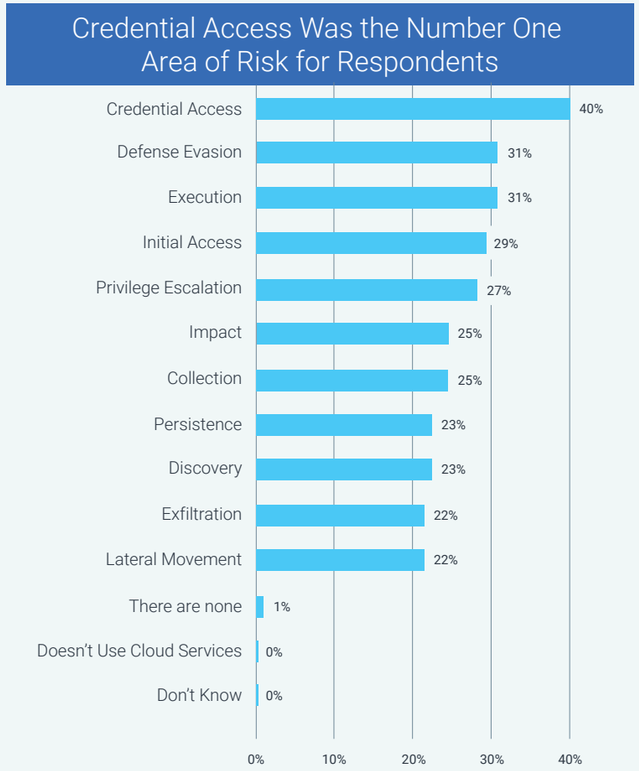
MITRE ATT&CK® Matrix for Enterprise Covering Cloud-based Techniques

MITRE ATT&CK® is a popular, open framework for implementing cybersecurity detection and response programs. The framework includes a vast knowledge base of adversarial tactics, techniques and procedures (TTPs) based on real-world observations.

Fallout from "The Great Resignation"

The recent, sudden growth in employee churn has also escalated risk posed by credential theft: two-thirds of respondents said that over the last 12 months, the accelerated rate of employee churn/turnover has caused security issues (for example, failure to deprovision access rights).

Respondents were asked about the cyber attacker tactics and techniques laid out in the MITRE ATT&CK® Matrix for Enterprise: which represented the biggest areas of risk for their organizations?



Q2. Which cyber attacker tactics and techniques (as laid out in the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques) represent the biggest areas of risk for your organization? Combination of responses ranked first, second and third.

Located throughout an organization's IT infrastructure and across applications and processes, poorly protected credentials are a primary means for attackers to gain a foothold to achieve their objectives: from stealing data or holding it hostage for financial gain to simple business disruption. No matter the goal, the first step is often gaining powerful privileged credentials that give them elevated access and the ability to move laterally to reach even more valuable data and assets.

Asked how confident they were about protecting against various credential access techniques, respondents were least confident about identifying and stopping the theft of unsecured credentials and application access tokens, as well as brute force attacks. Seventy-five percent said they do not have the ability to identify and stop a cyber attack stemming from phishing, one of the most common credential-snagging techniques.

What About Cybersecurity Insurance Against Attacks?

The survey found that, of the organizations that have a cyber insurance policy, more than three quarters (76%) had been targeted by at least one ransomware attack in the last 12 months. This suggests that cyber insurance investments may be largely reactive.

While each insurance broker's evaluation process differs, there are certain security controls that are almost always required for an organization to obtain, and keep, cyber insurance coverage.

Such mandates often involve Identity and Access Management (IAM) controls and best practices in alignment with industry standards put forth by the Center for Internet Security, CISA and others.

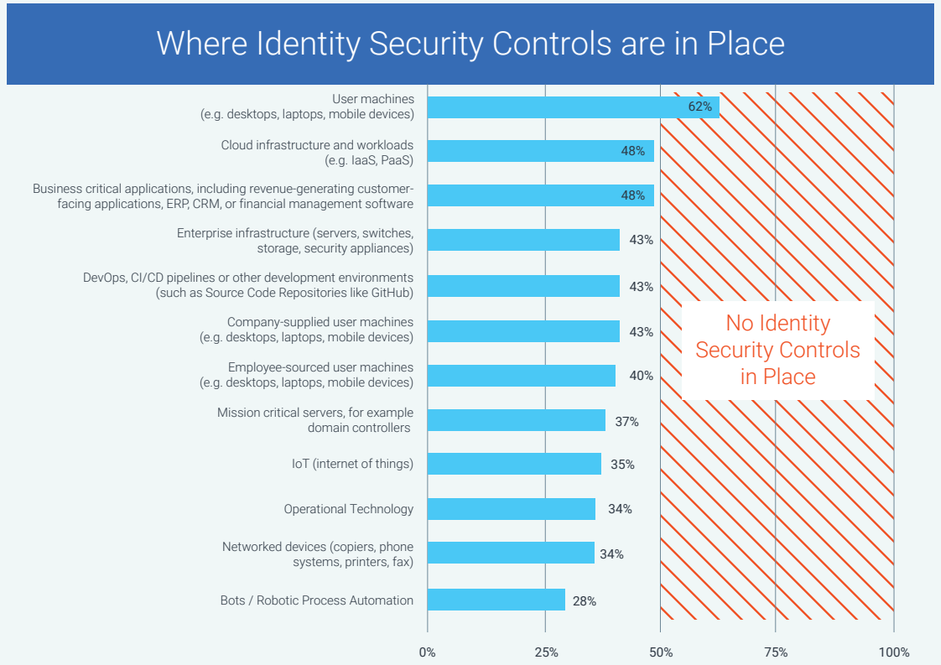
Getting Into Cybersecurity Debt

The Transformation Tradeoff of Identity-centric Cybersecurity Debt.

Security professionals agree their organizations' rapidly implemented IT and digital initiatives have come at a price — a buildup of cybersecurity debt. This debt represents the future necessary costs of addressing security vulnerabilities that accumulated — but were not "paid down"— as new systems and applications were deployed.

A significant source of this cybersecurity debt stems from failure to protect sensitive assets and data from unauthorized access as identities are created en masse and proliferate unchecked across the entire IT environment.

Participants were asked to specify where Identity Security controls — defined in the survey as privileged access management (PAM), access management, secrets management and entitlements management — existed within key areas of their IT environment. Most respondents reported these controls were absent from all but one of these key environments, driving up risk and leading to consequences.



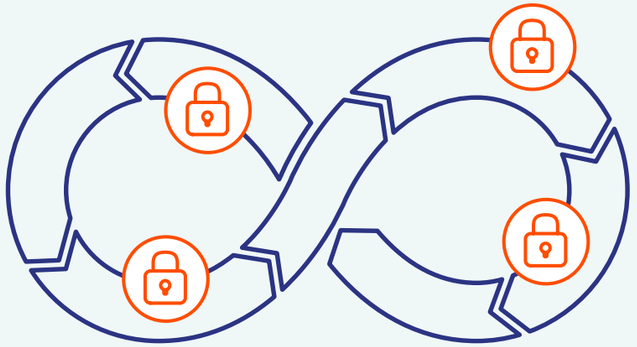
Q24. For which of the below environments and devices does your organization have Identity Security controls in place?

Fifty-two percent of respondents said identities across business-critical applications are unprotected. This is particularly concerning since more than half of workers have access to sensitive corporate data, often through these SaaS applications.

Nearly half of organizations lack Identity Security controls around cloud infrastructure and workloads. Mission-critical servers were similarly insecure. The result? Potentially thousands of misconfigured and over-permissioned identities that increase the attack surface and create cybersecurity debt.

Identity Security shortcuts are rampant in DevOps, CI/CD and other development environments, driving up more debt. Specifically:

- **87%** reported that secrets are stored in multiple places across DevOps environments.
- **Half of respondents** said application credential security is left up to developers — business users known for emphasizing speed and collaboration over security; 80% agreed that developers have more privileges than they need.
- **Only 3%** of organizations use a centralized secrets management platform to manage credentials used by applications.
- **Security concerns** have led 74% of organizations to slow down Robotic Process Automation (RPA) and bot deployments. Only 28% currently have Identity Security controls in place to secure RPA.



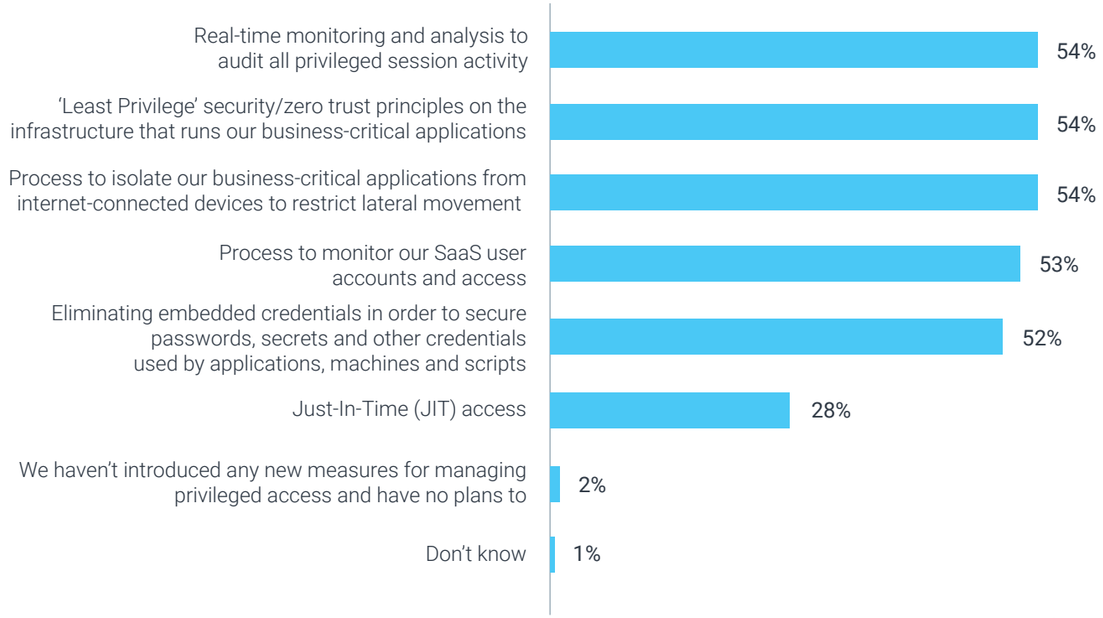
87% reported that secrets are stored in multiple places across DevOps environments

72% said that cybersecurity decisions taken during the last 12 months have introduced new areas of vulnerability to their organization.

Tackling Cybersecurity Deficiencies and Moving Forward Debt Free

Some organizations have committed to change, addressing existing cybersecurity debt and working to integrate security into new initiatives from the start. Participants identified several new measures their organizations have either already introduced, or plan to introduce, to better manage human and machine access to sensitive corporate assets.

1 New Measures for Managing Sensitive Access



Q 22. Which new measures has your organization introduced/does your organization plan to introduce to manage sensitive access for humans and non-humans?

2 Prioritizing Identity Security Controls to Enforce Zero Trust Principles

The survey showed nearly unanimous agreement that the Zero Trust cybersecurity model or philosophy of “trust nothing; verify everything” is foundational to establishing strong defense-in-depth controls and is the best path forward.

In examining organizations’ current position along the Zero Trust maturity curve, the survey found nearly 100% were doing something to establish Zero Trust principles.

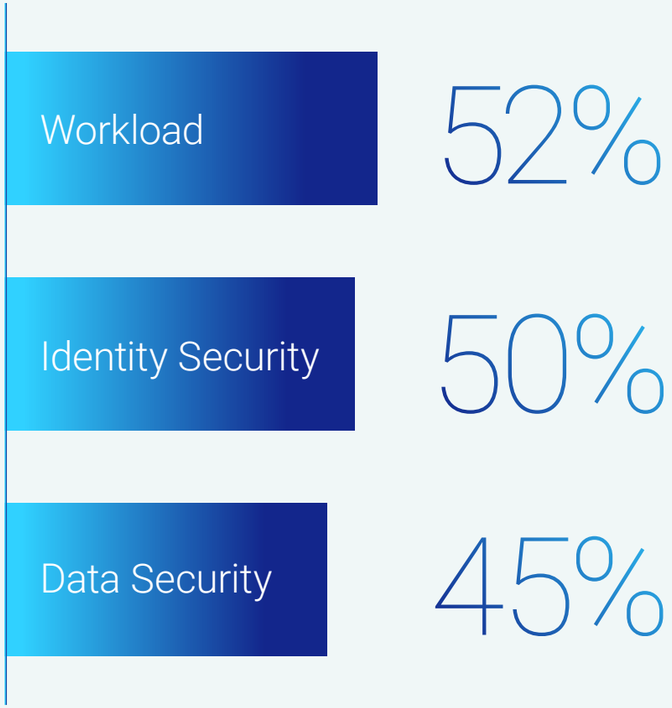
Participants were asked to name the technologies or strategic initiatives they had prioritized to pave the way for Zero Trust. Indicating progress in this area, half of respondents prioritized Identity Security tools as one of their top three initiatives, along with workload security (a top-three initiative for 52%) and data security (45%).

It was also reassuring to note that over half have either implemented or plan to implement the Zero Trust principle of “least privilege” on the infrastructure that runs their business-critical area. Least privilege controls help protect valuable systems and assets by limiting attacker movement and buying valuable time to detect and respond to an attack. The survey also found almost one-third (28%) plan to introduce just-in-time (JIT) access controls. With JIT controls, organizations can elevate human and non-human access to an application or system in order to perform a necessary task — for only the amount of time required, and no more

Best-in-class endpoint privilege managers let you implement conditional policies to block attacks involving trusted applications. For example, you could create a rule that would allow users to launch PowerShell with certain parameters. But then create another rule that would prevent other apps from launching PowerShell as a child process, thus eliminating chained exploit techniques.

Leading endpoint privilege managers support application greylisting to help you defend against unknown malware variants without impeding the operation of unknown applications that pose no known security risks. Greylist policies apply to applications that aren’t explicitly allowlisted nor denylisted. Leading solutions include pre-built policies that provide out-of-the-gate protection against ransomware and other advanced threats.

Half of respondents prioritized Identity Security tools as one of their top three Zero Trust initiatives



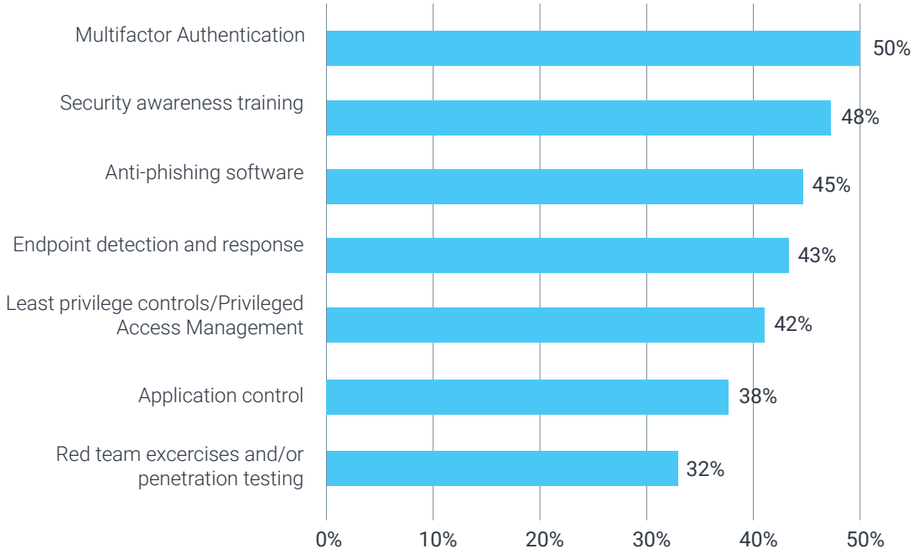
3 Embracing Defense-in-Depth Strategies

Eighty-two percent of respondents said their organizations had adopted an “assume breach” mentality. Nearly 100% said they had a defense-in-depth strategy in place to combat ransomware. As part of this, many are approaching cybersecurity debt and risk reduction efforts more holistically — not only emphasizing important technical controls but also people-centric initiatives to embed security-conscious behavior into their cultures.

As ranked by participants, the top three most effective components of a defense-in-depth strategy to combat ransomware are:

1. Multifactor authentication
2. Security awareness training
3. Anti-phishing software

4 The Most Effective Components of Ransomware Defense Strategies



Q9. What are the three most effective components of your organization's Defense-in-Depth strategy to combat ransomware? Combination of responses ranked first, second and third.

5 Raising the Bar for Software Product Security

Enhancing software supply chain security is not just a business necessity — it is a priority at the highest levels of U.S. government. A May 2021 Executive Order called for increased transparency and "more rigorous and predictable mechanisms for ensuring that products function securely, and as intended." It included guidance on requiring — among other provisions — a "software bill of materials" for all software sold to the federal government.

Akin to an ingredients list for a recipe, this bill of materials would provide greater visibility into the individual components (and associated supply chain relationships) found inside the software products organizations are deploying. This would include open-source elements that can introduce significant risk. According to survey participants, this would be a positive move: 85% say that a software bill of materials would reduce the risk of compromise in the software supply chain.

85% say that a software bill of materials would reduce the risk of compromise in the software supply chain.

Conclusion

An ever-expanding attack surface, rapidly proliferating identities and lagging cybersecurity investment collectively expose organizations to higher levels of cybersecurity risk: risk that was already heightened due to 2021's surge in ransomware threats and vulnerabilities across the software supply chain.

Attackers understand this and have been following a parallel path of innovation and investment to exploit vulnerabilities. Staying ahead of them requires an "assume breach" mentality as a starting point. The next logical step is to implement Zero Trust principles that put this defensive thinking into practice, working to minimize attackers' movements, their access to applications and systems and ultimately, their chances of success.

Zero Trust elements already exist in many organizations. For instance, some will have single sign-on (SSO) or multifactor authentication (MFA) for certain applications or services, while others have privileged access management (PAM) in place to manage and secure critical data and assets.

A complete Zero Trust practice means extending "never trust; always verify" thinking and protections across every facet of the IT environment: from business applications and distributed workforces to hybrid cloud workloads and throughout the DevOps lifecycle.

This can seem daunting — especially for those organizations grappling with significant cybersecurity debt. Creating a "pay-off plan" can help them identify high-risk areas to address first and then follow a feasible timeline for incorporating Zero Trust principles to eliminate remaining debt. With a solid identity-centric risk plan in place, organizations can effectively strengthen defenses against emerging threats while advancing key initiatives to propel their business forward.

The CyberArk 2022 Identity Security Threat Landscape Report

www.cyberark.com/ISTL22

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity — human or machine — across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow us on Twitter via @CyberArk, LinkedIn or Facebook.

U.S., 04.22 Doc: TSK-1010

CYBERARK®