THE 2019 ZERO TRUST PRIVILEGE MATURITY MODEL REPORT

Centrify®
ZERO TRUST PRIVILEGE

Centrify is redefining the legacy approach to Privileged Access Management by delivering cloud-ready Zero Trust Privilege to secure modern enterprise use cases. Centrify Zero Trust Privilege helps customers grant least privilege access based on verifying who is requesting access, the context of the request, and the risk of the access environment. By implementing least privilege access, Centrify minimizes the attack surface, improves audit and compliance visibility, and reduces risk, complexity and costs for the modern, hybrid enterprise. Over half of the Fortune 100, the world's largest financial institutions, intelligence agencies, and critical infrastructure companies, all trust Centrify to stop the leading cause of breaches – privileged credential abuse.

US +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia Pacific +61 1300 795 789
Brazil +55 11 3958 4876
Latin America +1 305 900 5354
sales@centrify.com

About this Report

The Centrify Zero Trust Privilege Maturity Model was created to help security professionals assess how developed their organization's ability is to prevent the #1 cause of breaches… privileged access abuse. This report will give you the tools to measure how well your organization can identify, protect, manage, monitor, audit, and limit privileged access. By using a maturity model for reference, this report helps organizations to assess where their implementation currently stands and where to improve it, working towards a mature level of implementation that allows the organization to maintain a state of Zero Trust Privilege, while dynamically providing necessary access to meet the operational needs of the business.

What is Zero Trust Privilege?

Zero Trust Privilege redefines legacy Privileged Access Management (PAM) for the modern enterprise IT threatscape. Organizations must discard the old model of "trust but verify" which relied on well-defined boundaries. Zero Trust mandates a "never trust, always verify, enforce least privilege" approach to privileged access, from inside or outside the network.

Zero Trust Privilege requires granting least privilege access based on verifying who is requesting access, the context of the request, and the risk of the access environment. By implementing least privilege access, organizations minimize the attack surface, improve audit and compliance visibility, and reduce risk, complexity and costs for the modern, hybrid enterprise.

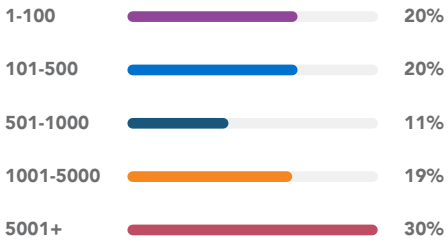
To provide context around the current state of Zero Trust Privilege in the wild, we surveyed 1,300 information security professionals to better understand what level of Zero Trust Privilege maturity is currently employed by their organization, what parts of the organization it protects, and whether the current implementation sufficiently protects against modern day attacks.

About Our Respondents

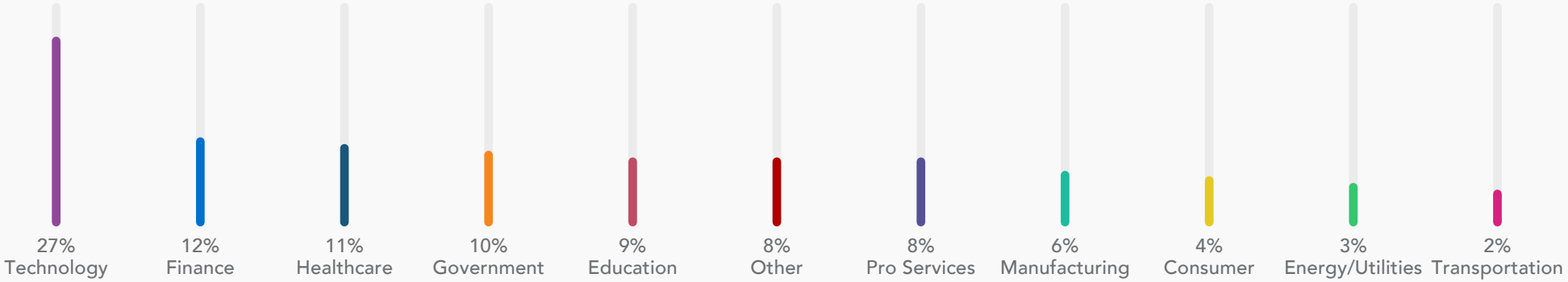
Over 1,300 organizations from the United States and Canada participated in this year's report.

Response by organization size (shown at right) provided us with a solid representation of organizations of every size. Organizations ranged from the small business (with less than 100 users) up to the enterprise (with more than 5,000 users).

The 11 industry verticals represented in this report are shown below, with significant representation from the Technology, Financial Services, and Healthcare verticals.



Breakout of Respondents by Industry



About the Contributors

David McNeely

David McNeely is Chief Strategy Officer at Centrify, where he is focused on helping customers meet the evolving security needs of the modern enterprise, while contributing to the strategic vision of the company's product portfolio. McNeely has been with Centrify for over 14 years, contributing to the company's high growth via product innovation. Prior to joining Centrify, he served in a variety of product roles at AOL and Netscape Communications (acquired by AOL).

Nick Cavalancia

Nick Cavalancia is a cyber-security expert with over 25 years of enterprise IT and security experience. He regularly blogs, writes, and speaks on a wide range of cyber security issues, helping organizations, IT professionals, Managed Service Providers, and technology vendors understand the state of both insider and external threats, and how to build and execute a strategy to minimize risk.

Centrify

Centrify is redefining the legacy approach to Privileged Access Management by delivering cloud-ready Zero Trust Privilege to secure modern enterprise use cases. Zero Trust Privilege mandates a "never trust, always verify, enforce least privilege" approach. Centrify Zero Trust Privilege helps customers grant least privilege access based on verifying who is requesting access, the context of the request, and the risk of the access environment.

The Zero Trust Privilege Maturity Model

The Zero Trust Privilege Maturity Model

The Centrify Zero Trust Privilege Maturity Model helps organizations better understand and define their ability to discover, protect, secure, manage, and provide privileged access. In addition, this model can be used to help mature existing security implementations towards one that provides the greatest level of protection of identity, privileged access, and its use.

Nonexistent

The organization has no technology in place to define, manage, verify, and monitor privileged access, with the protection of privileged access accounts limited to static passwords stored in Microsoft Office documents.

Vault-Centric

The organization has password vault technology in place to protect shared, alternate admin and local admin accounts, as well as secrets. Secure Admin Environments (SAEs), as well as privileged session management (PSM) may also be in place. They may also have processes in place to support just-in-time access to these privileged accounts.

Identity-Centric

In addition to the use of a vault, Secure Admin Environments (SAEs), and privileged session management (PSM), the organization has limited access to shared accounts, and uses identity consolidation through centralized identity management and authentication with their Enterprise Directory to reduce the threat surface and ease usability. They have implemented least privilege through temporary assignment of access and privilege elevation, and leverage multi-factor authentication (MFA).

Mature

The organization has sufficient technology in place to address both Vault- and Identity-Centric levels, while hardening the environment via a number of initiatives, including centralized management of service and app accounts, enforcing host-based session, file and process auditing, feeding privilege audit logs to your Security Event Information Management (SIEM) solution, and machine learning-based behavior monitoring of privileged account usage to detect threats.

The Zero Trust Privilege Maturity Model

A Detailed Look at the 4 Levels

The following pages provide specifics to both help identify your organization's current level of Zero Trust Privilege maturity, as well as to better understand the differences in how more mature levels operate.

	 Nonexistent	 Vault-Centric	 Identity-Centric	 Mature
Goals & Objectives	None	Discovery of all machines and privileged accounts. Management of and access to admin accounts is accomplished via a secure, centralized, password vault. Admin sessions go through a Server Gateway with session recording.	Consolidate identities, focusing on implementing Least Access and Privilege principles. Roles for computers, accounts, and operations are established, with privilege requests processed centrally though integrated workflow with IT Systems Management (ITSM) or Identity Governance and Administration (IGA). Multi-factor authentication (MFA) is a requirement.	A focus on hardening the environment and establishing higher levels of assurance around privileged requests is key. Integration with SIEM and use of host-based auditing is established to ensure compliance. Management expands to include application and service accounts.
Identities	Shared root accounts are used for privileged access.	The organization uses a checkout model to leverage shared accounts, alternate admin accounts, local admin accounts, and digital authentication credentials (secrets).	Because of identity consolidation, enterprise directory individual and alternate admin accounts are primarily used, with a limited use of shared and local accounts. At this level, machine identities are also established.	In addition to the consolidation of both individual and admin accounts, centralized management of service accounts and application accounts is included.

CONTINUED ON NEXT PAGE ›

The Zero Trust Privilege Maturity Model

A Detailed Look at the 4 Levels

	Nonexistent	Vault-Centric	Identity-Centric	Mature
Credential Management	Shared static passwords are maintained on a spreadsheet or word document.	A secure password or Secure Shell (SSH) key vault with credential rotation is used. Some degree of policies is in place to track the combination of requesting user, admin account, and target server.	Directory-based authentication via short-lived, federated credentials (such as Kerberos, SSH certs, Private Key Infrastructure (PKI) certs, and OAuth tokens) is used.	At this level, management of credentials includes auto-managed machine PKI certificates to identify machines.
Multi-Factor Authentication (MFA)	None	Access to the vault requires MFA at National Institute of Standards and Technology (NIST) authentication assurance level 2.	At login and at privilege elevation, MFA is to be used at NIST authentication assurance level 2 enforced by each target server.	Use of MFA should also include machine learning-based adaptive MFA. Sensitive environments should target NIST authentication assurance level 3 for all MFA.
Secure Admin Environment	None. Server access is accomplished directly from local workstations.	Distributed jump hosts or Privileged Admin Workstations (PAW) facilitate access to servers which serve as "clean source" for admin access.	Additionally, 3rd party access is established via Federation. Any remote access is provided by secured web-based remote access without requiring network or VPN access.	Methods used in both Vault-Centric and Identity-Centric levels are used here.
Session Monitoring & Auditing	None	Gateway-based session recording is used to monitor sessions and provide auditing detail.	Session watch and terminate is provided for supervised or "4 eyes" access to sensitive systems.	Host-based session recording is used in conjunction with file and process monitoring. Session auditing streams are integrated with SIEM platforms.

CONTINUED ON NEXT PAGE ›

The Zero Trust Privilege Maturity Model

A Detailed Look at the 4 Levels

	 Nonexistent	 Vault-Centric	 Identity-Centric	 Mature
Workflow	None.	Privileged access follows simple request and approval workflows to provide notification and accountability.	Delegated request and approvals are integrated with IT Service Management and/or Identity Governance solutions for access as well as privilege elevation.	N/A
Least Privilege	The root admin account is the only level of administrative granularity.	Root admin and/or specific-use admin accounts are used via the vault.	Establish privilege elevation with roles and rights.	Fine-grained roles. Role mining and analysis.
Least Access	All servers are accessible by the root admin account.	N/A	Define server "zones" based on management groups or computer role to further limit which accounts can access which servers. Access is granted to groups of servers based on role assignments or based on workflow requests.	Access is only granted based on a workflow request.

CONTINUED ON NEXT PAGE ›

The Zero Trust Privilege Maturity Model

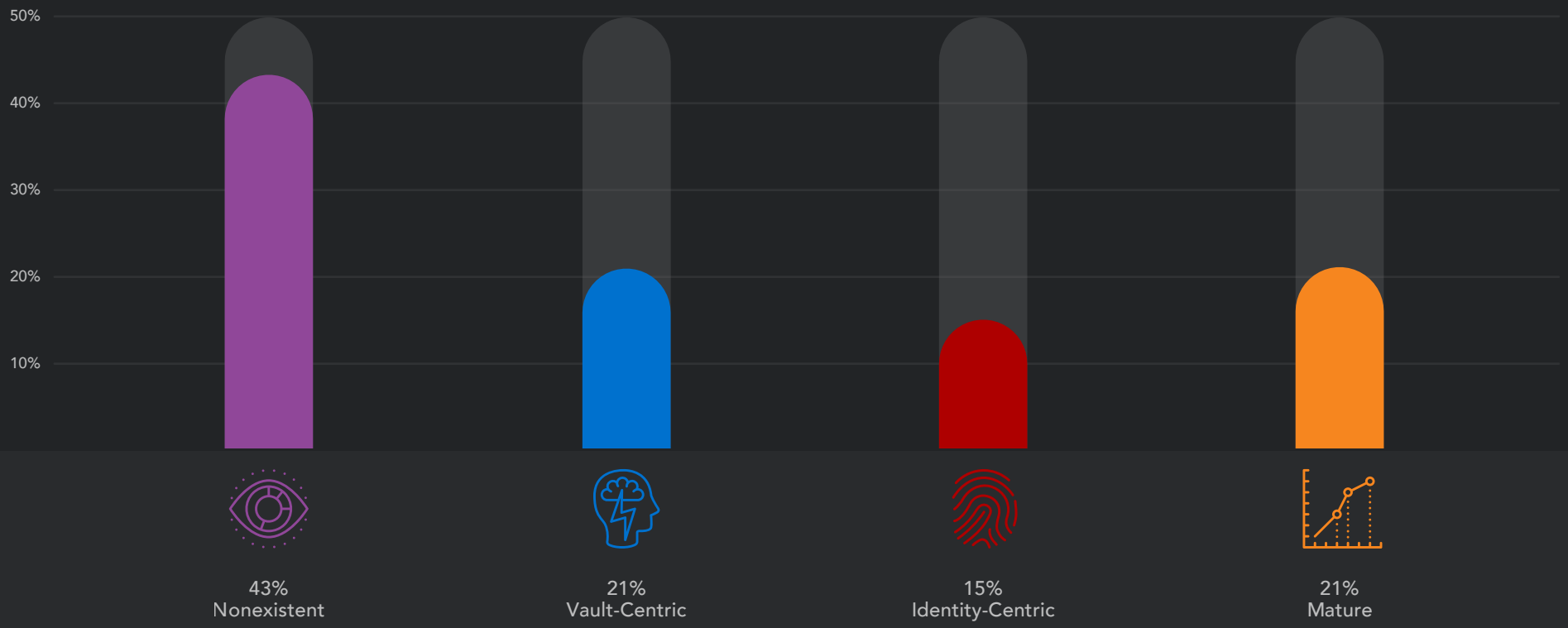
A Detailed Look at the 4 Levels

	 Nonexistent	 Vault-Centric	 Identity-Centric	 Mature
Reporting	Other than native auditing data, no reporting exists.	The vault should provide basic reporting such as "Who has access to vaulted accounts?" and "Who accessed what?". Audit logs from individual hosts may require correlation with the vault logs to determine the exact user performing activities on the host.	Improved reporting should include role usage, who is authorized for what, as well as reporting around privileged account use without requiring log correlation with the vault.	Reporting should dive into privileged user activity as captured by each host with identity of the user clearly visible without requiring any log correlation. Attestation should also be possible via integration with IGA solutions.
Security Configuration Management	If existing at all, limited scope local policies on each machine are configured.	N/A	N/A	Centralized management exists with local enforcement for system configuration (e.g., local account control, local group memberships, local SUDOer, SSHD config, firewall policies, etc.).

The Zero Trust Privilege Maturity Model

Benchmarking Implementation Maturity

The majority of organizations have not yet implemented a Zero Trust Privilege strategy, with 43% of organizations rated as Nonexistent. Smaller organizations made up the majority of those in the Nonexistent maturity level, with the mid-market owning the majority of Vault-Centric, and larger enterprises dominating both Identity-Centric and Mature levels of implementation.

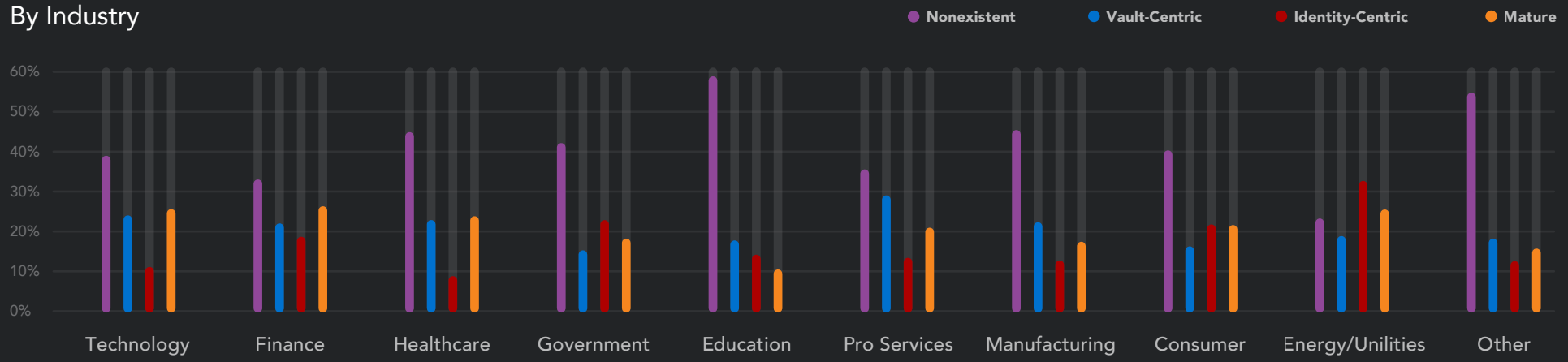


The Zero Trust Privilege Maturity Model

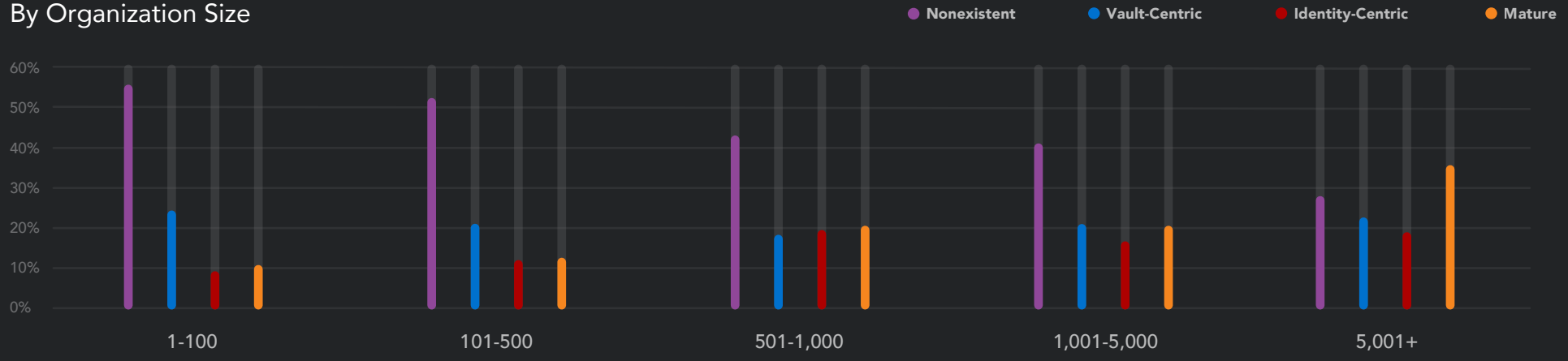
Zero Trust Privilege Maturity by Demographic

We've further broken down implementation maturity by both industry and organization size below. Here you can compare the maturity of Zero Trust Privilege implementations in organizations similar to yours. Industries with well-known critical data sets, such as Technology, Financial Services, Healthcare, and Energy have some of the highest instances of Mature implementations. And as maturity increases, we found a general following of the overall average with the majority of organizations at Nonexistent, a lower percentage of organizations at Vault- and Identity-Centric levels, and then a relative increase in the percentage of organizations with a Mature Zero Trust Privilege implementation.

By Industry



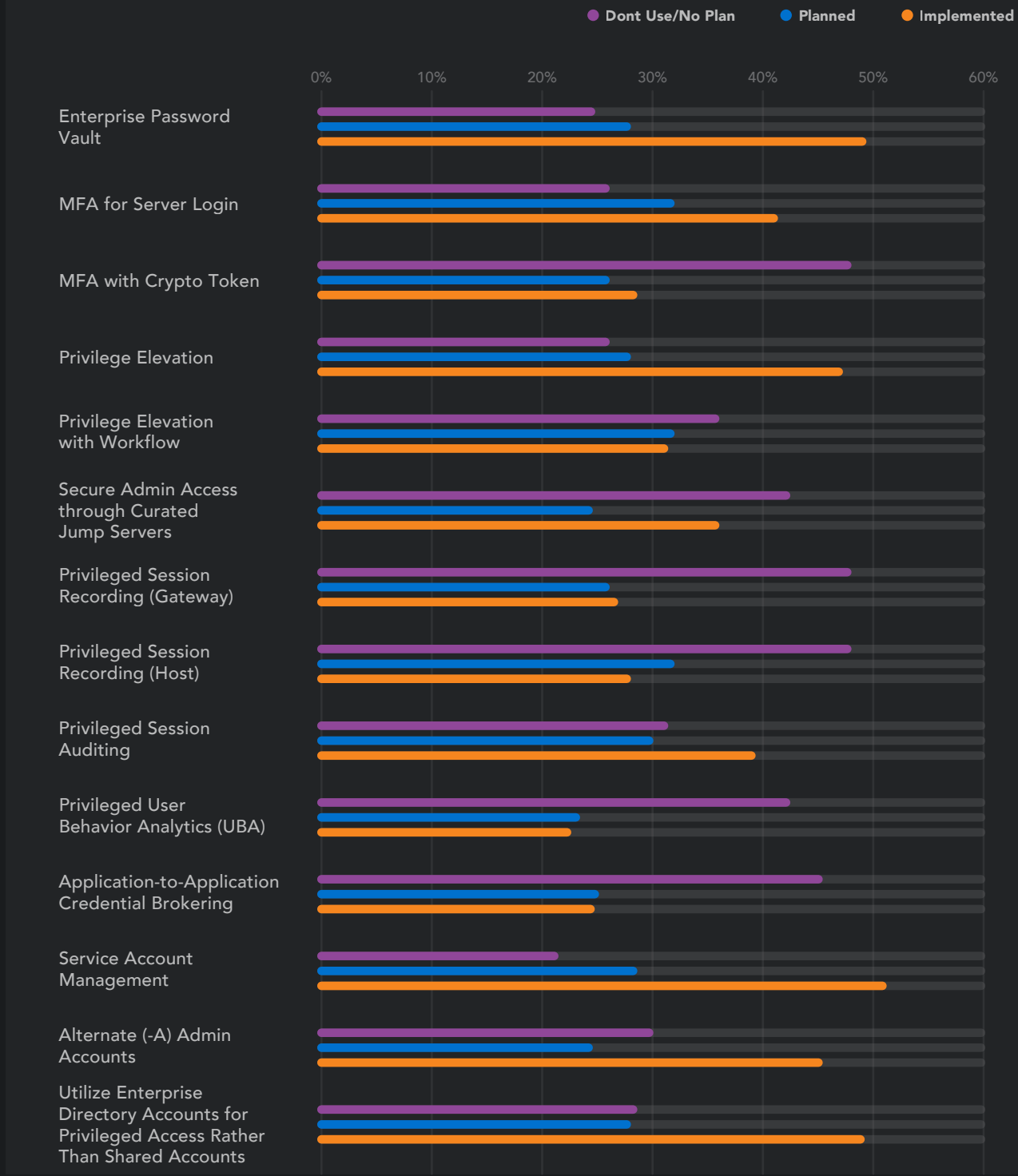
By Organization Size



The Zero Trust Privilege Maturity Model

Security Technologies, Methods, and Policies in Place

The majority of organizations generally rely on some type of password vault solution, multi-factor authentication, privilege elevation, service account management, alternate admin accounts, and enterprise directory accounts as part of their Zero Trust Privilege implementation. We were surprised to see that Privileged User Behavior Analytics (UBA) and Application-to-Application Credential Brokering are still emerging technologies, despite their critical importance in protecting new attack surfaces, such as DevOps. The use of all the solutions and technologies listed here are necessary to mature your implementation of Zero Trust Privilege.

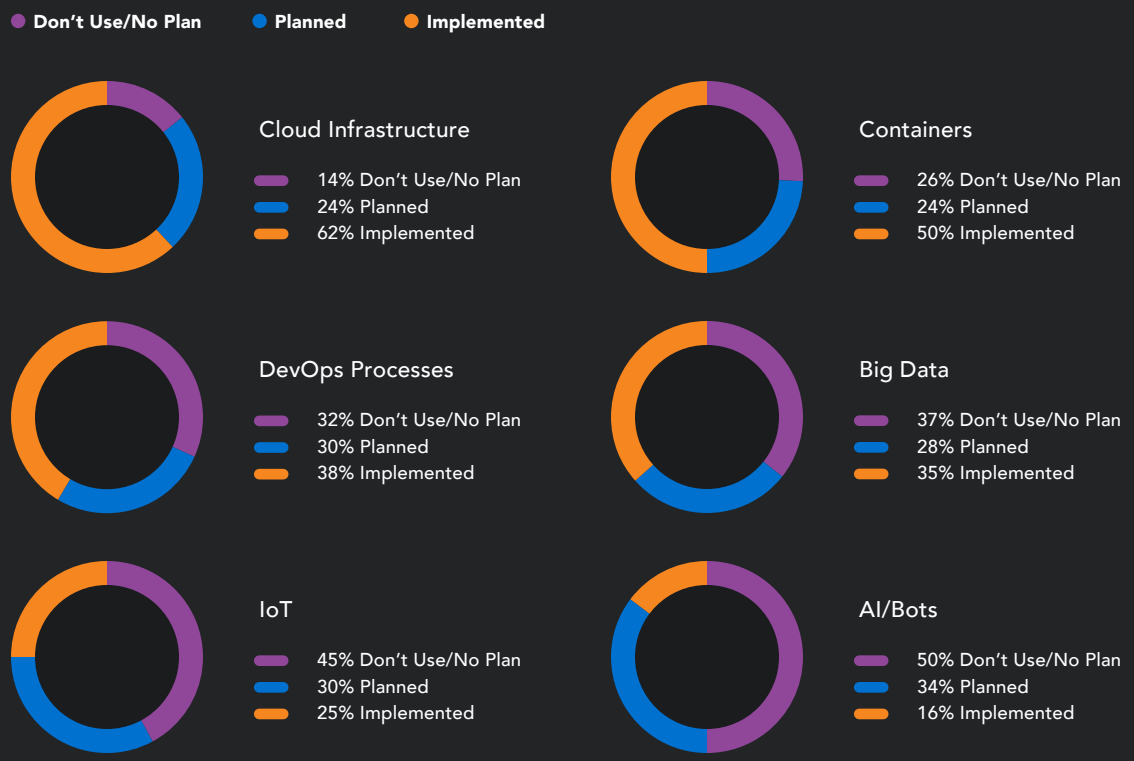


The Zero Trust Privilege Maturity Model

Technologies at Risk

As organizations begin to embrace new technologies to transform the way they do business, ensuring security equal to that of an on-premises environment becomes a challenge. We asked which transformational technologies organizations are using or planning on using. With at least half of all organizations surveyed either using or planning to use every technology here, the lack of inclusion of these technologies in a Zero Trust Privilege implementation by slightly more than half of all organizations puts the organization and its data at risk.

Usage or Plans for Transformational Technologies



Are these technologies included in your Zero Trust Privilege strategy?

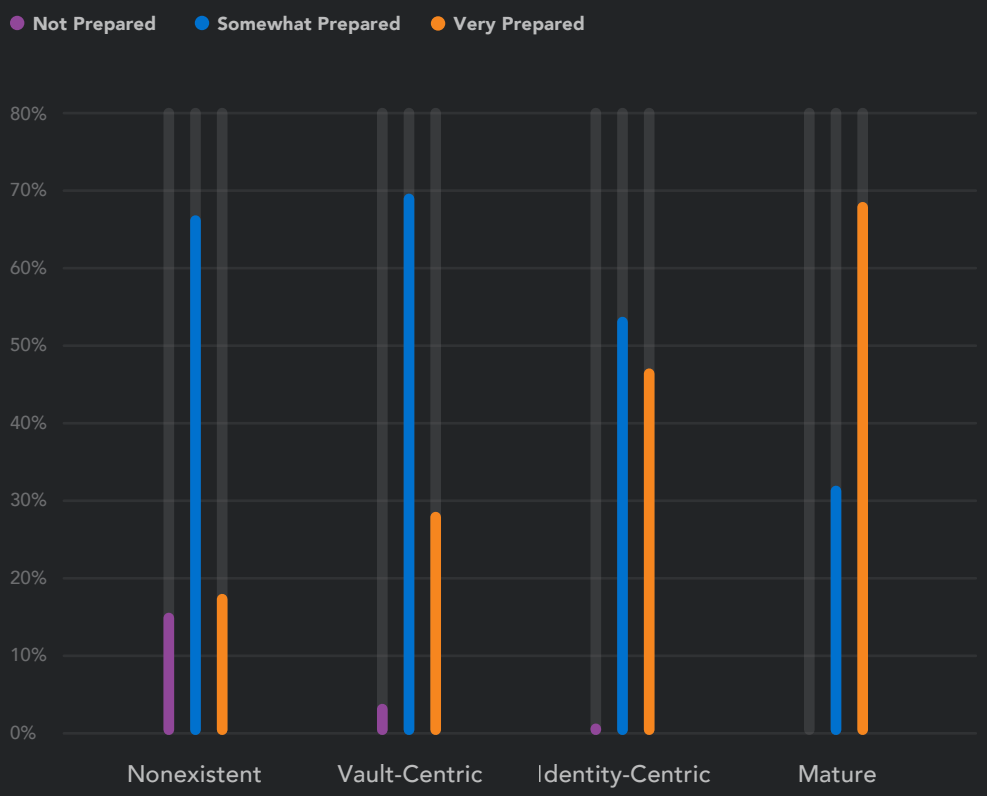
According to our respondents, 51% of organizations do not protect transformational technologies with Zero Trust Privilege, leaving these initiatives susceptible to attack.

The Zero Trust Privilege Maturity Model

Attack Readiness - External Threats Involving the Use of Privileged Credentials

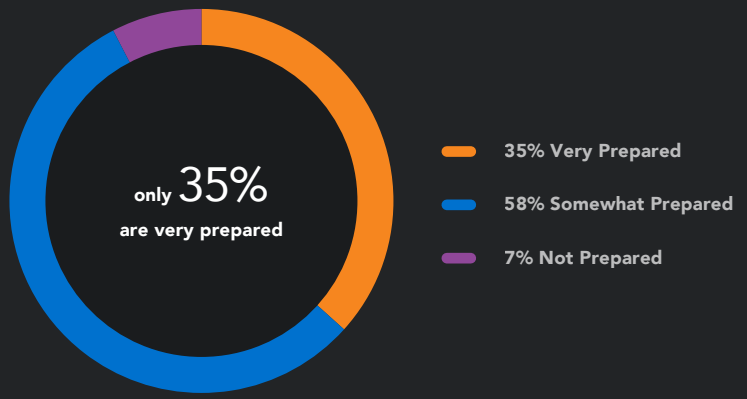
With 80% of data breaches connected to compromised privileged credentials[1], it makes sense to understand how prepared organizations are against such a threat. So, we asked, "How prepared is your organization against external threats involving the use of privileged credentials?" As shown below, the majority of organizations feel prepared to varying degrees, with the feeling of preparedness increasing as the maturity level increases.

Preparedness by Maturity Level



Breakout of organizations preparedness for an external threat that uses privileged credentials.

According to our respondents, only 35% of organizations are very prepared for an external threat. The remaining organizations have elevated levels of risk when dealing with this threat.



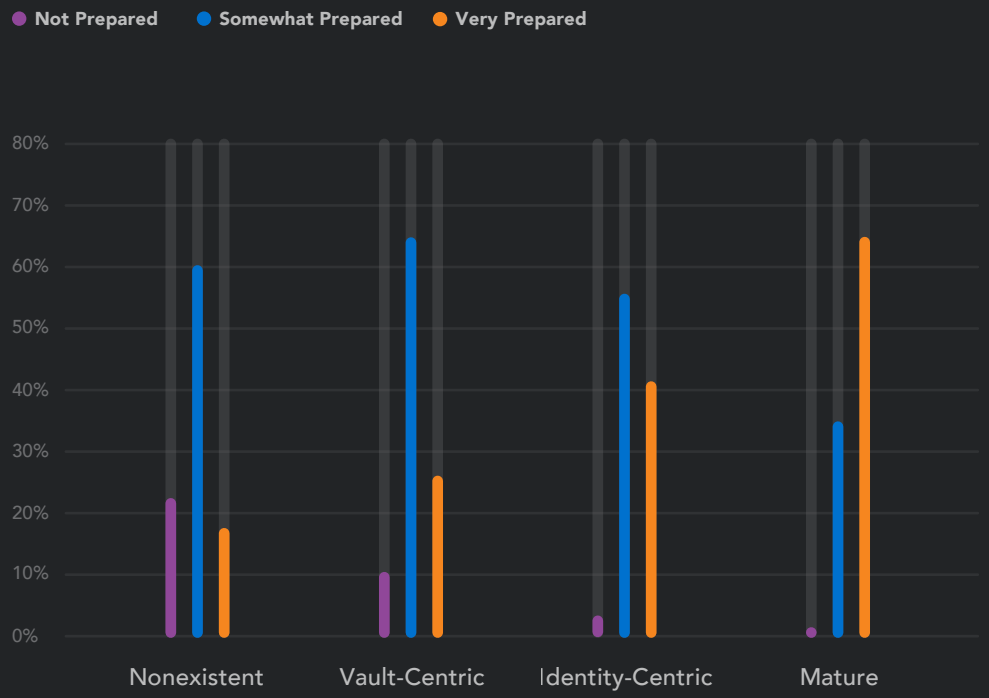
[1]Forrester, Forrester Wave: Privileged Identity Management (2018)

The Zero Trust Privilege Maturity Model

Attack Readiness - Insider Threats Involving the Use of Privileged Credentials

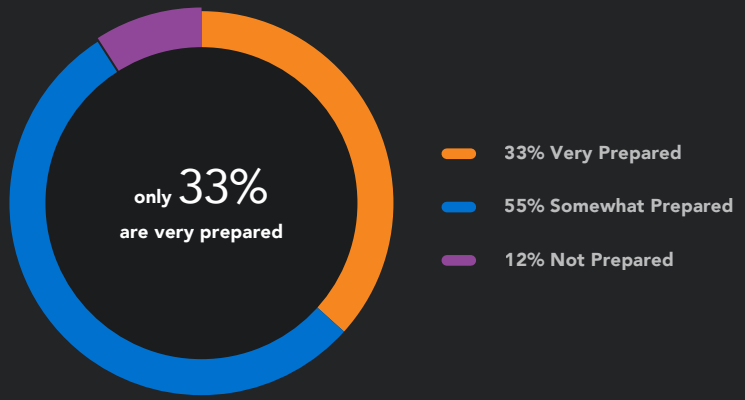
Insiders make up the balance (28%) of threat actors[1], requiring a measured focus on insider misuse of privileged credentials. We asked, "How prepared is your organization against internal threats involving the use of privileged credentials?" While a slightly larger portion of organizations feel unprepared for insider threats than that of external threats, we see the same climbing levels of confidence as the maturity level increases. The challenge with Insider Threats is that, without workflow-integrated privileged elevation and privileged user behavior analytics – technologies normally found within Identity-Centric and Mature implementations, Vault-Centric organizations that believe themselves to be prepared may not have sufficient visibility into user activity to identify threatening actions.

Preparedness by Maturity Level



Breakout of organizations' preparedness for an insider threat that uses privileged credentials.

With only one-third of organizations truly prepared for an insider threat, two-thirds are uncertain as to how well they will address an insider threat.



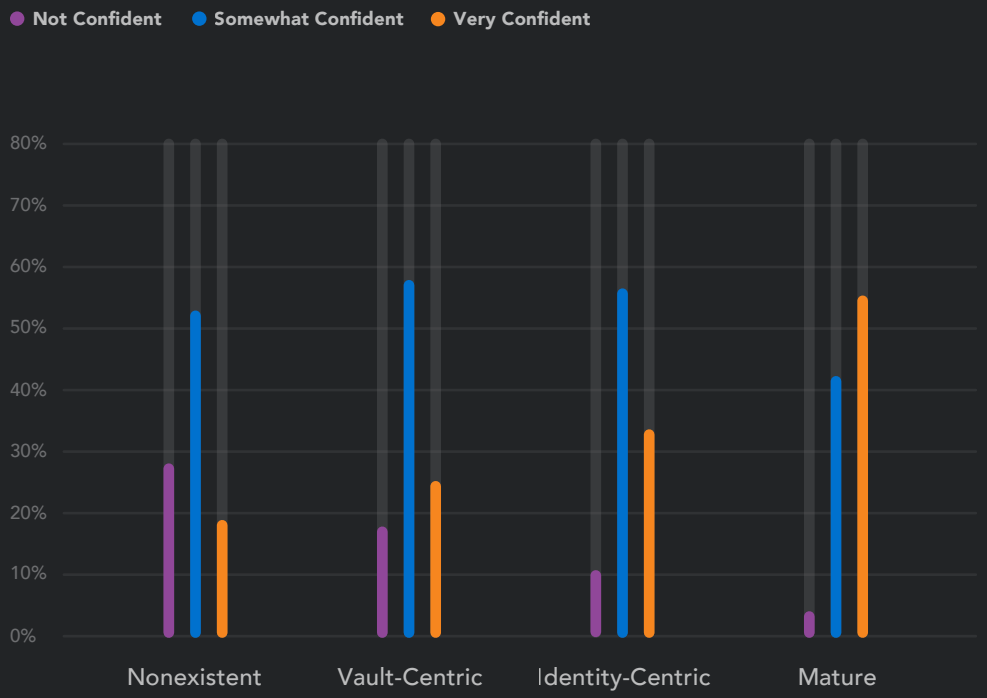
[1]Verizon, Data Breach Investigations Report (2018)

The Zero Trust Privilege Maturity Model

Attack Readiness - User Working Around Controls

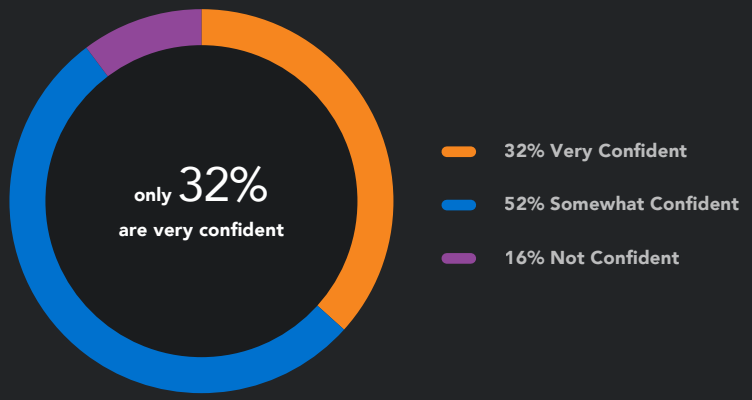
Security can often add layers of complexity to the user experience, causing users to simply find alternate ways to work around the controls, putting the organization at risk. We asked, "How confident are you that users are unable to work around your controls?" Of the three Attack Readiness questions we asked, this one had the largest % of uncertain organizations. As shown below at left, maturity level has the least amount of influence on the growth in confidence when compared to readiness for either external or insider attacks. Regardless of maturity level, material portions of organizations remain only somewhat confident or not confident at all.

Confidence by Maturity Level



Breakout of organizations confidence around users inability to work around security controls.

Slightly less than one-third of organizations are fully confident users are unable to work around their security controls. The remainder are not able to fully guarantee users aren't working against the principles of Zero Trust Privilege.



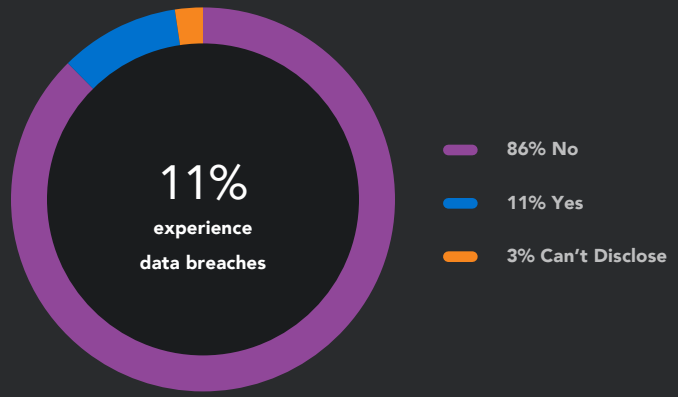
The Zero Trust Privilege Maturity Model

Putting the Model to the Test – Data Breaches Involving Privileged Credentials

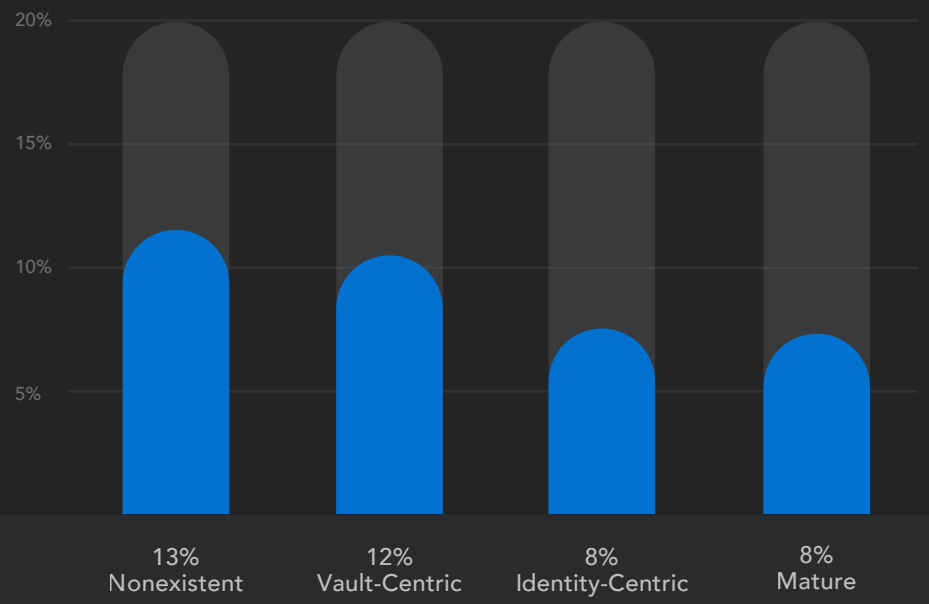
Of our respondents, 11% of organizations surveyed have experienced a data breach in the last 24 months. The largest hit based on size of organization were midsize businesses (501-1,000) and large enterprise (5,001+) at 10% and 11% respectively. Professional Services, Technology, Consumer/Retail, and Energy & Utilities topped the list by industry vertical, each with a minimum of 10%.

We found that organizations at every level of Zero Trust Privilege maturity experienced data breaches. When digging into the data, we uncovered that as an organization's level of Zero Trust Privilege maturity increased, the lower the percentage that experienced one or more data breaches involving privileged credentials in the last 24 months.

% of organizations experiencing a data breach involving privileged credentials in the last 24 months



% of breached organizations at each maturity level



Key Action Items

The goal for every organization is to adopt Identity-Centric and Mature levels of Zero Trust Privilege best practices described above. To minimize threats – both external and internal – privileged access needs to go beyond the fundamental host-enforced model and look to encompass network- and gateway-based privileged access that addresses every means by which the organization leverages privileged credentials. The following action items – in conjunction with the maturity model details provided in this report – will help evaluate your current state of security, and move your organization towards a higher level of Zero Trust Privilege.

Take Inventory of Your Attack Surfaces

You can't protect what you don't know about. So, the first step is to understand where privilege is used within your environment. Start with the obvious on-premises privileged accounts, but also include service accounts and their credentials, privileged accounts in the cloud, on Infrastructure-as-a-Service (IaaS) hosted systems, and access keys. Then consider (as is appropriate) any privileged accounts used as part of your DevOps initiatives, Big Data, Containers, and IoT.

Assess Your Security Technologies

It's nearly impossible to implement any Zero Trust Privilege maturity level without the assistance of security technologies. Having a clear understanding of which technologies are implemented within your organization is a key starting point. Keep in mind that this report mentions several similar technologies that are implemented differently to achieve increasing levels of security.

Key Action Items

Assess Your Security Processes

The processes by which you grant, monitor, manage, and remove privileged access should also be examined. There are a number of questions you can use to scrutinize the current state of security processes. Some examples include:

- Who decides who can access your servers or privileged accounts?
- Do you have disparate processes for different privileged systems? For example, Windows vs. UNIX/Linux?
- What process do you follow to give someone access? To monitor or remove that access?
- Who manages the user accounts used to access privileged accounts and systems?
- What process do you follow to validate their identity?
- Is this process performed at NIST 800-63 Identity Assurance Level 2? Level 3?
- What process do you use to handle lost MFA credentials or forgotten passwords?
- Who monitors the effectiveness of your processes/controls?
- What process do you follow when you detect abnormal/malicious activity?
- Who reviews the audit logs or watches the recorded sessions to detect potential threats?

Expand to Cover the Breadth of Your Attack Surface

With an average of 34% of organizations either planning to use or having implemented transitional technologies, it's surprising to see that slightly more than half have no plans to including those technologies within the context of Zero Trust Privilege. This only expands your attack surface. To properly reduce the threat potential, Zero Trust Privilege technologies and best practices need to be extended to protect the entirety of your organization's environment.

Identify Your Maturity Level & Plan to Improve

Using the guidelines in this report on pages 8-11, ascertain the level of maturity that best represents your organization. Keep in mind that your organization may be more mature in one aspect of the model and less mature in another, making it difficult to place your organization firmly in one level of the model.

Key Action Items

Focus on the Goal of Zero Trust Privilege

The closer you get to Zero Trust – the state at which every access request made requires intelligent scrutiny around granting least privilege access based on verifying who is requesting access, the context of the request, and the risk of the access environment, with zero access allowed by default– the more mature your implementation will be. Rather than blindly looking to implement a list of technology solutions that exist within this report, the goal is to look for technologies that will specifically advance the state of Zero Trust. As the survey indicated, the higher your Zero Trust Privilege maturity, the more confident you are protected from external and insider threats and that your security controls are not being subverted. That confidence leads to more agility to transform your business for a new digital generation.

Start Your Path to Zero Trust Privilege

Every organization desires to reduce the risk of privilege misuse by both internal and external threat actors. The increasing use of Zero Trust Privilege principles and technologies can vastly improve visibility into where privilege is utilized, when and how it's used, and when it's being abused. It starts with tightening access to, and the use of, privileged accounts using a password vault – the basis for a Vault-Centric level of maturity.

But in a Zero Trust world, a password vault alone isn't enough. Mature organizations feel more confident in their ability to address both internal and external threats over Vault-Centric organizations by a factor of nearly 2.5 times. Mature organizations also enjoy a similar increase in confidence over Vault-Centric organizations that their controls are not being subverted. These increases demonstrate that legacy Privileged Access Management is not enough for the modern threatscape with deperimiterized networks. In short, organizations desiring to ensure the security of privileged accounts and the data they provide access to, need to mature their implementation of Zero Trust Privilege.

As organizations transform their business, they open new attack surfaces. The inclusion of these environments (cloud, big data, DevOps, IoT, etc.) into a Zero Trust Privilege strategy in the same way as they do their on-premises resources significantly decreases the likelihood of privilege misuse enterprise-wide.

We no longer live in a world where privileged access can simply be allowed; organizations need to grant least privilege access based on verifying who is requesting access, the context of the request, and the risk of the access environment. This "never trust, always verify" approach taken by Zero Trust Privilege implementations provides the greatest levels of security. By striving to achieve a Mature level of implementation, organizations can work to ensure access is appropriate, sanctioned, compliant, and secure.

US +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia Pacific +61 1300 795 789
Brazil +55 11 3958 4876
Latin America +1 305 900 5354
sales@centrify.com