ManageEngine

Enterprise Password & Key Management

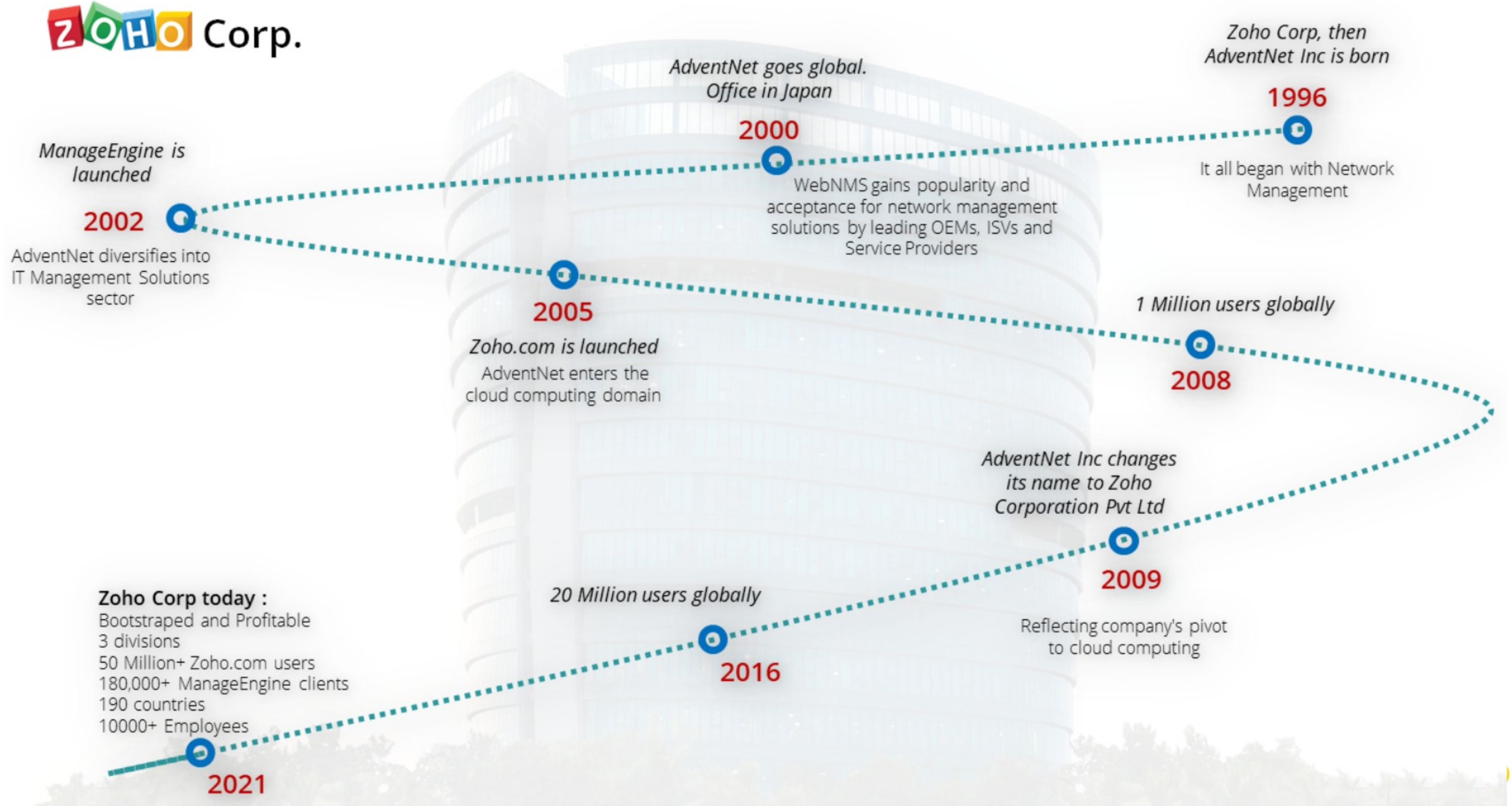
- Missing element in the Access Management Strategy for NFP's

Nirmal Nathan,
ManageEngine Solution Consultant

ZOHO Corp.
25 Years of Impact

ManageEngine
a division of Zoho Corp.

ZOHO Corp.



Zoho Corp, then AdventNet Inc is born

1996

It all began with Network Management

AdventNet goes global. Office in Japan

2000

WebNMS gains popularity and acceptance for network management solutions by leading OEMs, ISVs and Service Providers

ManageEngine is launched

2002

AdventNet diversifies into IT Management Solutions sector

2005

Zoho.com is launched

AdventNet enters the cloud computing domain

1 Million users globally

2008

AdventNet Inc changes its name to Zoho Corporation Pvt Ltd

2009

Reflecting company's pivot to cloud computing

20 Million users globally

2016

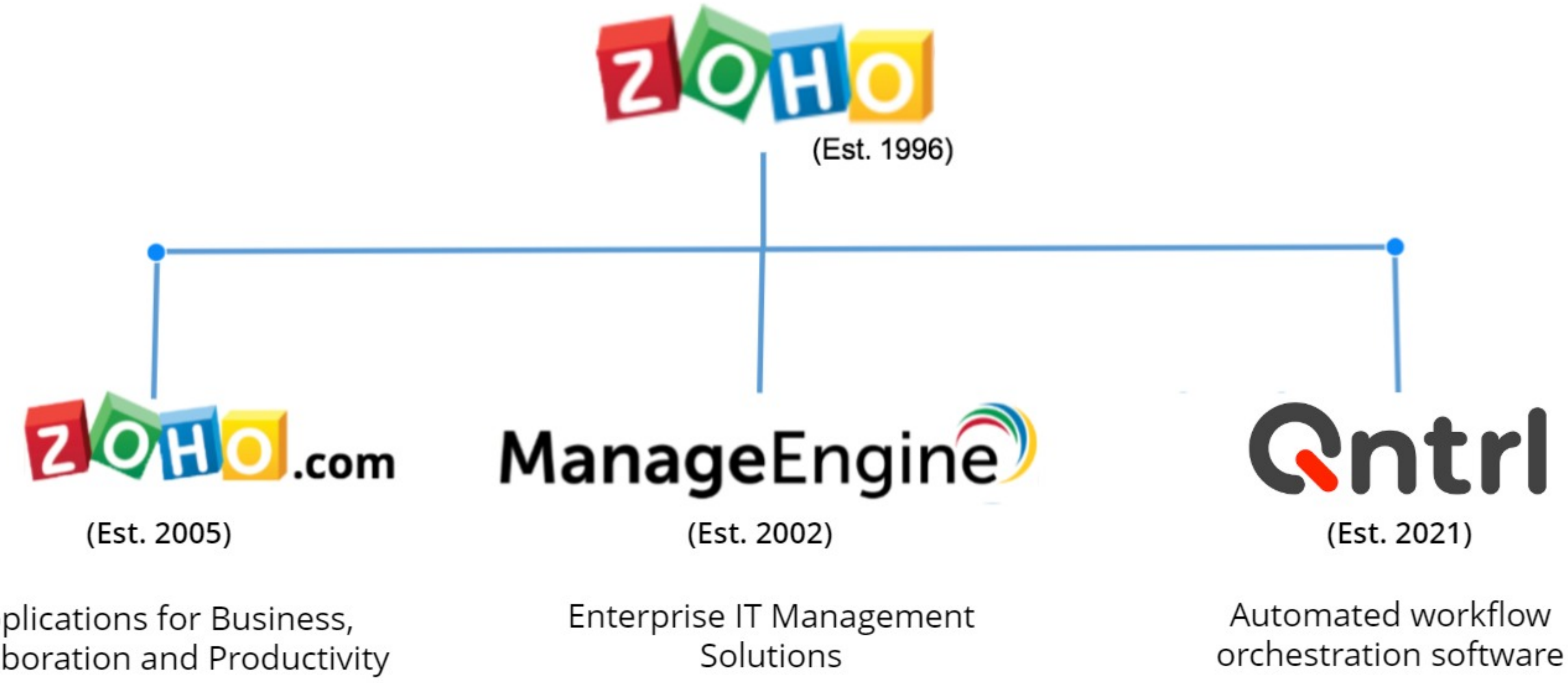
Zoho Corp today :

Bootstraped and Profitable
3 divisions
50 Million+ Zoho.com users
180,000+ ManageEngine clients
190 countries
10000+ Employees

2021

Zoho Corporation Pvt Ltd

Profitable since its inception, the organisation now has 10000+ employees, millions of users around the world and offers a diverse range of products and services.



ZOHO

(Est. 1996)

ZOHO.com

(Est. 2005)

Applications for Business, Collaboration and Productivity

ManageEngine

(Est. 2002)

Enterprise IT Management Solutions

Qntrl

(Est. 2021)

Automated workflow orchestration software

Service management

Full stack ITSM suite
IT asset management with CMDB
Knowledge base with user self-service
Built-in and custom workflows
Orchestration of all IT management functions
Service management for all departments
Reporting and analytics

Identity & access management

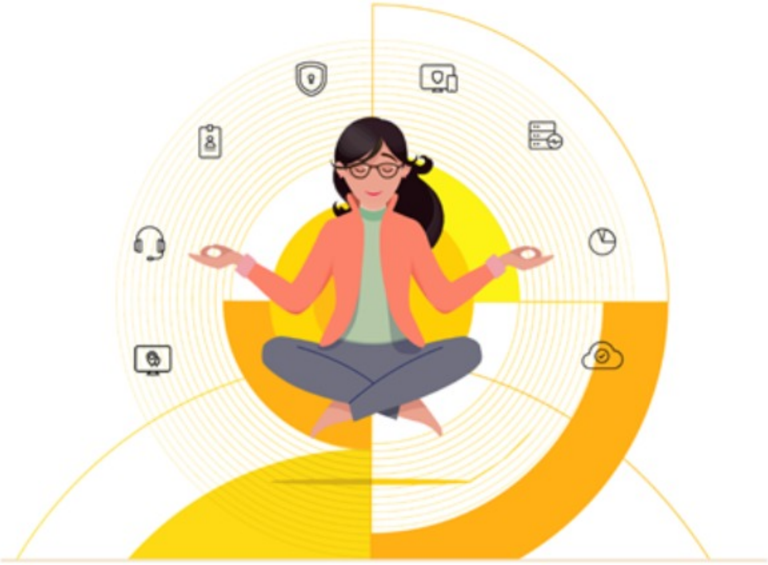
Identity governance and administration
Privileged identity and access management
AD and Azure AD management and auditing
SSO for on-premises and cloud apps with MFA
Password self-service and sync
Microsoft 365 & Exchange management and auditing
AD & Exchange - backup and recovery
SSH and SSL certificate management

Security information & event management

Unified SIEM for cloud and on-premises
AI driven user and entity behavior analytics
Firewall log analytics
Data leakage prevention and risk assessment
Regulatory and privacy compliance

ManageEngine

Bringing IT together



ManageEngine crafts comprehensive IT management software for all your business needs

Available for

Enterprise IT | Managed service providers (MSPs)

as

Self-hosted on-premises
Self-hosted in public cloud (AWS, Azure)
Zoho Cloud-native

Unified endpoint management & security

Desktop and mobile device management
Patch management
Endpoint device security
OS and software deployment
Remote monitoring and management
Web browser security
Monitoring and control of peripheral devices

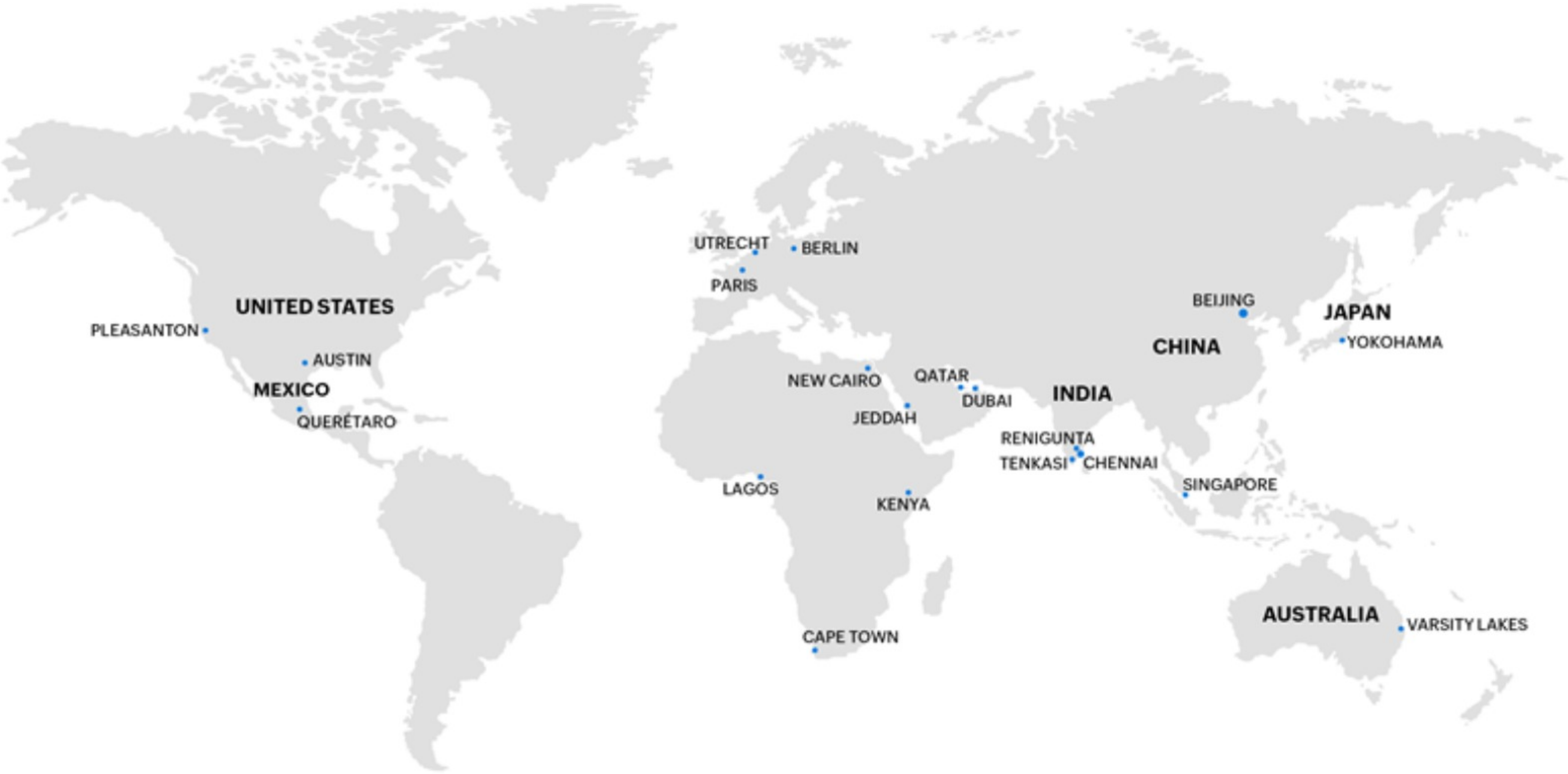
IT operations management

Network, server and application performance monitoring
Bandwidth monitoring with traffic analysis
Network change & configuration management
Application discovery & dependency mapping
Cloud cost and infrastructure monitoring
End-user experience monitoring
AIOps

Advanced IT analytics

Self-service IT analytics
Data visualization and business intelligence for IT
Hundred of built-in reports and dashboards
Instant, flexible report creation
Out of the box support for multiple data sources

Our Global Presence



ManageEngine

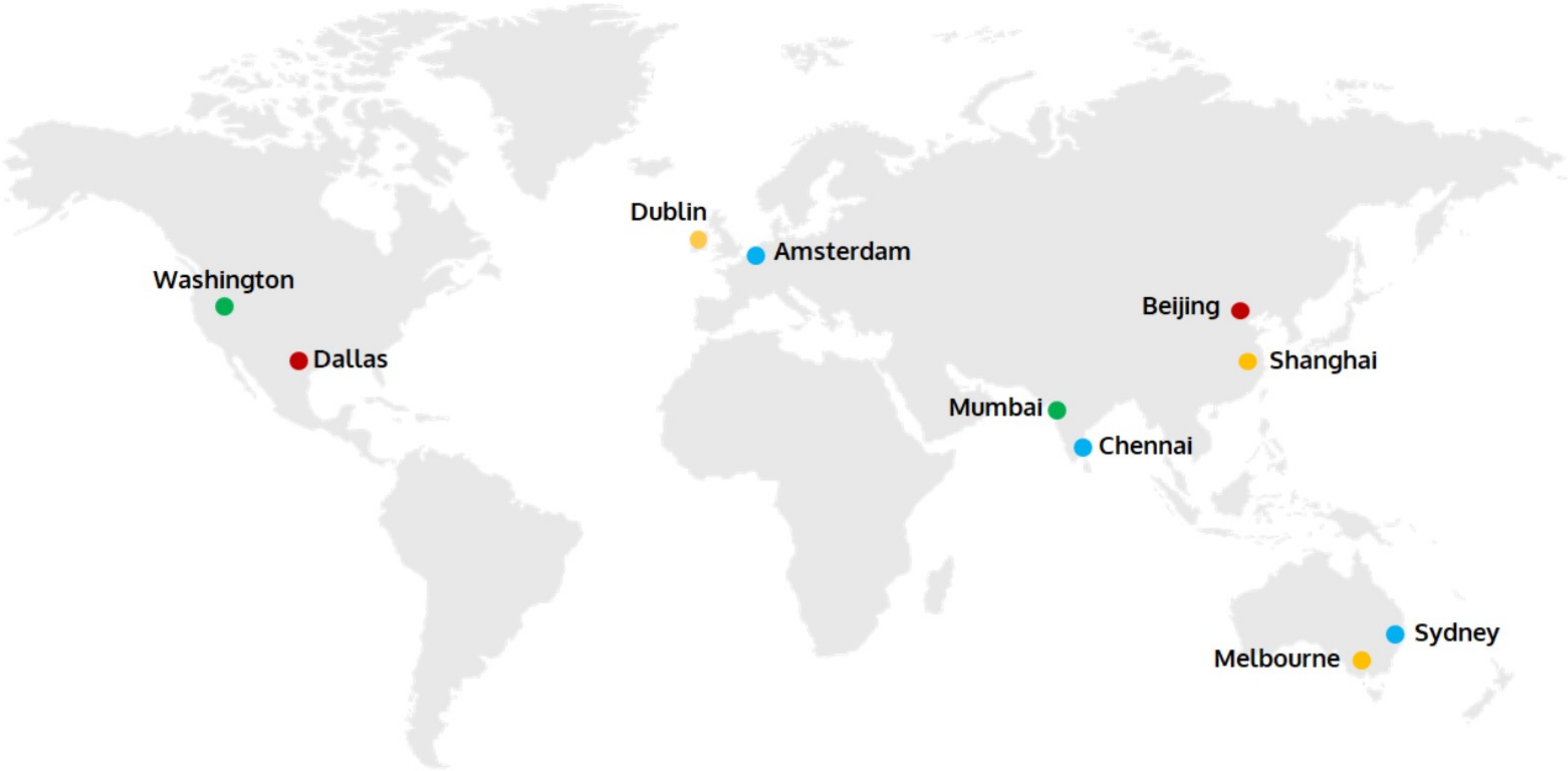
Our extended arms

200+ Channel & Technology Partners across the globe

Asia Pacific Europe Africa Middle East North America Latin America

ManageEngine

Our Datacenters



Security at ZOHO

More than **60 million users** place their trust in us to run their businesses - Our security, privacy, and compliance practices are built on the foundation of that trust.

ISO 27001

ISO 27017

ISO 27018

Soc-2 type II

Trust-e

GDPR

Privileged Password & Key Management

> Why is this an missing element?

ManageEngine

What's in your IT Kingdom?

Firewalls, Routers, Hypervisors, Database, Applications

Cloud

Firewalls, Routers, Servers, Database, Applications

On-Premise Data Center

Web Accounts, Banking, Credit Cards, Contacts

Personal

Laptops, Tablets, Smartphones

End Points

Types of accounts

Personal user accounts	Privileged accounts	Software or service accounts	Generic accounts
- Desktop - Application - Network access	Administrator or root of : - Servers - Databases - Network devices - Applications	- Application to application - Application to database - Windows service accounts and scheduled tasks	Accounts intentionally created for shared use in - Directory servers - FTP servers - File servers
Characteristics	Characteristics	Characteristics	Characteristics
- Highly accountable - Impact localized to the user	- High privilege but lack identity - Usually shared among many users	- High privilege but lack of identity - Usually hard coded in applications and scripts	- Low privilege but lack of identity - Always shared among users with no tracking

Let's ask ourselves few questions?

1. Do we know how many privileged accounts are there in our infrastructure?
2. Who has those accounts password & how are they maintaining it?
3. What process we follow to provide and revoke access to privileged accounts?
4. How frequently do we change privileged account passwords?
5. How are we providing access to privileged accounts without sharing the passwords?
6. How are we monitoring the actions performed in such sessions?
7. Do we have privileged account passwords hard-coded with plain text in scripts and applications ?
8. How are we controlling the proliferation of SSH private keys across our network?
9. How are we managing SSL certificates in our infrastructure?
10. How are we preparing for regulatory audits with regards to privileged accounts?

The hard reality today

STORAGE

- Excel sheets, text files
- Hard copies in a physical vault
- Hard coded in scripts
- SSH keys in multiple systems

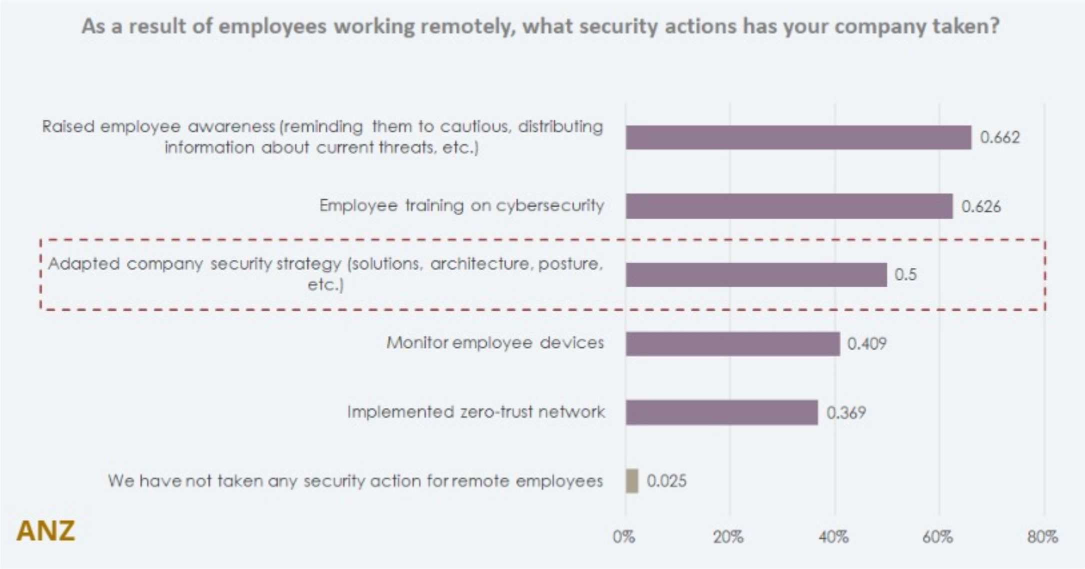
CONTROL

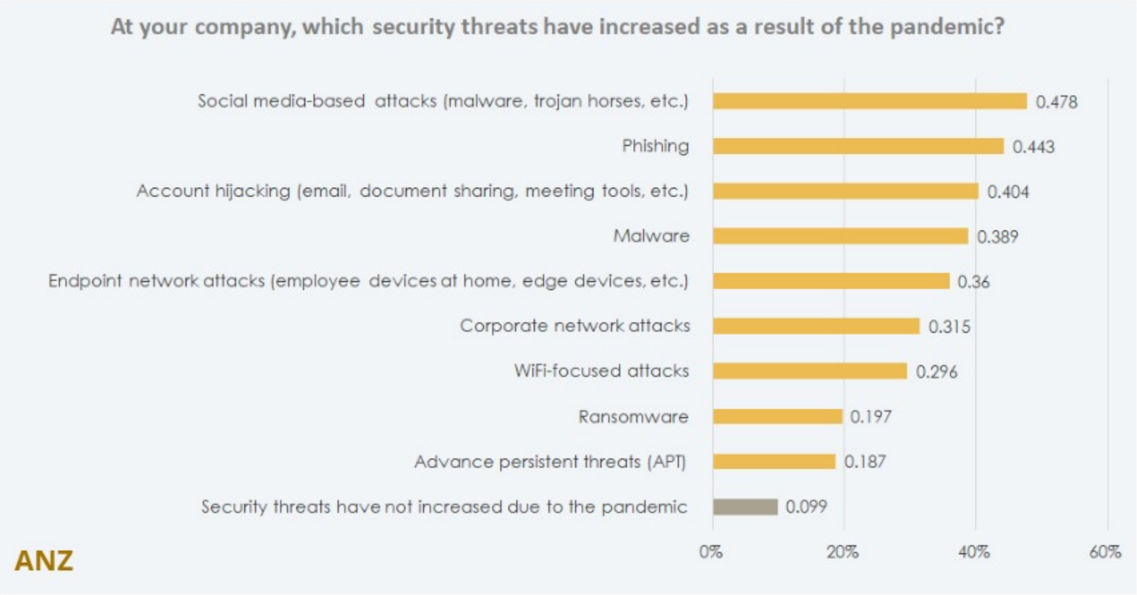
- No central control or visibility
- No clear policies
- Use of manual processes or trivial tools so passwords are rarely modified

ACCESS

- Uncontrolled for administrators
- Shared ad hoc
- Proliferates to no end

Some stats from our "Digital Readiness Survey"





Global:

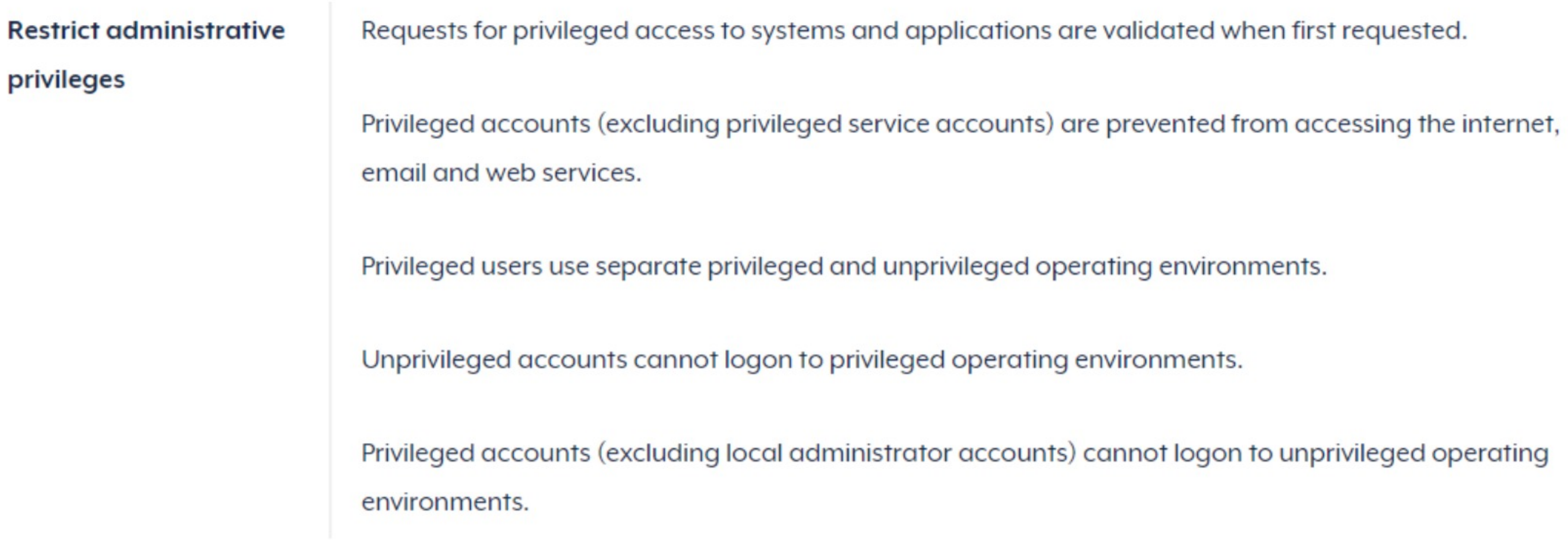
- **74%** of data breaches start with privileged credential abuse, and **65%** of organizations have shared administrative access to privileged systems.
- Only **56%** of companies have changed their security strategy—despite remote employees being directly targeted more often.
- **83%** of respondents revealed that remote workers increase security risks.

Essential 8 Maturity Model

Strategies to Mitigate Cyber Security Incidents

Australian Government
Australian Signals Directorate

ACSC
Australian
Cyber Security
Centre



Restrict administrative privileges

Requests for privileged access to systems and applications are validated when first requested.

Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services.

Privileged users use separate privileged and unprivileged operating environments.

Unprivileged accounts cannot logon to privileged operating environments.

Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.

How do we help combat?

ManageEngine
PAM360

7 ways to reinforce privileged access security in your enterprise

1 Create visibility into all the privileged access in your network:

Discover & identify privileged accounts

Scan networks and discover flavors of Windows, Linux, VMware, AWS and network devices for the associated ***privileged accounts***, including ***Windows service accounts***.

Discover & identify certificates/SSH keys

Scan networks and discover all ***SSL certificates*** deployed in your network regardless of the CA, and ***SSH keys*** deployed systems.

Centrally store & secure

Securely store privileged passwords, digital certificates, license keys, etc in a ***central location*** using ***256-bit Advanced Encryption Standard (AES)***. Dual-encrypt data at the application and database level.

Organize resources into "Groups & Sub-Groups"

Organize resources under ***"Static" & "Dynamic"*** groups to ***better manage*** permissions and to perform ***bulk operations*** like password reset, notifications, transfer resources ownership, etc

2 Build multiple layers of security for privileged access:

Configure granular access permissions

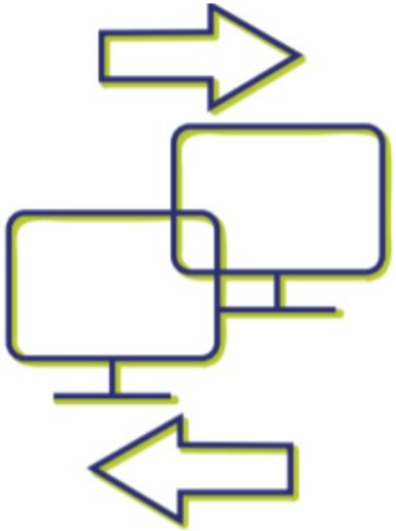
Configure & Apply ***fine-grained access restrictions*** on users based on their roles for the secure usage of the ***Product & Privileged Credentials.***

Implement multi-factor authentication

Add an extra layer of security by enforcing ***Two-factor Authentication*** for two successive stages of authentication to access the web console.

Allow launching direct connection

Allow ***Secure Login*** to resources through emulated Windows RDP, SSH and Telnet sessions from any HTML5-compatible browser ***without sharing the password.***



3 Adopt easier and quicker workflows to improve business productivity:

ManageEngine

Impose release controls

Necessitate the use of well-architected ***access control workflows to request and release*** the privileged passwords on approval or to allow secure login.

Automatically approve exclusive/time-based access

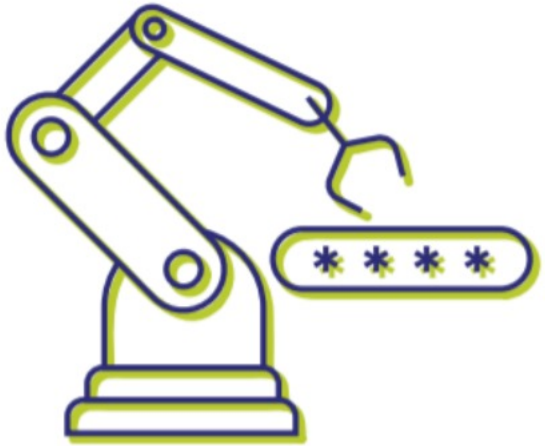
Pre-approve exclusive access to passwords for a time duration; ***Schedule automatic approval*** of requests raised during a specific time period in the day.

Set automatic password reset

Automatically ***reset passwords upon usage*** to avoid unauthorized access attempts in the future; Automate the process of ***scheduled password rotation***.

Just-in-time privilege escalation

Assign & revoke ***just-in-time controls*** for your domain accounts with ***higher privileges*** only when required by the users.



4 Condense the attack surface by eliminating credential hard-coding:

Application credential security through API's

Eliminate the use of ***hard-coded credentials*** stored on local machines across the networks by ***providing secure APIs*** for application-to-application and application-to-database credential management.

Plug-ins to restore security in DevOps environments

Solve the problem of ***embedded credentials*** by facilitating integration with various ***CI/CD platforms*** to securely fetch credentials and carry out the required operations, automating and orchestrating access provisioning, granular control, and auditing without compromising on speed and agility.

5 Improve oversight and accountability of privileged sessions:

Record privileged session activities

Have foolproof and ***fine-grained recordings of privileged sessions*** launched by trusted privileged ***insiders and third-party vendors*** facilitating easier governance and better accountability of privileged sessions.

Shadow privileged sessions in real-time

Shadow privileged sessions, and monitor them in real-time to promptly detect and ***terminate suspicious activities***, and efficiently investigate risky sessions.

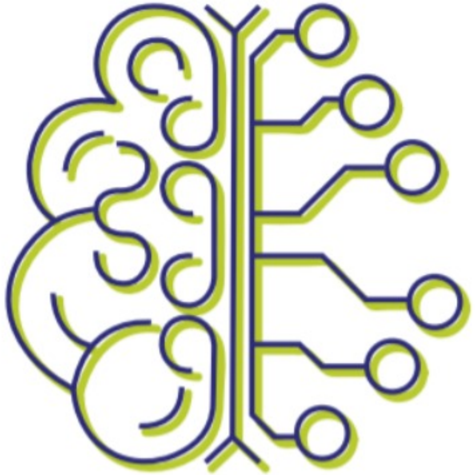
6 Readily demonstrate compliance with regulations and security policies:

Maintain comprehensive audit trails

Capture all events involving privileged credentials and access in clear, downloadable audit trails and reports of **'who', 'what' and 'when'** of entire password access scenario in your enterprise.

Demonstrate compliance

Stay ever-ready for compliance audits like ***SOX, HIPAA, and PCI DSS*** with built-in reports and essential guidelines.



7 Integrate with advanced technologies to make better business decisions:

Privileged user behavior Analytics

Adopt ***AI and ML-driven*** monitoring capabilities to continuously ***detect unusual*** and potentially ***harmful privileged activities***, and automatically set off mitigating controls to prevent damage.

Ticketing system integration

Add ITSM into the mix to streamline privileged access requests, and bolster the access approval workflows by incorporating ticket ID validation. Authorize credential retrieval for service requests requiring privileged access only upon ticket status verification.

ManageEngine PAM360

7 ways to reinforce privileged access security in your enterprise

1 Create visibility into all the privileged access in your network:

2 Build multiple layers of security for privileged access:

3 Adopt easier and quicker workflows to improve business productivity:

4 Condense the attack surface by eliminating credential hard-coding:

5 Improve oversight and accountability of privileged sessions:

6 Readily demonstrate compliance with regulations and security policies:

7 Integrate with advanced technologies to make better business decisions:

Q
A

Thank You

nirmal.d@zohocorp.com

ManageEngine

www.manageengine.com.au