ManageEngine

Building a resilient cybersecurity strategy for 2019: Part I

ManageEngine

How UEM can enhance your enterprise cybersecurity

Giridhara Raam

Agenda

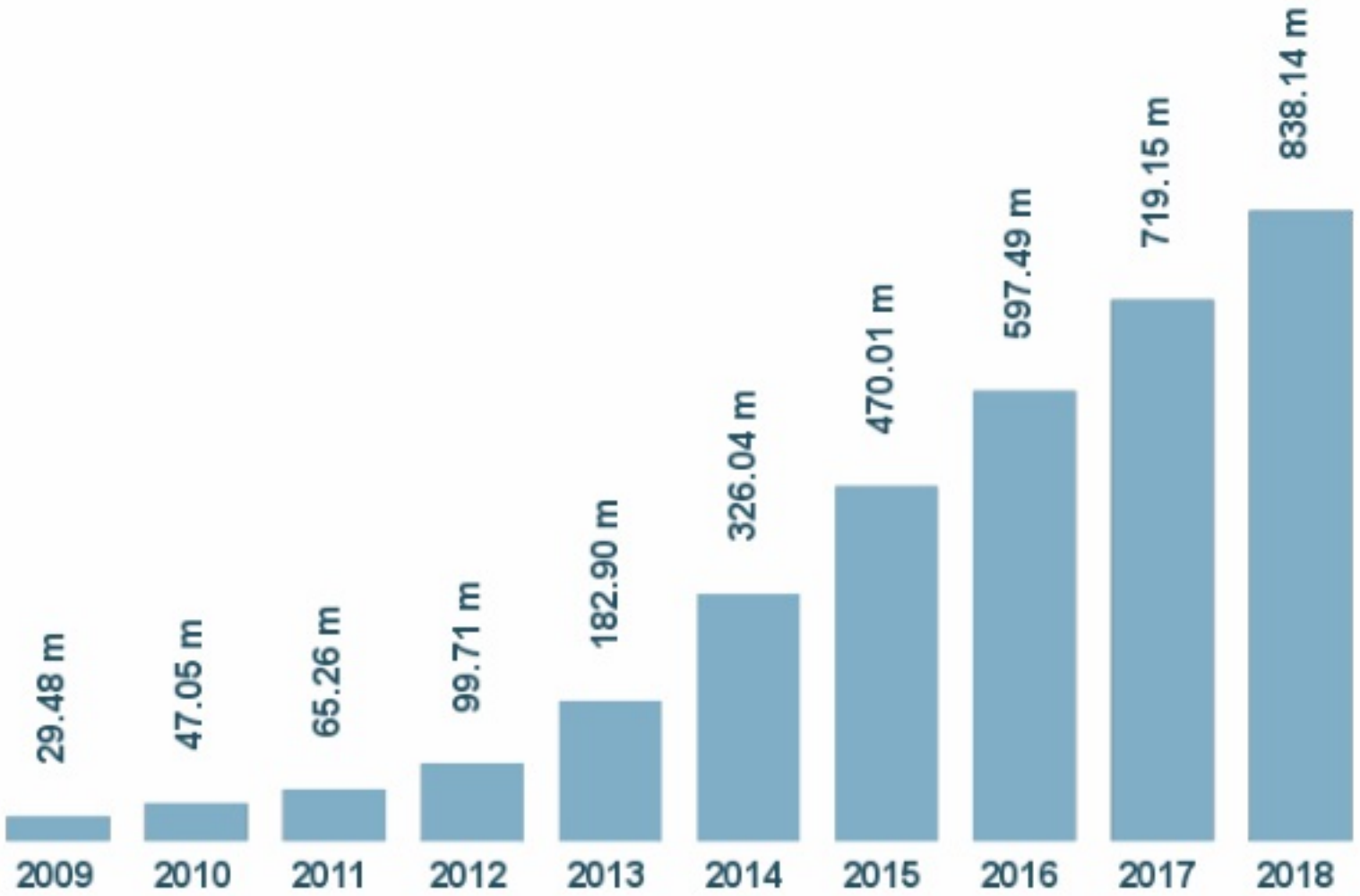
- Cyberattacks 2018 & 2019
- Understanding the cybersecurity challenges
- How can UEM make a difference?
- UEM best practices for 2019
- Anatomy of insider attacks
- Key findings and predictions for 2019
- Securing your privileged access is crucial

ManageEngine

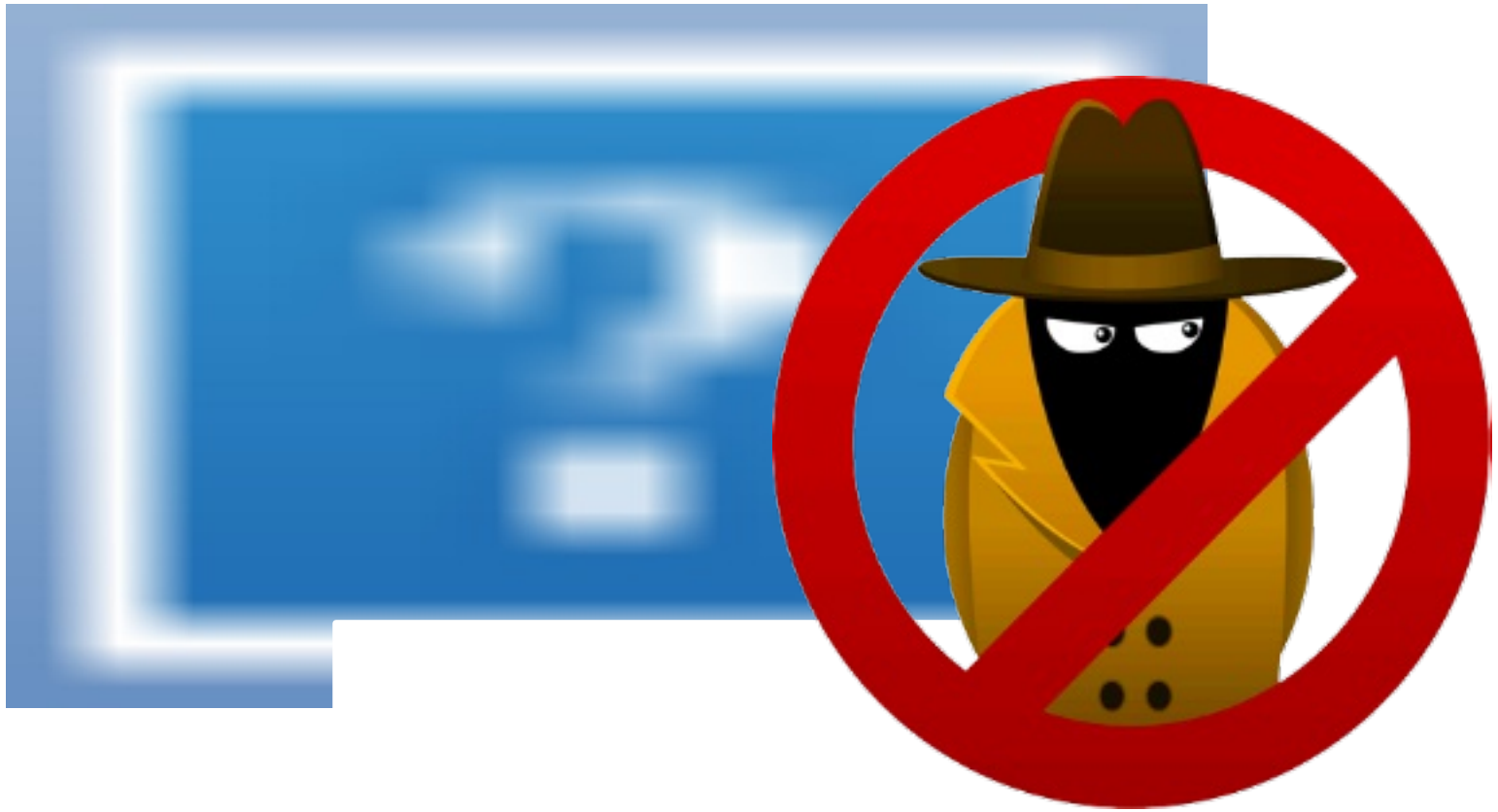
Cyberthreats 2018

Malware

Total malware

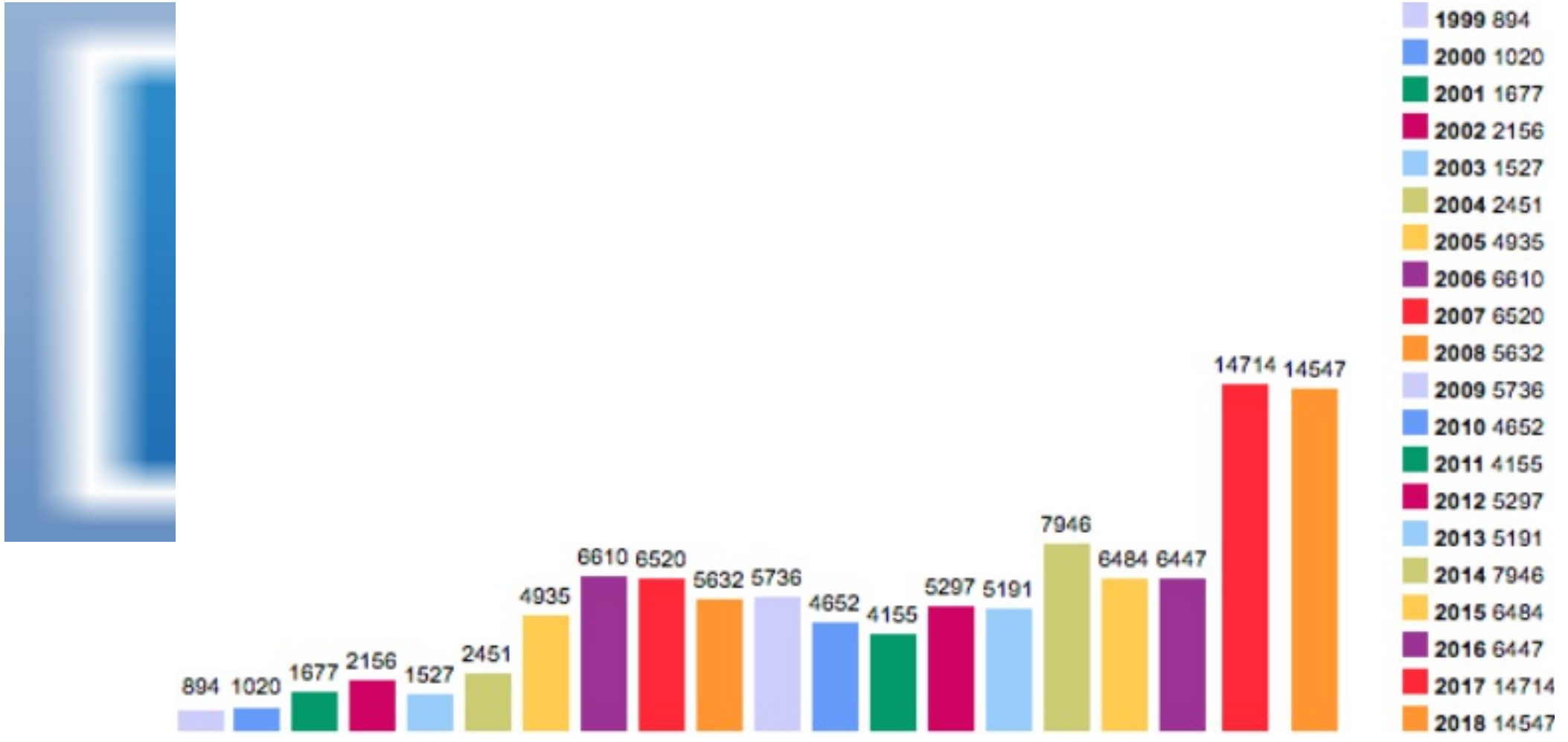


Ransomware

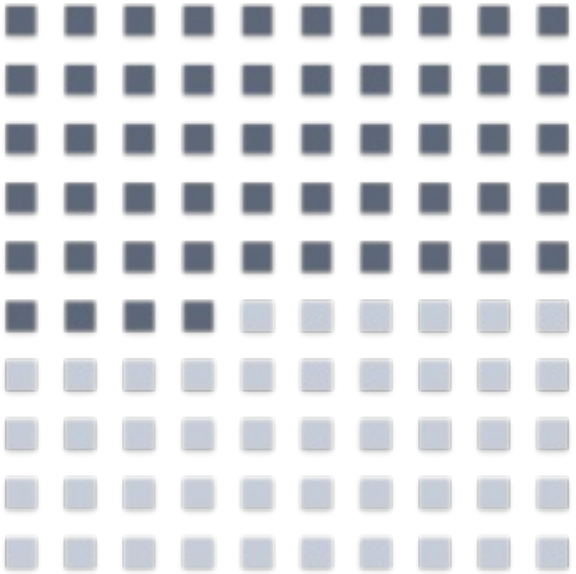


Zero day exploits

Zero day exploits



ManageEngine



54%

of companies experienced one or more successful attacks that compromised data and/or IT infrastructure

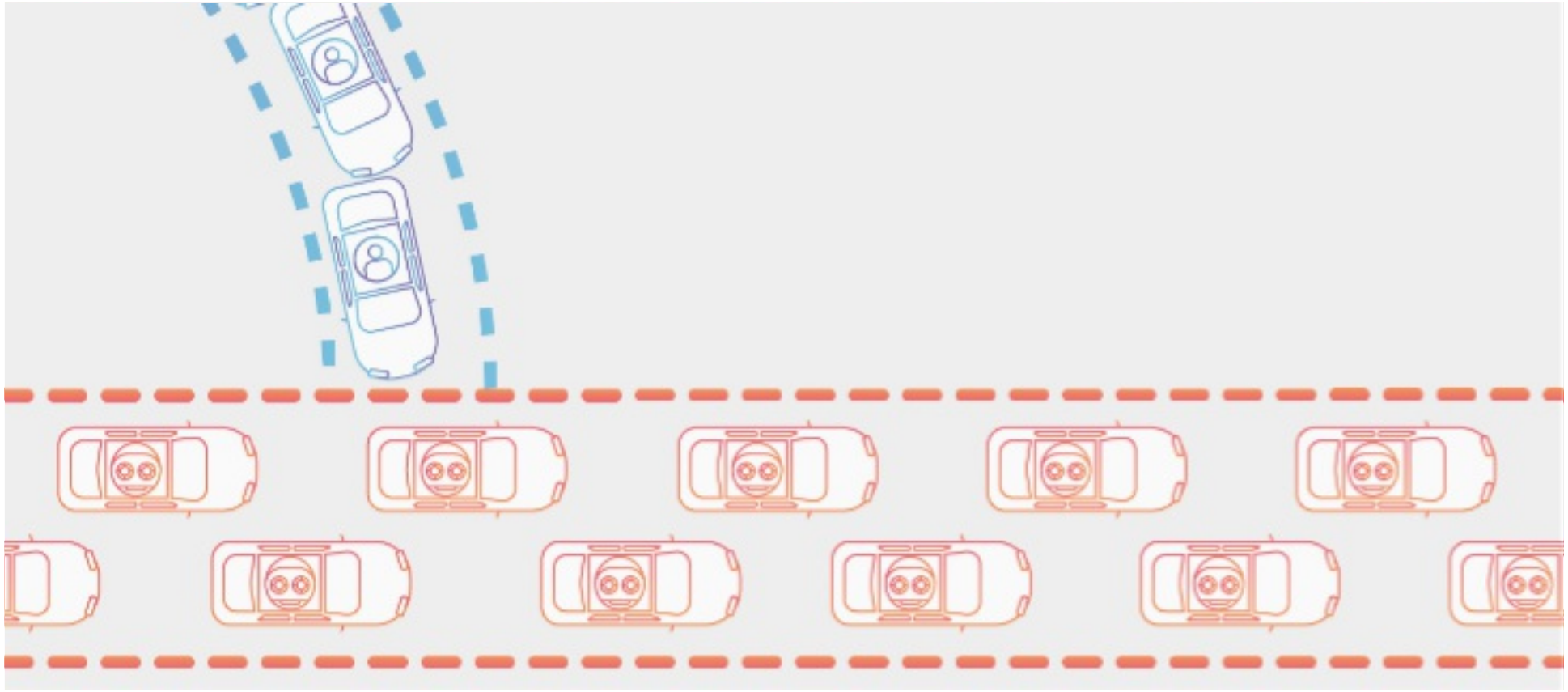
77%

of those attacks utilized exploits or fileless techniques

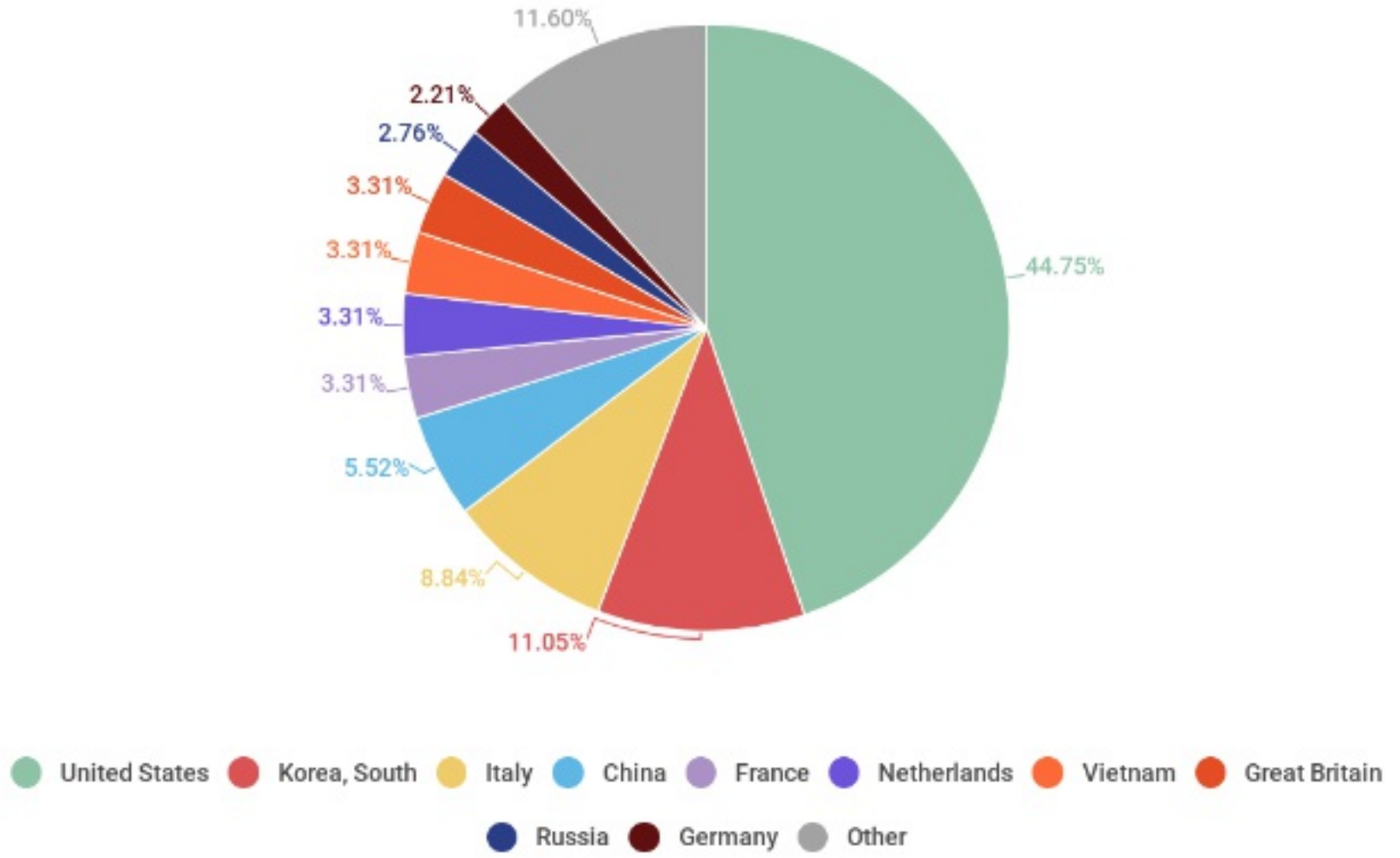
ManageEngine

Man-in-the-middle attacks

DDoS attacks



DDoS attacks



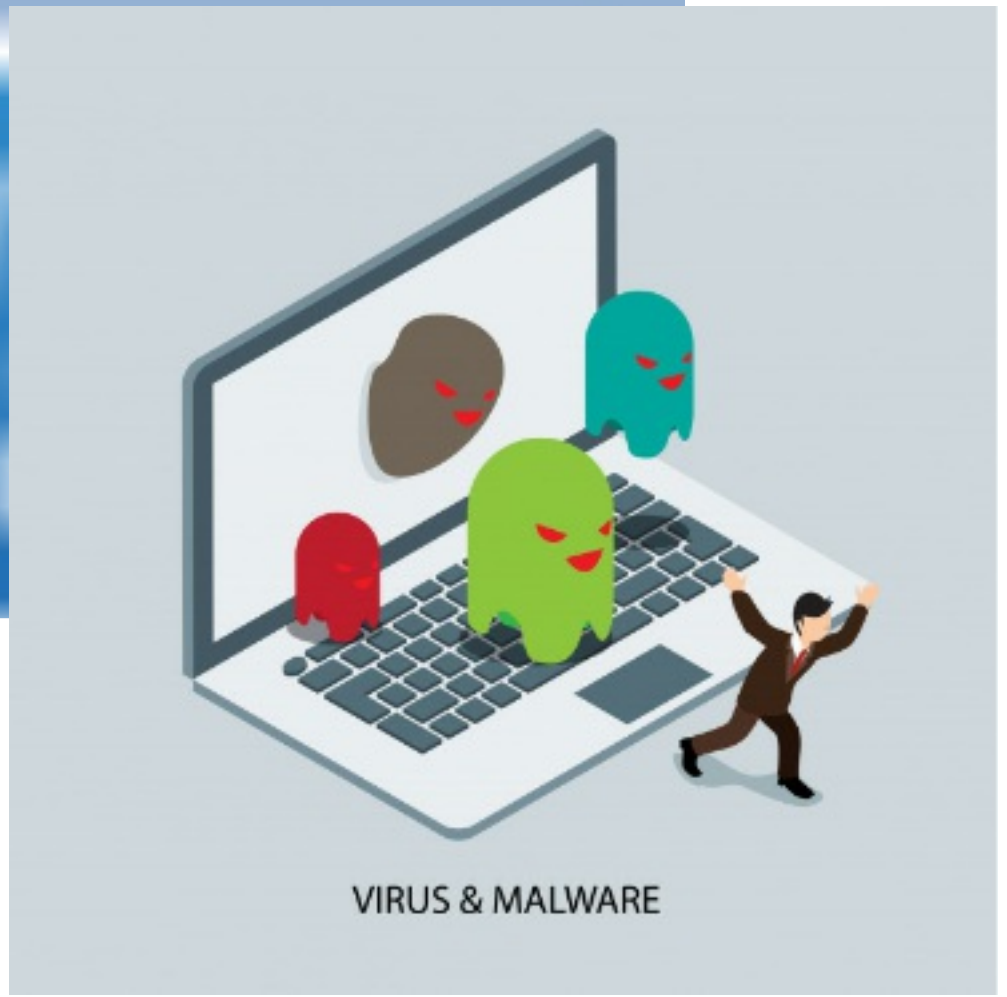
ManageEngine

ManageEngine

Cyberattacks 2019

AI powered attacks

Sandbox evading malware



ManageEngine

Compromising IoT devices

ManageEngine

Understanding the cybersecurity challenges

Complex devices

- Device type
- Device models
- Firmware types
- Operating system

Complex applications

- Windows applications
- mac OS applications
- Linux applications
- Android applications
- iOS applications

Different type of users

- Static users
- Dynamic users
- Contract based users
- Guest users

Cloud computing

- Cloud based software
- Corporate and personal data
- Single touch point

ManageEngine

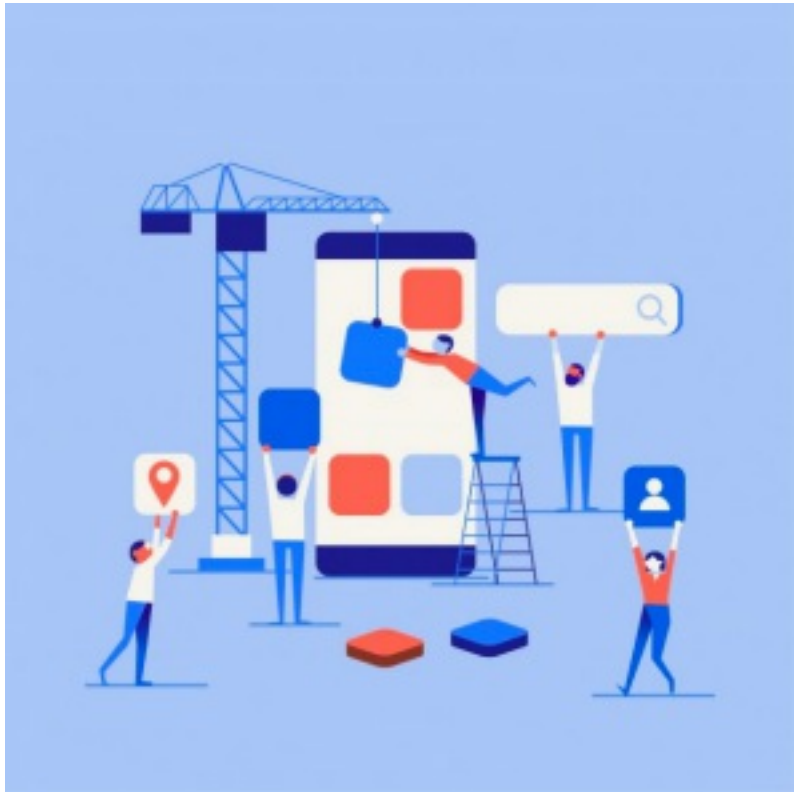
How can UEM enhance your cybersecurity?

Complex devices

Unified device management

Complex applications

Unified application management



Different type of users

User management and control

ManageEngine

Cloud computing

Securing browsers

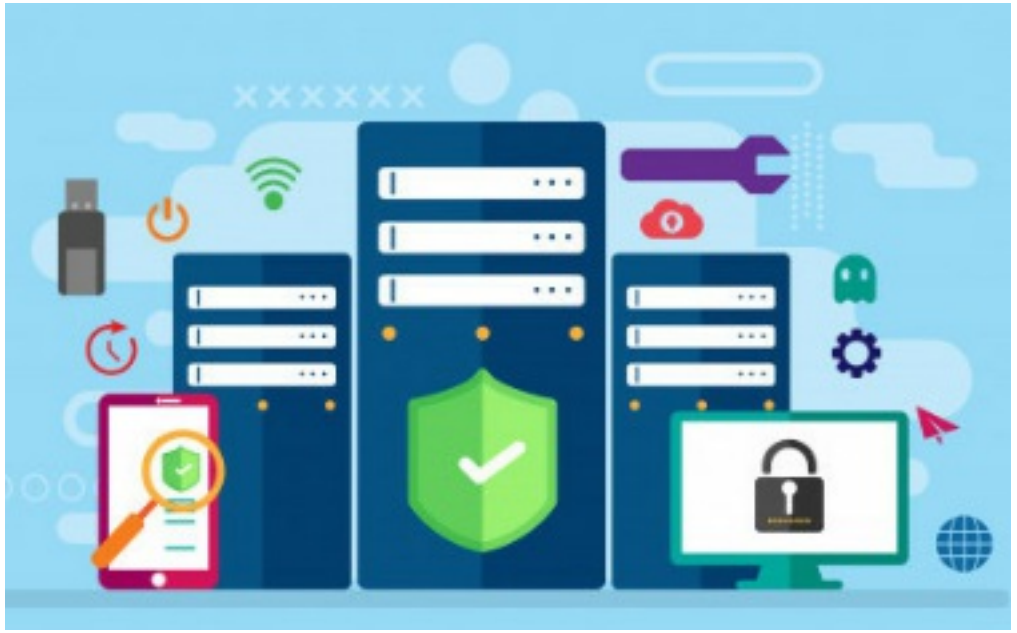
ManageEngine

Ensure data security and user privacy

"Mobile apps account for 89% of mobile media time, with the other 11% spent on websites."

Secure your data at rest, on move and in use

- Securing data on mobile devices
- Securing email communications
- Identifying compromised devices
- Equipping containerization



Offer user privacy

- Restricting privileged access for technicians
- Defining data boundaries for employees

ManageEngine

ManageEngine

Scenarios & Examples

Scenario 1

A new cyberattack is spreading across countries, for example 'WannaCry'. Will our IT administrators be able to fix this using a Automated Patch Deployment procedure?

Scenario 2

Employees can plug-in USB drives to steal business sensitive documents from computers? How to prevent these insider threats?

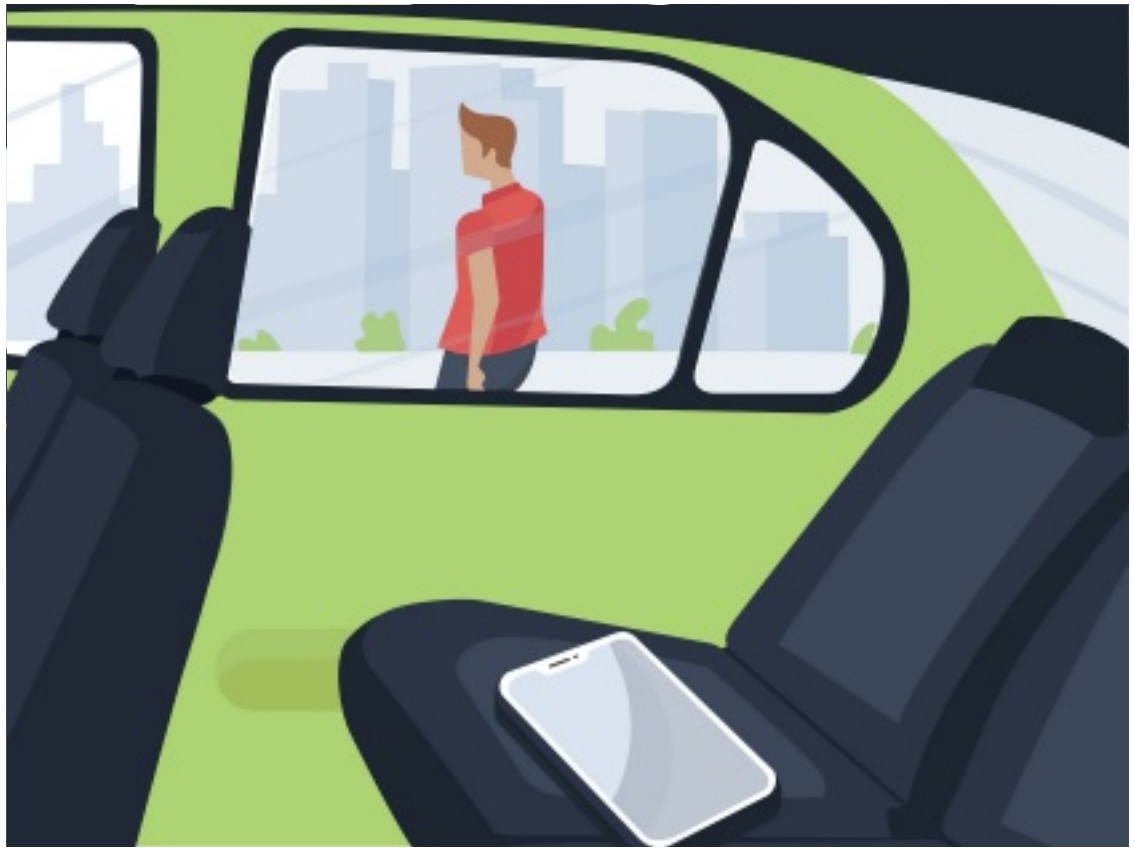
Scenario 3

Data breach into any personal app can leave your sensitive information in business apps wide open.

How to prevent these unforeseen Man-in-the-disk and mobile malware attacks?

Scenario 4

Employees can lose their smartphones at times. Along with their lost devices goes business sensitive data. How to recover these devices and their data?



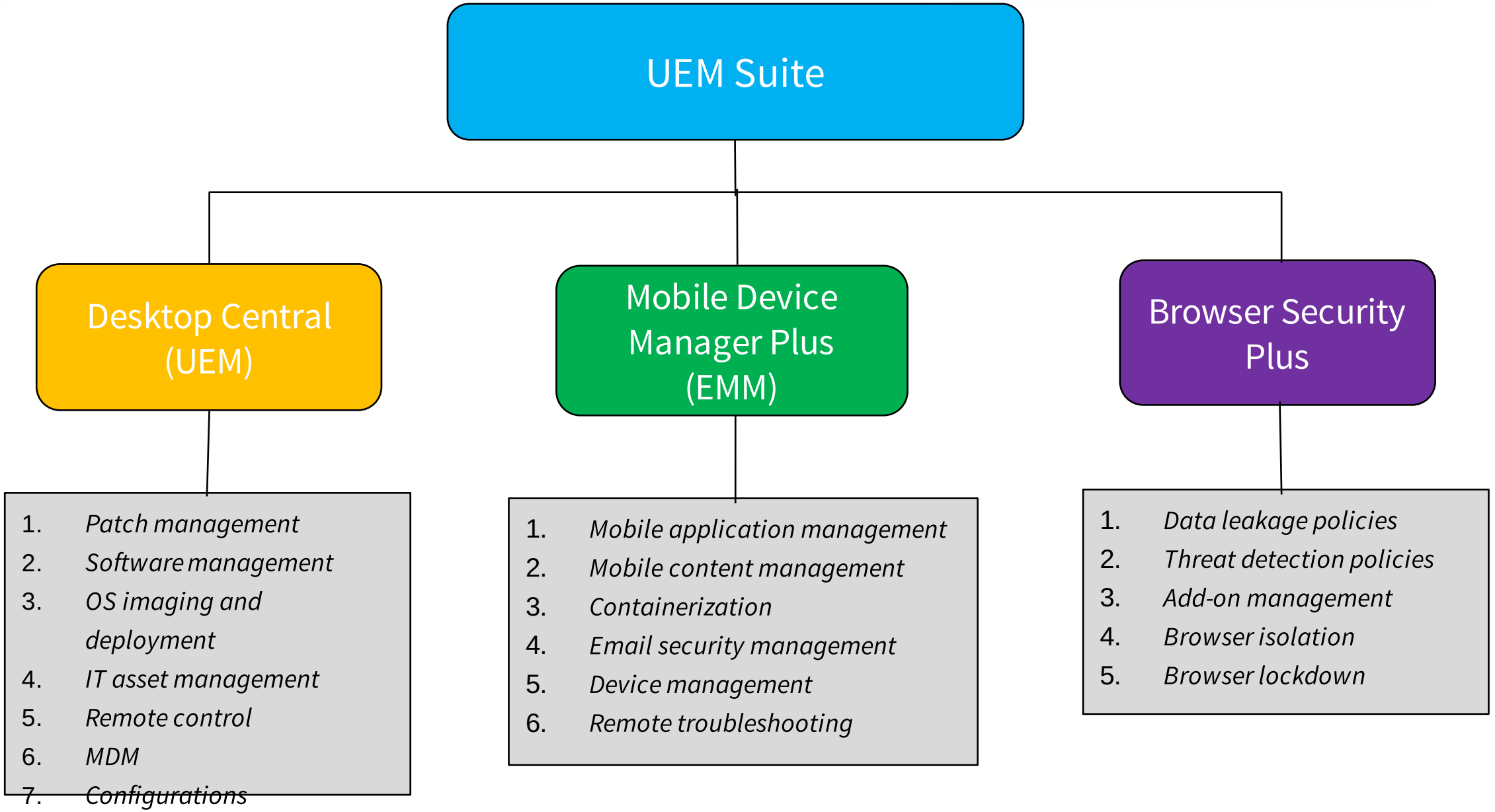
Scenario 5

In case of the processor bugs, Meltdown and Spectre the threat was at hardware level, and the patching procedure was also quite complex as it required AV compatability check as well.

Can a UEM solution mitigate these sort of complex situations?

Scenario 6

When two employees communicate over a mail, they can share business sensitive documents as an attachment, how to make sure this communication and the information shared among them stays secured?


UEM Suite
Desktop Central (UEM)
Mobile Device Manager Plus (EMM)
Browser Security Plus
1. Patch management
2. Software management
3. OS imaging and deployment
4. IT asset management
5. Remote control
6. MDM
7. Configurations
1. Mobile application management
2. Mobile content management
3. Containerization
4. Email security management
5. Device management
6. Remote troubleshooting
1. Data leakage policies
2. Threat detection policies
3. Add-on management
4. Browser isolation
5. Browser lockdown

Australian Cyber Security Centre

- Defined eight strategies to mitigate cybersecurity incidents
- Desktop Central can help you with 6/8 strategies
- Australian Cybersecurity Blog

- Defined twenty critical security controls for establishing an effective cybersecurity strategy.
- Desktop Central can help you with 10/20 security controls.
- Ten security controls infographic

Seven best UEM practices for 2019

1. Automated patch management
2. IT asset management
3. User and group privilege management
4. Firewall and browser configuration
5. BYOD management
6. Mobile application management (MAM)
7. Data management life cycle

ManageEngine

ManageEngine

Product overview

1. Desktop Central (UEM solution)
2. Mobile Device Manager Plus (EMM solution)
3. Browser Security Plus New

ManageEngine

Session 2: A proactive approach for combating insider threats in 2019

Shwetha

ManageEngine

Insider attack – One of the nine major cyber threats to look out for 2019

[Source: Threat horizon 2019]

The insider threat cyber kill chain

Recruitment / Tipping point: Represents the entry of malicious users or the 'tipping point' where existing employees decide to act against the organization and steal information.

Data Acquisition: Insider gains access to target systems by exploiting the vulnerabilities, extracts data from a series of locations.

Search & Reconnaissance: The malicious insider scans your network and identifies potential, vulnerable targets.

Exfiltration: The final stage of the attack where acquired data is prepared to be exfiltrated from their orignal locations.

[Source: Introducing the insider threat kill chain by ZoneFox]

Nature of insider threats

- **Accidental exposure:** Negligent employees are tricked by phishing attacks and often end up sharing company's sensitive information by clicking on malware or spoofed websites.
- **Malicious attack:** Disgruntled employees exploit vulnerabilities within the network and exfiltrate sensitive data for personal gain, revenge etc.,

What is at stake?

- Credential theft
- Access control issues
- Poor data hygiene
- Possibilities of data spill
- Surreptitious fourth-party infiltration

ManageEngine

World-renowned organizations fall victim to insider attacks

Target Data Breach (Nov - Dec 2013)

- **40 million** user credit and debit accounts exposed.
- Attackers infected **40,000** to **60,000** POS terminals with malware.
- Hackers gained access to privileged credentials of one of Target's vendors.
- Infiltrated into Target's network—installed malware.

Nuance Communications Breach (Nov - Dec 2017)

- US-based speech recognition firm fell victim to breach of thousands of patient records.
- **Cause**: Third-party unauthorized access
- Former employee gained access to the firm's critical servers; accessed personal information of **45,000** patients.

ManageEngine

Present-day scenario

Australian Cyber Security Centre (ACSC)

- CERT Australia, a wing of the ACSC, declares insider threats are the hardest to mitigate, detect and prosecute.
- Strongly recommends organizations to implement the "Essential Eight".
- **Restricting administrative privileges** is one of the top priorities.

Cyber security threat landscape in APAC

Direct cost

- Potential economic loss in APAC due to cybersecurity breaches account to **$1.745 trillion**—more than **7%** of the region's total GDP.
- Large-sized organizations incur an average loss of **$30 million** and average sized organizations **$96,000**.

Indirect cost

- **67%** (7 in 10) organizations faced loss of jobs due to security incidents.

[Source: Securing the modern enterprise in a digital world, Frost & Sullivan study]

GDPR compliance and Privileged Access Management

- The basic intent of the GDPR is data protection—more specifically, making personal data secure.
- Personal data is all-pervasive and is found nearly in every piece of your IT infrastructure.
- Organizations need to enforce strict access controls and meticulously track access to data to comply with the GDPR.
- PAM is a security discipline that aims to keep an organization safe from accidental / deliberate misuse of privileged access.

Key findings & predictions for 2019

- **90%** of cybersecurity professionals feel their organization is vulnerable to insider threats.
- **58%** of data breaches in the healthcare industry involved insider activity [2018 Verizon PHIDBR]
- Too many users with excessive access privileges (**37%**) are the main enablers of insider threats.
- Privileged credentials (**52%**) remain to be one of the predominant attack surfaces of an insider attack.
- Weak passwords (**56%**) and bad password sharing practices (**44%**) are the biggest vulnerabilities for insider threats.

[Source: 2018 Insider threat report, CA Technologies]

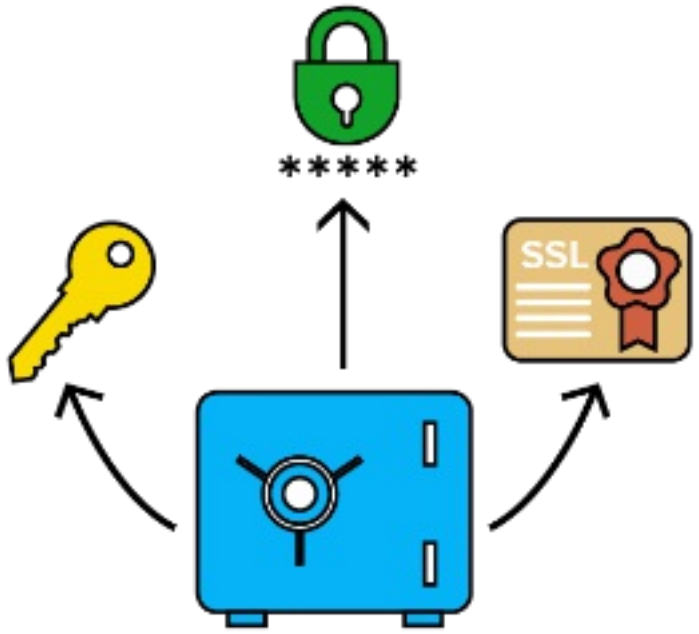
ManageEngine

How to combat?

Adopt a proactive approach: Secure your privileged access

Discover & Consolidate

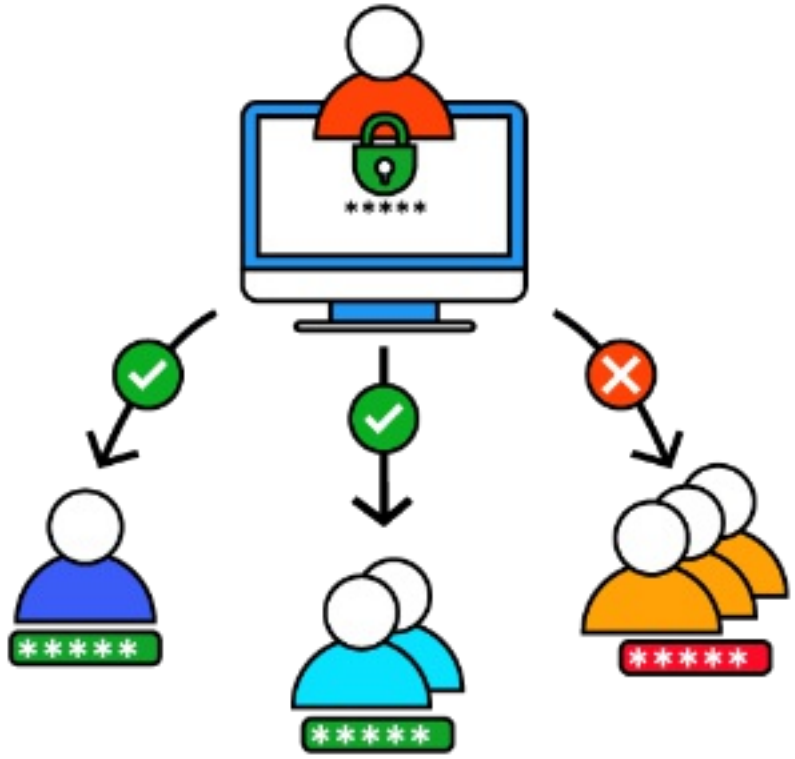
Discover and consolidate all your privileged identities in a secure, centralized repository.



Adopt a proactive approach: Secure your privileged access (Cont'd..)

Regulate access

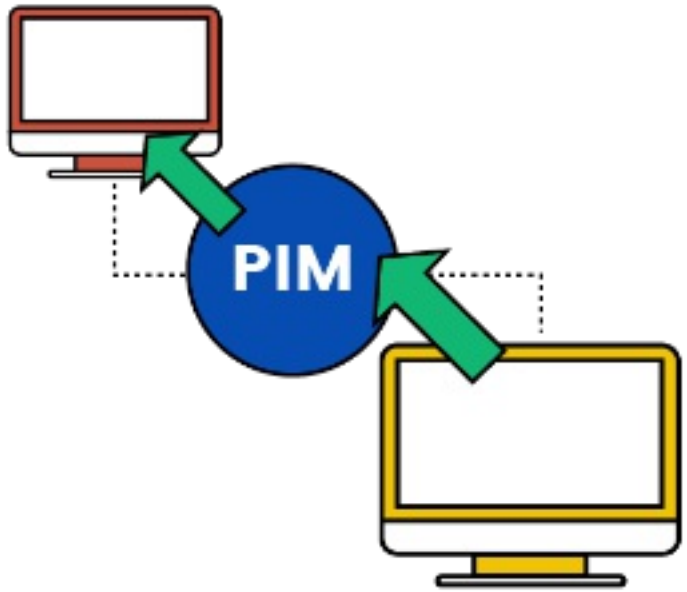
- Enforce fine-grained access restrictions
- Chart out a strong password access control workflow



Adopt a proactive approach: Secure your privileged access (Cont'd..)

Centralized control on access pathways

- Shut off remote access requests from unapproved solutions; implement a centralized remote access mechanism.
- Eliminate sharing of passwords in clear-text.



Adopt a proactive approach: Secure your privileged access (Cont'd..)

Audit all user activities

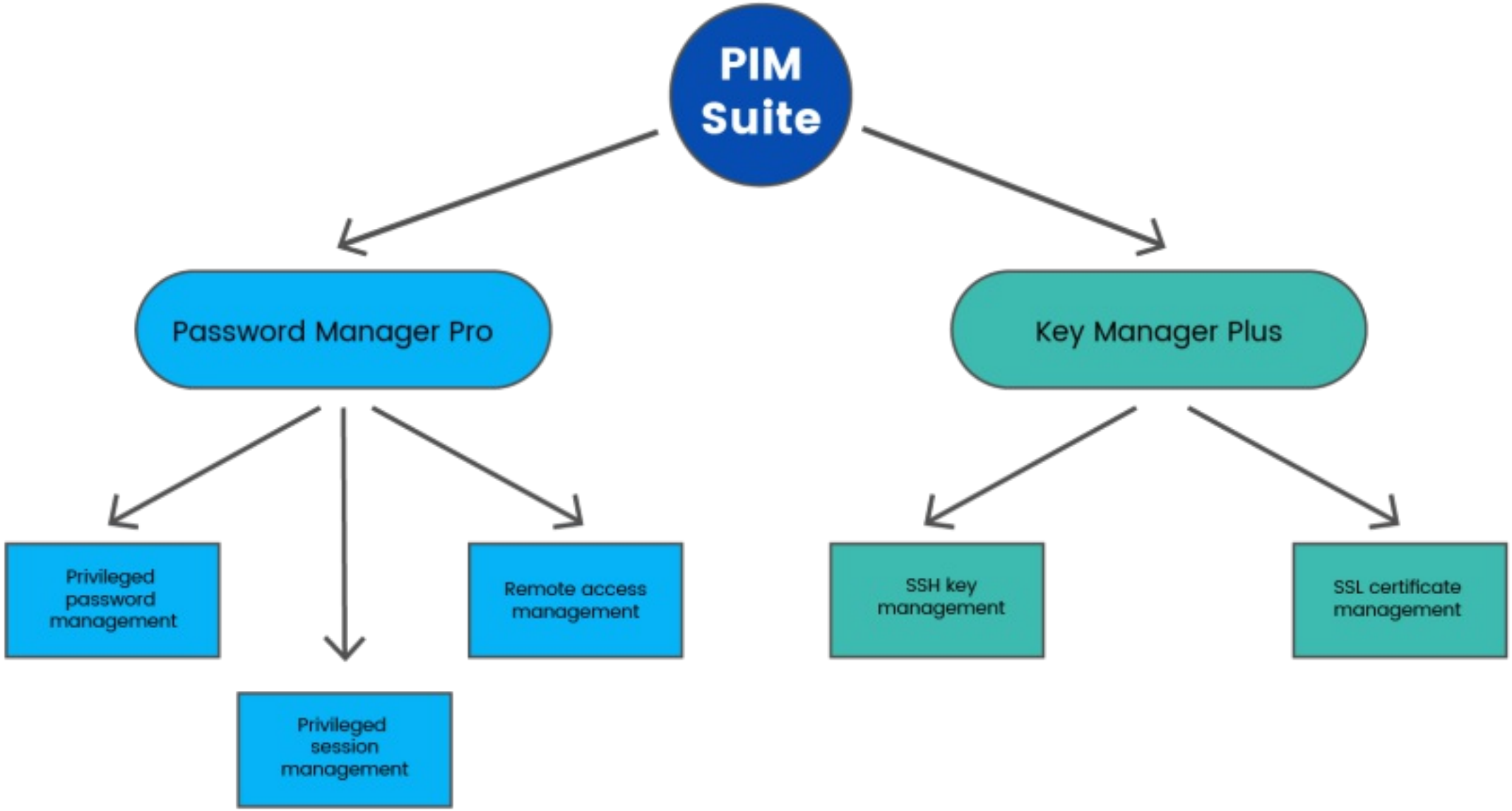
- Keep close tabs on all user activities around privileged account operations; Tamper proof your audit records and make them retrievable only for authorized administrators.
- Real time notification for critical operations such as privileged account creation, deletion, remote access etc.,

3 Rules of the thumb

- ✓ Get 'em all under one roof
- ✓ Start caring about sharing
- ✓ Check and double-check everything

ManageEngine

Our privileged identity management (PIM) suite serves as the one-stop solution for managing all your privileged identities


PIM Suite
Password Manager Pro
Key Manager Plus
Privileged password management
Privileged session management
Remote access management
SSH key management
SSL certificate management

Questions, please!

Thank you

ManageEngine

www.manageengine.com