# The Cybersecurity Blueprint

## How to adopt the right cybersecurity strategy for your business

WHITE PAPER

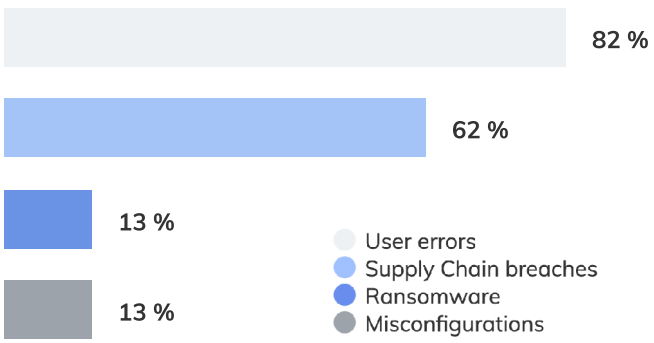
hexnode

# TABLE OF CONTENTS

# 1

# Why does cybersecurity matter? Some stats to ponder over

Cybercrime is on the rise. The continuance of remote work and the introduction of IoT, wearables and other interactive devices helped open up multiple gateways for cyber attacks to break through. It is high time to implement strong cybersecurity measures to protect businesses online.




The rise of cybercrimes is a worrying reality that is being continually emphasized across many stats brought out by industry experts and other infosec organizations. Verizon's DBIR report is an annual publication that analyzes various trends on information security incidents and data breaches. It helps to shed some light on the kind of implementations businesses need to take up to avoid being the next targets for cybercriminals. Some of the key findings of the latest report includes:

- **13%** increase of ransomware attacks.
- Supply chain breaches contributed to **62%** of system intrusion incidents.
- **13%** of data breaches were a result of misconfigurations.
- **82%** of breaches were contributed by user errors.

2

# Identifying recent attack patterns

According to a cyber outlook survey conducted by the World Economic Forum, ransomeware attacks continue to increase at an alarming rate, with 38% of businesses reporting loss of brand reputation as a result of these attacks.


of businesses reported a loss of brand reputation as a result of ransomeware attacks.

With cyber attacks increasing at alarming rates, researches have been made to identify the underlying attack patterns as a mechanism to capture and communicate the attacker's perspective.

Attack patterns are the cumulative results of studies done over a period of time. Incidents of a similar nature are grouped into a single pattern. Since they follow the same threat vector, the controls required to minimize the occurrence of these threats would be the same in most cases.

Some of the recent attack patterns businesses should be wary of include:

## BASIC WEB APPLICATION ATTACKS

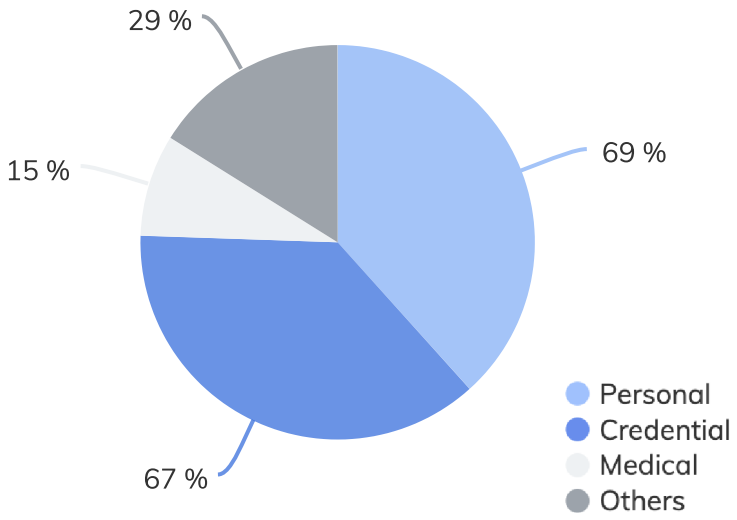
### Types of attacks

- Cross-site scripting
- SQL injection
- Path traversal

### Types of data compromised

- **Frequency:** 4751 incidents
- **Confirmed data disclosure:** 1273

**Source:** Data Breach Investigation Report 2022




## MISCELLANEOUS ERRORS

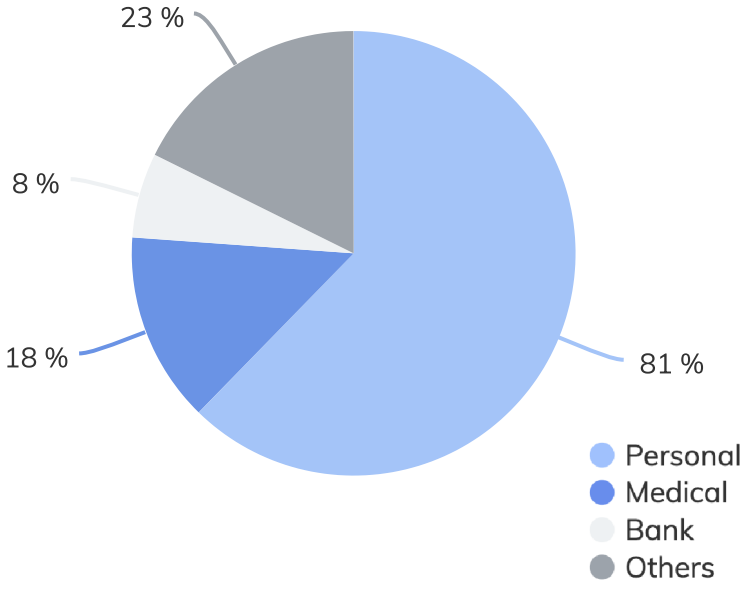
### Types of attacks

- Ransomware attacks
- Man-in-the-middle attacks

### Types of data compromised

- **Frequency:** 715 incidents
- **Confirmed data disclosure:** 708

**Source:** Data Breach Investigation Report 2022



## SOCIAL ENGINEERING

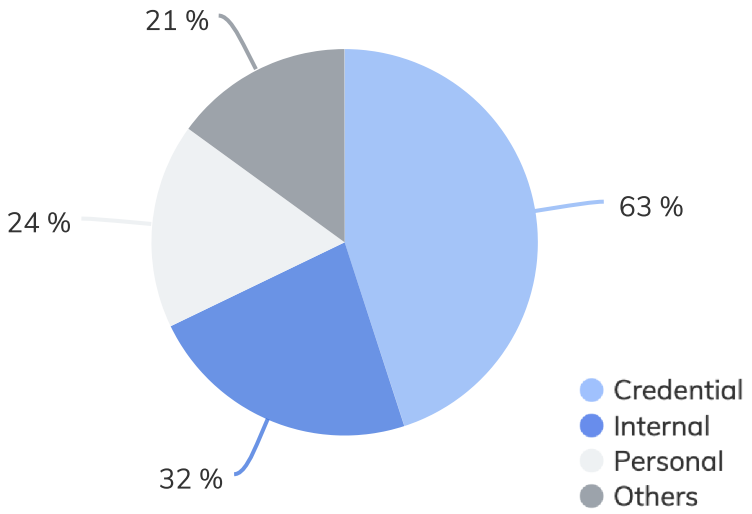
### Types of attacks

- Spear phishing
- Pretexting

### Types of data compromised

- **Frequency:** 2249 incidents
- **Confirmed data disclosure:** 1063

**Source:** Data Breach Investigation Report 2022




## SYSTEM INTRUSION

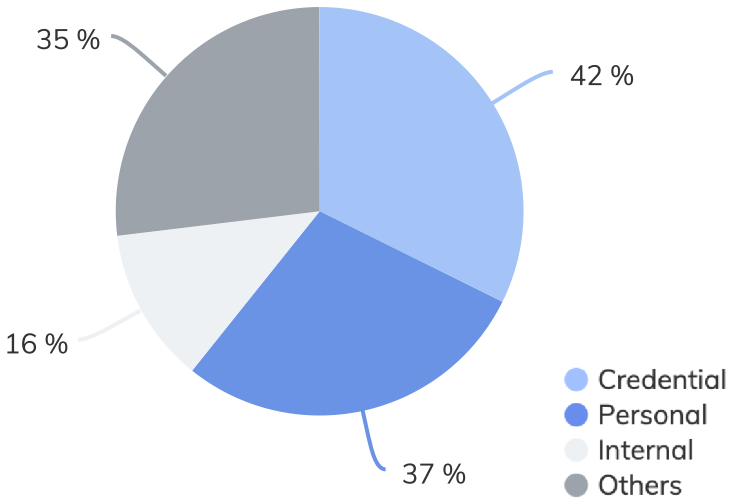
### Types of attacks

- Malware
- Spyware

### Types of data compromised

- **Frequency:** 7013 incidents
- **Confirmed data disclosure:** 1999

**Source:** Data Breach Investigation Report 2022



3

# How to choose the right cyber security framework for your business

A cybersecurity framework is a guideline that defines a set of rules and processes organizations need to follow to minimize or mitigate any risks related to data, devices and any other assets that is a part of the digital world.

Data is being processed and managed on a large scale on a continual basis. Enterprises face 130 cyberattacks per year on an average. One of the biggest challenges of implementing cybersecurity is deciding on the right controls. Usually, these technical controls are specific to the workflows and requirements of the organization. You can rely on a number of tools to achieve that baseline level of security needed to keep your organization's data secure but if that's the case, your entire security foundation would be built upon shaky grounds and that's the last thing you need.

Following a framework that is right for your organization helps you get rid of all the chaos that usually surrounds the implementation of data security. Unfortunately, there is no 'one size fits all' approach for this.

Unfortunately, there is no 'one size fits all' approach for this. Choosing the right framework depends on the current maturity level of your security program. Some of the most commonly followed frameworks are the NIST framework and CIS controls.

## NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Created by the National Institute of Standards and Technology (NIST), this framework sets the guidelines for cybersecurity that can be used across various industries. The NIST framework is split into five core functions. These include:

- Identify
- Protect
- Detect
- Respond
- Recover

These functions help organizations to properly secure information, manage and mitigate various risks, have an ongoing process to properly identify and address threats. It also plays an important role in helping organizations improve their security infrastructure by having corrective actions in place to prevent the reoccurrence of any security incidents or data breaches.

### Identify

This function aims for organizations to have a thorough understanding of their business context and identify other critical assets and functions. It also guides organizations to understand and manage all the risks falling under their scope by performing a risk assessment at the beginning of any project. Some of the processes tied in with this function includes:

- Making a list of all assets
- Understanding the business context of your organization
- Making a list of all applicable risks and assess those to evaluate its impact
- Having processes in place to treat or mitigate those risks

## Protect

This function revolves around implementing adequate technical and administrative safeguards to protect data and critical services within the organization. These include:

- Implementing the right access controls
- Conducting awareness training sessions on a periodic basis
- Ensure data security by having an information classification policy
- Carryout periodic maintenance of all critical assets
- Implement protective technology

## Detect

This function revolves around the ability with which you'll be able to quickly respond to an information security incident determines how mature your security implementations really are. This function guides organizations to have enough documented processes and technical controls in place to detect the presence of a threat before they begin impacting other systems. It aims at the timely discovery of cybersecurity events. The processes included within this function include:

- Detecting various anomalies, events and threats
- Continuously monitor the security implementations of the company
- Implement other detection processes

## Respond

This function aims to implement appropriate processes to adequately respond to the security incidents or data breaches. Responding to the incidents in a timely manner helps to ensure these incidents don't impact other systems even further. The processes of this function include:

- Planning and documenting response activities.
- Maintaining proper communication channels.
- Conduct analysis on a periodic basis to mitigate these incidents in the future.
- Documenting improvements that can be made and integrating it within the daily operations of the organization.

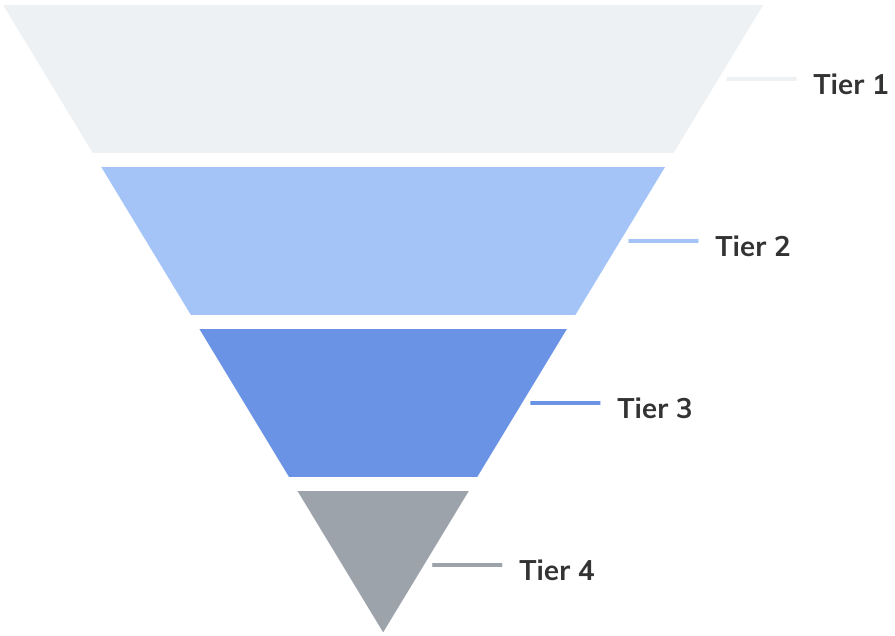
### Recover

This function aims to develop processes to ensure continuity and recovery of critical functions that have been impacted during the event. Various procedures within these functions include:

- Taking backups of all critical data and services.
- Planning and documenting recovery processes and requirements.
- Making improvements.
- Ensuring appropriate communication channels between the IT security team and management.

## NIST FRAMEWORK IMPLEMENTATION TIERS

The NIST framework consists of multiple tiers of implementation. Each of these tiers ties in with the level of security posture of the company.




### Tier 1 (partial)

This tier includes businesses lacking various security processes and limited awareness to cybersecurity. Risk management is conducted at irregular intervals and the business would often lack the resources to establish communication channels to identify, manage and effectively respond to cybersecurity threats.

## Tier 2 (risk informed)

Businesses that fall into this tier understand all the risks they are applicable to and already have processes in place to meet some of the requirements of the regulatory compliances that come under their scope. However, they have policies to address various security issues at an organizational level. They are aware of their cybersecurity needs but lack the capabilities to quickly respond to an event.

## Tier 3 (repeatable)

The risk management processes of the businesses in this tier are well established. The cybersecurity practices have been approved by the management and are capable enough to quickly respond to any threats or vulnerabilities spotted within the systems. The external participation of these organizations is quite high. They regularly get in touch with other entities. They are well grounded on all cyber supply chain risks applicable to their product and services. Employees are assigned specific roles and responsibilities to ensure cybersecurity is integrated to all the daily operations of the businesses.

## Tier 4 (adaptive)

The cybersecurity practices of organizations in this tier are based on their current activities and lessons learned from previous incidents. They continually improve their security implementations to analyze the events and adequately protect the assets accordingly before these events occur or make them adapt to the threats. By maintaining an environment that calls for continual improvement, businesses of this tier would be well adapted to respond to sophisticated cybersecurity threats and improve their security landscape by adopting advanced threat detection technology.

# HOW DOES THE NIST FRAMEWORK HELP YOUR ORGANIZATION?

If your organization falls in either Tier 1 or Tier 2, the best way to begin your cybersecurity implementations is to document all your requirements as security policies and make them available to employees and other required parties.

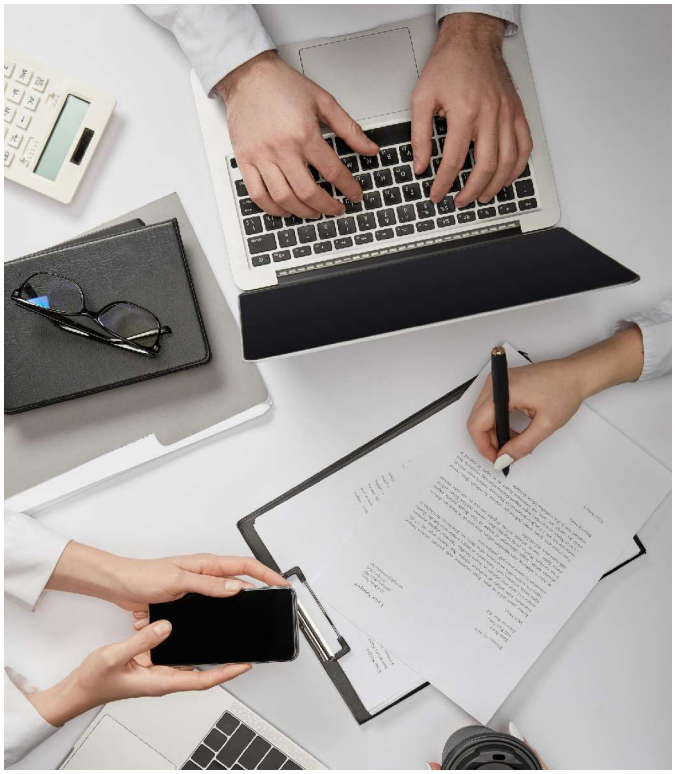
Conducting security awareness trainings at a semi-annual or quarterly basis can be of big help as your employees would have a thorough understanding of the responsibilities they hold in securing the data they work with, this would include deploying strong password policies and making sure all devices are encrypted.

As the security posture of your business improves, you can begin using third-party tools to ensure endpoint security and scan your networks on a continual basis for real time threats. One of the important requirements of NIST is the need to maintain an updated asset inventory. An asset inventory gives your IT team a concrete list of all the assets managed and used by your organization.

The NIST framework further emphasizes on the need to continually monitor all the risks applicable to your organization. Identify all the risks that falls under the scope of your organization and establish enough processes to assess and treat those risks. It would not be possible to treat all the risks you've identified. Such risks should be bought down to an acceptable level to ensure they don't impact your systems any further.

## CENTRE FOR INTERNET SECURITY (CIS)

Organizations that fall under tier 1 and tier 2 of the NIST cybersecurity framework have to build upon a really good foundation to reach the stage in which they can incorporate more advanced technology to detect the presence of threats before they well advance their way into the systems.



The CIS controls often work alongside the NIST framework and provides organizations with a guideline of all the measures and controls they need to take up to advance their way into further levels of the implementation tiers.

Version 8 is the latest version of the CIS controls, where the number of controls has been cut down from 20 to 18.

The controls include:

- Inventory and control of enterprise assets
- Inventory and control of software assets
- Data protection
- Secure configurations of enterprise assets
- Account management
- Access control management
- Continuous vulnerability management
- Audit log management
- Email and web browser protections
- Malware defenses
- Data recovery
- Network infrastructure management
- Network monitoring and defense
- Security awareness and skills sharing
- Service provider management
- Application software security
- Incident response management
- Penetration testing

## HOW DOES CIS CONTROLS HELP YOUR ORGANIZATION?

CIS controls give businesses a more methodical approach to implementing cybersecurity. It is not mandatory to implement all these controls. These controls can be chosen based on the current requirements of your organization and used to strengthen the efficiency of your security program. Grouping the controls into separate implementation groups makes it easier for your team to know the controls they need to prioritize.

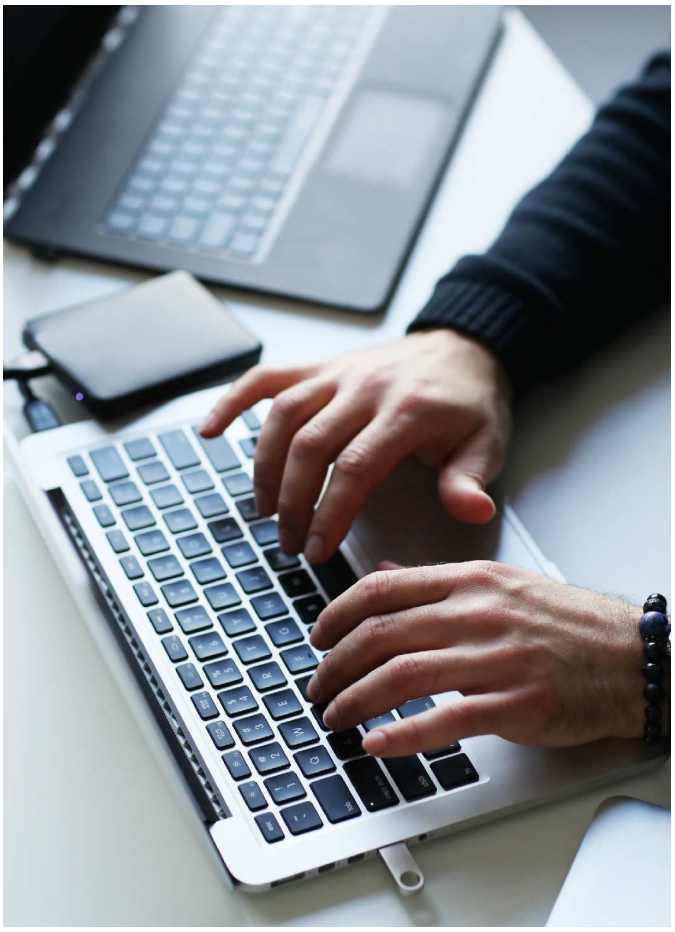
The following controls are used to understand all the people, devices and assets connected to your corporate network and the levels of access they maintain:

- Inventory and control of enterprise assets
- Inventory and control of software assets
- Access control management
- Secure configuration of enterprise assets
- Audit log management

> ***" CIS controls are globally accepted security best practices created and developed by a community of experts from the Center for Internet Security. "***

Then there's a separate set of foundational controls that guides organizations on the various technical controls they need to take up to improve their security. Processes to boost email security, data security and systems are usually defined within the following controls:

- Data protection
- Email and web browser protections
- Malware defenses
- Network infrastructure management
- Network monitoring and defense
- Additional access controls
- Wireless access controls
- Boundary defenses



The remaining controls can be clubbed into best practices to ensure adequate awareness, preparedness and efficient response to an incident:

- Security awareness and skill sharing
- Incident response management
- Penetration testing
- Application software security
- Establish secure coding practices to prevent or rectify the occurrence of any weaknesses

# 4

# Implementing cybersecurity within the organization

Insider threat continues to be one of the leading causes of data security breaches.

According to the latest cost of insider threats global report brought out by Ponemon Institute, 56% of incidents were caused as a result of negligence and the average annual cost taken to rectify it was $6.6 million.

The best way to successfully implement cybersecurity within the organization is to follow its three pillared approach known as the CIA, which looks into maintaining the confidentiality, integrity and availability of the information and services.

**Confidentiality** – this ensures data is only available to concerned parties by limiting access to authorized parties. Access can be restricted by the means of implementing strict access controls. Other ways in which you can ensure the confidentiality of the information is via encryption and deploying strong password policies.

**Integrity** – maintaining data integrity protects the data from unauthorized modification during transmission. These modifications can arise from a number of factors such as human errors, misconfigurations and insider threats.

**Availability** – this component of the CIA triad defines all the processes organizations need to follow to make sure all resources, especially critical ones are made available when required. All recovery processes such as backups and recovery tests need to be carried out to ensure the availability of resources. Establishing effective communication channels in this process is vital as inter departmental dependencies are always required when ensuring the availability of critical services during an outage.

## WHAT SECURITY MEASURES CAN YOU IMPLEMENT WITHIN A COMPANY?

- Create an updated asset inventory listing all the hardware and software assets used and managed within your organization.
- Deploy strong password policies and strict access controls to ensure access to resources are limited to just authorized people.
- Enforce restrictions to make sure devices continue to function in accordance with the security requirements of your organization.
- Conduct security awareness training sessions at periodic intervals.
- Encrypt all devices to ensure data security.
- Create separate work containers on personal devices of employees to prevent the mixing of personal and work-related data.
- Manage applications through the entirety of its lifecycle to improve application security.
- Manage, track and approve all changes happening within the organization.
- Configure network settings to ensure remote users securely access corporate resources.

# ROLE UEM PLAYS IN IMPLEMENTING THESE MEASURES

The enterprise landscape continues to shift rapidly with the continual influx of different kinds of endpoints. UEM offers a centralized platform where a wide variety of endpoints ranging from laptops, desktops, mobile devices, rugged devices and IoT devices can be managed. Managing these devices manually can be a hassle. Pushing the necessary configurations needed to secure these devices can be painstakingly drawn out process. A UEM solution helps in remotely pushing these configurations to individual devices and groups of devices and users.

Security management is a critical aspect of UEM. Its functionalities are centered towards securing endpoints and data from a number of threats and vulnerabilities. Being compliant with a number of regulatory requirements is now a priority for many businesses. Most of the technical controls you need in improving the security infrastructure of your organization can be done with the help of a UEM solution. These include:

## Defining complex password requirements

Weak passwords can be an easy gateway for hackers to hack into your systems. In addition to creating a password policy that is unique to your organization, you can define the level of security your passwords should contain by configuring the values it needs to consist of to make it more complex. Your team can even set the password history and password age to refrain users from following a predictable pattern while setting passwords.

## Set adequate restrictions

By setting additional restrictions such as preventing the copying of sensitive information between normal and work profile and disallowing screenshots helps to ensure the confidentiality of your corporate data.

## Enable encryption on devices harbouring essential data:

Secure critical applications and systems by remotely enabling full disk encryption programs like FileVault and BitLocker.

## Restrict users from accessing unsecure websites

Web filtering helps to prevent employees from accessing websites prone to cyberattacks. This limits your employees from sharing sensitive information online falsely under the pretext of exchanging information with a legitimate party.

## Implement Data Loss Prevention (DLP) policies

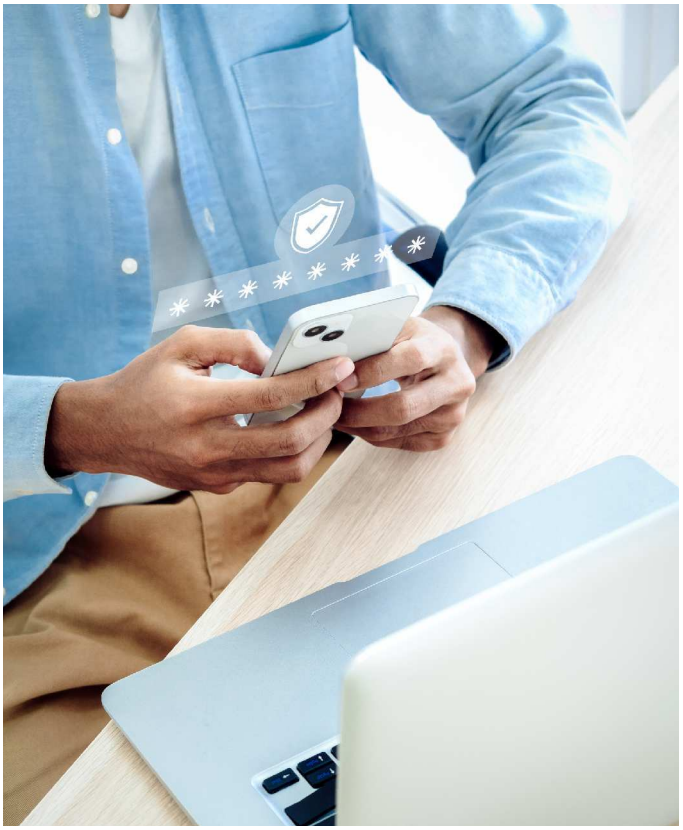
Create encrypted work containers on BYO devices to ensure corporate data stays within the confines of the work profile. Policies can be remotely deployed to the managed devices to ensure managed applications and other important files are not opened from unmanaged sources.

## Ensure app and content security

Pre-configure app permissions and various other settings to make sure they continue to function in alignment with the policies set by your organization.

Create managed app catalogs and assign them to specific users to strengthen your implemented access control measures. You can create enterprise applications of your own and make them available to users within the managed app catalogs.

You can add in an additional layer of security to prevent the sharing of files to unauthorized users by disabling bluetooth, USB and Wi-Fi tethering.



## Secure lost devices

No devices are completely lost if they are managed well. Whenever a user reports a lost device, your team can immediately track its whereabouts by getting real time location updates. You can prevent unauthorized users with malicious intent from accessing the data stored within these devices by initiating remote lock and data wipe on the lost device.

## Regularly update software and OS

Operating on an outdated operating system can leave your systems exposed to a lot of threats and vulnerabilities. Updating your systems and conducting periodic patch updates can fix any of the loopholes hackers may find in burrowing their way into your networks and systems. Admins can update critical applications with any user intervention making the process more streamlined without affecting the productivity of the employees.

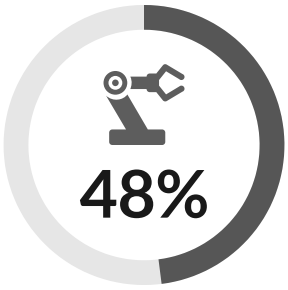
## Detect the presence of jailbroken and rooted devices

Jailbroken and rooted devices can be a security hazard. It gives users unrestricted admin privileges to the device they use. A UEM can detect the presence of these devices and stop them from connecting to your corporate networks.

5

# Looking past the challenges

As the complexity of cyber threats continue to evolve, it's important for businesses to incorporate the use of AI and other third party tools to quickly detect anomalies and efficiently respond to data breaches in real time.




of respondents believe automation and machine learning will help transform cybersecurity

Manually implementing controls and training your staff not only takes up a huge chunk of IT's time but also increases the overall costs of cyber security spendings. Relying on other tools that can easily streamline this process can help decrease IT costs to a great extent. AI and machine learning plays an important role in strengthening your security posture by analyzing and identifying attack patterns from past results.  AI also offers the benefit of processing large amounts of data and predicting the possibility of any threats even before they occur. Moreover, according to a cyber outlook survey conducted by the World Economic Forum, 48% of the respondents believe automation and machine learning will help transform cybersecurity in the near future.



Mitsogo Inc., Unites States (HQ), 111 Pine St #1225,
San Fransisco, CA 94111
Tel: Intl +1-415-636-7555, Fax: Intl +1-415-646-4151