ManageEngine's

Cybersecurity solutions guide

ManageEngine

Table of contents

Introduction to cybersecurity 3
- Why is cybersecurity important? 4
  - Preventing downtime and losses: The business case for cybersecurity 5
  - Avoiding financial penalties: The regulatory need for ensuring data security and privacy 6

What is cybersecurity? 8
- Data security: Keeping the highwaymen at bay 11
- CIA: The foundation of a data security policy 12
- For your eyes only: Data privacy in the cybersecurity context 13

Making cybersecurity work: A closer look at its components 14
- IAM: Managing access and protecting sensitive data 15
- SIEM: Rapid response threat detection and investigation 21
- UEMS: Securing endpoints against vulnerabilities and other threats 27
- Network security: Preventing network downtime and intrusions 32
- Data security: Safeguarding organizational data against breaches 37

Compliance: Staying on the right side of the law with cybersecurity solutions 42
- General Data Protection Regulation (GDPR) 43
- California Consumer Privacy Act (CCPA) 44
- Protection of Personal Information Act (POPIA) 45

Best practices: Guidelines on ensuring comprehensive security coverage 46
- CIS Controls® 47
- Essential Eight Maturity Model 48

Introduction to
Cybersecurity

The widespread adoption of the Internet and advances in communications technology have brought several changes in the way businesses and society operate. Cloud computing, remote work, the Internet of things (IoT) are all powered by the Internet. However, today's technology and its widespread use have opened up organizations to new threats.

Phishing, malware, denial-of-service, and brute-force attacks are just some of the types of cyberattacks organizations across the world face on a regular basis. To protect their people, processes, networks, and data against these threats, organizations need to adopt effective cybersecurity policies and tools.

To do this, it's important to first understand the why, what, and how of cybersecurity.

Why
is cybersecurity important?

Data is the new gold, and just like the highwaymen of the past, cybercriminals are always looking to plunder it. These modern-day thieves come in several varieties, from lone wolves to criminal organizations, and even nation-states. What's more, not all threats are external—insider threats account for 30 percent of all data breaches!*

A lack of focus on cybersecurity makes it easy for these cybercriminals to gain access to an organization's network, devices, or other assets. This access in turn enables them to carry out a variety of attacks against the organization and its partners.

This can damage an organization in a variety of ways, including:

Economic costs: Theft of intellectual property, corporate information, disruption of operations, and the cost of repairing damaged systems.

Reputational costs: Loss of consumer trust and loss of current and future customers to competitors due to unfavorable media coverage.

Regulatory costs: With data breach laws like the GDPR, organizations could get hit with regulatory fines or sanctions in the wake of a cyberattack.

This means implementing security measures is not only good for business, but it's required by law.

*Source: Verizon Data Breach Investigations

Preventing downtime and losses: The business case for cybersecurity

Data, networks, and devices form the backbone of every modern organization. Data is the foundation on which the organization runs, enabling processes and actions, while the organization's network enables its devices to connect and communicate with each other.

Let's take a look at each of these elements and see how an attack on them can impact an organization

Data

An organization's data can be vast and varied, and usually includes several of the following: sensitive customer data like personally identifiable information (PII) and electronic protected health information (ePHI); sensitive business information like customer lists, financial data, trade secrets, and intellectual property; and employee information.

If an attacker manages to leak, tamper with, or prevent access to this data (by encrypting it with a ransomware, for example), it can have severe consequences for an organization and its employees and customers.

Networks

The advent of remote work, IoT, Industry 4.0, and other innovations across fields have made networks more important than ever. The organization's network is what helps employees and customers access the resources they need to carry out day-to-day operations.

Any unplanned downtime in an organization's network can bring its daily operations to a grinding halt, impacting all its users. This can be especially detrimental in sectors like manufacturing where even a few hours of production down time can severely impact the company's revenues.

The ransomware attack on United Health Services (UHS), the attack on Norsk Hydro (among other manufacturers), and the distributed denial-of-service (DDoS) attack on the New Zealand stock exchange are but a few examples of how cyberattacks can impact an organization.

Avoiding financial penalties: The regulatory need for ensuring data security and

Apart from the business case for implementing good cybersecurity practices, there also exist regulatory requirements. Governments across the world have been implementing regulations to curb fraud and protect their citizens' data and privacy on the internet.

Sarbanes-Oxley Act (SOX)

SOX was enacted in 2002 to protect investors and the general public from fraud after the Enron, WorldCom, and Tyco scandals. This includes specific provisions on data security, requiring all publicly traded companies in the United States of America (USA) to develop and implement a comprehensive data security strategy to protect and secure all financial data stored and utilized during normal operations.

General Data Protection Regulation (GDPR)

The GDPR was designed to protect the data of all European Union (EU) residents and applies to any organization that handles the data of EU residents. It requires organizations to ensure lawful, fair, and transparent collection, usage and transfer of personal data. Organizations are only allowed to retain this data when there is a legal reason for it. The GDPR also mandates swift reporting in the event of a data breach.

Payment Card Industry Data Security Standard (PCI DSS)
This standard exists to protect the security of cardholder data and is mandatory to comply with for organizations that process credit card data. The standards consist of several levels. Organizations with greater involvement in processing credit card data need to comply with higher PCI DSS levels. This applies to all merchants, banks, and other vendors.

Health Insurance Portability and Accountability Act (HIPAA)
HIPAA was created to ensure proper protection for individuals' ePHI while ensuring the flow of healthcare information needed to provide quality healthcare information needed to provide quality healthcare. This regulation applies to all hospitals, healthcare providers, insurance companies, and anyone else who processes medical information.

In addition to this we have the **California Consumer Privacy Act (CCPA)**, the **South African Protection of Personal Information Act (POPIA),** and more.

Organizations operating in these sectors and regions need to ensure they comply with these regulations. The cost of non-compliance can be quite high. Take the GDPR for example: severe violations of this regulation can result in fines of up to **€20 million** or 4 percent of the company's annual revenue, whichever is higher.

What is
Cybersecurity?

At a rudimentary level, cybersecurity can be understood as a system of technologies, processes, and practices that protect an organization's networks, devices, and data from attack, tampering, and unauthorized access. People, processes, and technology are the three building blocks of cybersecurity.

People need to be trained and made aware of the cyberthreats they may encounter and the steps and precautions they need to take to protect personal and organizational data and resources.

Processes need to be established to ensure secure storage, handling, and transmission of sensitive information; proper asset management; the integrity of the organizational network; and more. It's also important to have processes in place to mitigate and manage security incidents.

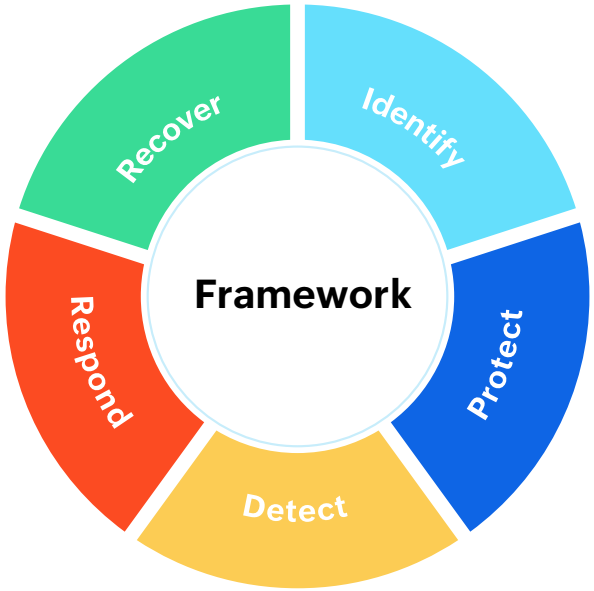
Technology refers to the variety of tools an organization needs to adopt or create to facilitate their people and processes; secure their assets; and detect, react to, and recover from cybersecurity incidents.

Of course, training, creating processes, and adopting technologies cannot happen in a vacuum. Organizations need a foundation on which to build their cybersecurity initiatives.

This is where the NIST Cybersecurity Framework comes in.

Created and maintained by the National Institute of Standards and Technology (NIST) of the USA, this framework lists five major functions that an organization must work towards to ensure effective cybersecurity risk management. It provides clear guidance to help organizations improve on existing cybersecurity practices or create new ones from the ground up.

The functions are organized sequentially to create a security life cycle. Each function informs and supports the next, and an organization must implement all these functions to ensure a complete cybersecurity program. These functions are as follows:



*Source: National Institute of Standards and Technology

Identify

Develop the organizational understanding needed to manage cybersecurity risks to people, data, systems, assets, and capabilities. By understanding the business context, critical resources, and the related cybersecurity risks, organizations can focus and prioritize their risk management strategies.

Protect

Develop and implement appropriate safeguards to ensure the delivery of critical infrastructure services. This function also covers the ability to mitigate the impact of potential cybersecurity events.

Detect

Develop and implement the appropriate activities to recognize the occurrence of cybersecurity events. This is a crucial step in a cybersecurity program: the faster an incident is detected, the faster its effects can be mitigated.

Respond

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. Creating an incident response plan and ensuring compliance with this plan is vital to this step. Security teams must also carry out analysis and mitigation activities to identify and mitigate threats to their organization.

Identify	Asset Management	**ID.AM**
	Business Environment	**ID.BE**
	Governance	**ID.GV**
	Risk Assessment	**ID.RA**
	Risk management Strategy	**ID.RM**
	Supply Chain Risk management	**ID.SC**
Protect	Identity Management and	**PR.AC**
	Awareness and training	**PR.AT**
	Data Security	**PR.DS**
	Information protection processes & procedures	**PR.IP**
	Maintenance	**PR.MA**
	Protective Technology	**PR.PT**
Detect	Anomalies and events	**DE.AE**
	Security Continuous Monitoring	**DE.CM**
	Detecting Processes	**DE.DP**
Respond	Response Planning	**RS.RP**
	Communication	**RS.CO**
	Analysis	**RS.AN**
	Mitigation	**RS.MI**
	Improvements	**RS.IM**
Recover	Recovery Planning	**RC.RP**
	Improvements	**RC.IM**
	Communication	**RC.CO**

*Source: National Institute of Standards and Technology

Recover

Develop and implement the appropriate activities for resilience and to restore any capabilities or services that were impaired due to a security event. The goal of this function is to ensure quick recovery in the wake of a cybersecurity incident. A good recovery program will help minimize the impact of cybersecurity events and help organizations stay on track with their objectives.

Each function is further broken down into various categories, each of which is further broken down into various subcategories.

Without going into too much detail, these categories cover the breadth of cybersecurity objectives for an organization with a focus on business outcomes.

Subcategories are the deepest level of abstraction in this framwork. There are a total of 108 subcategories, each of which is an oucome-driven statement that provides considerations for organizations to create or improve their cybersecurity program. The framework also offers technical references for each subcategory to assist organizations in implementing various cybersecurity requirements.

By being outcome based and not mandating how these objectives must be fulfilled, the NIST framework offers organizations the freedom to customize their cybersecurity programs as per their needs.

Now that we have an understanding of the basics of cybersecurity, let's explore two key aspects: data security and data privacy.

Data security:
Keeping the highwaymen at bay

Data security is a set of standards and technologies deployed to protect data from a variety of dangers, including unauthorized access, accidental loss, corruption, and destruction. It focuses on protecting all types of data (including personal data) from unauthorized access, malicious attacks, and exploitation.

The processes involved in ensuring data security vary from organization to organization based on the data an organization handles.

The confidentiality, integrity, and availability (CIA) triad discussed in the following section provides a good foundation for the planning and creation of data security policies.

Some common data security methods, practices, and processes can include:

Activity monitoring

Network security

Access control

Multi-factor authentication (MFA)

Data encryption

Backup and recovery

CIA: The foundation of a data security policy

The CIA triad, also known as the ultimate goal of information security, is a security model that has been developed to help people think about the various aspects of data security. The CIA triad comprises of three key principles: **C**onfidentiality, **I**ntegrity, and **A**vailability — and unlike its more famous namesake, it has more to do with preventing espionage than carrying it out.

Here's a brief explanation of what these principles stand for and a few examples of cases where they are violated:

Confidentiality

Ensuring that information is not made available or disclosed to unauthorized individuals, entities, or processes. To maintain confidentiality, organizations must implement proper access controls.

Some example violations: Emailing the PII of one customer to another; external attackers gaining access to customer data; sharing confidential company information on public forums

Integrity

Ensuring the accuracy and completeness of data through its life cycle. To maintain the integrity of data, organizations must ensure the security of data in use, in transit, and at rest (storage); restrict edit access to their information to authorized users only; and monitor their data for any unapproved changes.

Some example violations: Unauthorized changes to stored data; corruption of data due to hardware/software errors; defacement of websites.

Availability

Ensuring that information is accessible and usable on demand by authorized entities. To maintain availability of data and other critical assets, organizations must be able to monitor their network, react to anomalies and threats, and quickly recover from a disaster.

Some example violations: Unavailability of a website or service due to DDoS attacks; IT systems being taken offline by malware; unavailability of services due to server failures.

Understanding these principles and how to comply with them can help organizations ensure the security of their data.

For your eyes only: Data privacy in the cybersecurity context

Data privacy refers to the rules and regulations set forth to ensure:

1. Personal and private information is being controlled in line with the preferences of the individual(s) to whom it pertains.

2. Proper handling (processing, storage, and use) of data.

3. Consent was received from the individuals whose data is being stored.

4. Compliance with regulatory obligations.

Building on the general definition of privacy, which refers to an individual's right to freedom from intrusion, prying eyes, and the right to be left alone, data privacy refers to the rights of individuals with respect to their personal information.

In a business context, data privacy concerns often revolve around:

- An organization's handling of personal data throughout its life cycle, from creation to destruction. It also covers aspects such as whether this data is shared with third-parties, and if so, how, for what purpose, and under what circumstances.

- Data minimization and retention — to minimize their attack surface, organizations need to ensure they only collect and retain the information that is needed for their operational and legal requirements, and that they dispose of redundant, obsolete, and unimportant data within a reasonable time frame.

- The application of and continued adherence with governing data privacy regulations like the GDPR, CCPA, POPI, and more.

- Managing contracts and policies for employees, vendors, and customers.

An important point to note here is that data security and privacy, while strongly interconnected, **are not the same.**

It is possible to build systems that are secure but do not provide data privacy. However, one cannot have data privacy without ensuring data security. In other words, **effective data security is a prerequisite for achieving data privacy.**

One way of looking at the relation between data privacy and data security is this: data privacy limits access to information and data security provides the processes and applications for limiting that access. The amalgamation of the two is known as data protection.

Making cybersecurity work: A closer look at its components

Every cybersecurity implementation consists of several solutions that complement each other, helping build a robust security system. Just like each function of the NIST framework contributes and supports the next, eeach cybersecurity solution also plays a critical role in reducing risks and ensuring holistic cybersecurity coverage.

These solutions can be categorized as follows:

1. **Identity and access management (IAM)**
2. **Security information and event management (SIEM)**
3. **Unified endpoint management and security (UEMS)**
4. **Network security**
5. **Data loss prevention**

IAM: Managing access and protecting sensitive data

With the increase in remote users, the use of personal devices, adoption of cloud services, and more, traditional perimeter-based security measures are ineffective. Organizations can no longer afford to operate on the assumption that all users within their network can be trusted. Granting implicit trust to any user weakens an organization's security posture, as this approach fails to account for compromised devices and credentials.

This approach is especially risky in light of the fact that attackers often need to compromise just one device to gain access to an organization's network, and it doesn't have to be a work device — an unsecured personal device on a remote employee's home network may be enough to help attackers breach defenses.

To protect against the evolving risks posed by modern work approaches like bring your own device (BYOD) and cloud solutions, organizations need to adopt a Zero Trust security model.

Zero Trust security consists of three key concepts:

1. **Secure access:** Requiring secure and authenticated access to all resources
2. **Controlling access:** Implementing principles of least privilege and enforcing access control
3. **Inspecting traffic:** Inspecting and logging all activities using data security analytics

Implementing IAM can help organizations fulfill the first two requirements of a Zero Trust model.

IAM refers to a framework of policies, processes, and technology solutions employed by organizations to manage digital identification, authentication, and authorization within their infrastructure. IAM solutions enable IT teams to control and monitor user access to critical assets using methods like role-based access control to ensure that the right users get the right level of access to only the resources they need.

IAM solutions enable organizations to:

- Enforce Zero Trust principles such as the principle of least privilege and just-in-time access.
- Protect sensitive enterprise systems, assets, and information from unauthorized access or use.
- Extend access to information systems across a variety of applications and tools without compromising on security.
- Track and record privileged user sessions for easy audits.
- Ensure compliance with IT mandates.
- And more.

Zero Trust:
A brief explanation

The principle behind Forrester's Zero Trust is quite simple but compelling: trust is not an attribute of location. Enterprises shouldn't trust something simply because it is behind an enterprise firewall. Instead, everything including each user, device, and even the network itself should be considered untrustworthy until proven otherwise.

Data transfer should occur only after trust has been established through strong authentication and authorization. Additionally, analytics, filtering, and logging should be deployed to monitor insider threats continuously.

Three key principles of any Zero Trust implementation are:

- Ensure secure and authenticated access to all resources.
- Adopt the principle of least privilege and enforce policy-based access control.
- Inspect and log all activities using data security analytics.

Learn more

Below are some common IAM use cases with examples showing how ManageEngine solutions can help organizations meet these requirements.

01

An IT admin for a large organization needs to manage account creation for thousands of new users every year. Besides this, they also need to monitor and track all changes made in the Active Directory (AD) environment for thousands of users to maintain control and security.

The IT admin for this institution uses predefined templates in ADManager Plus to create users in bulk with the necessary AD attributes pertaining to their job titles, roles, and departments. The admin can either use the bulk import feature of the product to import user details from a CSV file from the human resource management system or import user details through an ITSM integration to a platform such as ServiceNow or ServiceDesk Plus.

During the appraisal or promotion cycle, at end of the calendar year, or during any other event involving a change in a large number of users' profiles, access requirements, departments, or more, the admin can once again leverage the user management template to modify user profiles in bulk.

Next, the admin uses ADAudit Plus to enable real-time tracking of all changes in the organization's AD environment.

Every change made across multiple sites and domains, including small tweaks, are brought together in easy-to-understand reports and graphs. These reports are grouped by category with individual views for changes made to AD objects, authentication logs, security modifications, and user account manipulation, giving the admin complete insight into their AD environment.

In addition to this, ADAudit Plus also generates real-time alerts when it detects anomalous activities, unauthorized access, changes to sensitive files, and more. This ensures that the admin knows about any critical issues and can take immediate action to mitigate the danger posed by these incidents.

02

An IT admin for a large organization with a distributed mobile workforce needs to reduce their organization's attack surface. To do this, they plan to deactivate dormant and expired accounts, enforce stronger password policies, and purge dormant email distribution lists and excessive mailbox permissions.

To start, the IT admin uses ADManager Plus' built-in reports to find accounts that have been inactive for a certain number of days. The admin can then take action on these accounts directly from the report. Inactive accounts can be disabled and moved to a different organizational unit as needed. Disabled accounts can also be reactivated as needed.

The admin can automate this process by setting simple or elaborate identity life cycle automation rules that can disable user accounts after a certain period of inactivity, delete those that have been disabled for a certain duration, and more.

To protect against password-based attacks, the admin uses ADSelfService Plus to strengthen AD password policies. They import dictionaries into their password policy controls, preventing users from using these terms in their passwords. They also set password pattern controls to prevent users from making common password pattern mistakes.

As an additional layer of security, the admin enables MFA for all users and systems. They also implement single sign-on (SSO) with advanced authenticators (biometrics, RSA SecurID, or more) for enterprise applications to ensure security while providing easy access to their users. Next, the admin enables self-service password reset with MFA authentication to allow users to reset their passwords themselves securely. This frees the help desk from dealing with these time-consuming requests, letting them focus on more critical tasks while ensuring secure password resets.

Finally, to reduce the email attack surface, the admin uses Exchange Reporter Plus' Inactive Distribution Lists report to identify and eliminate inactive distribution lists (DLs). This lowers the chances of users being exposed to spam and reduces the footprint available for attackers to exploit.

03

An IT admin for an organization that handles sensitive data needs to allow secure remote access to external partners and consultants while ensuring privileged credentials are secure. They also need to be able to audit privileged sessions to protect against misuse of privileged access.

The IT admin uses PAM360 to securely store all privileged credentials of both on-premises and cloud infrastructure devices. These credentials are stored in a fully encrypted form (AES-256 encryption) in PAM360's password vault.

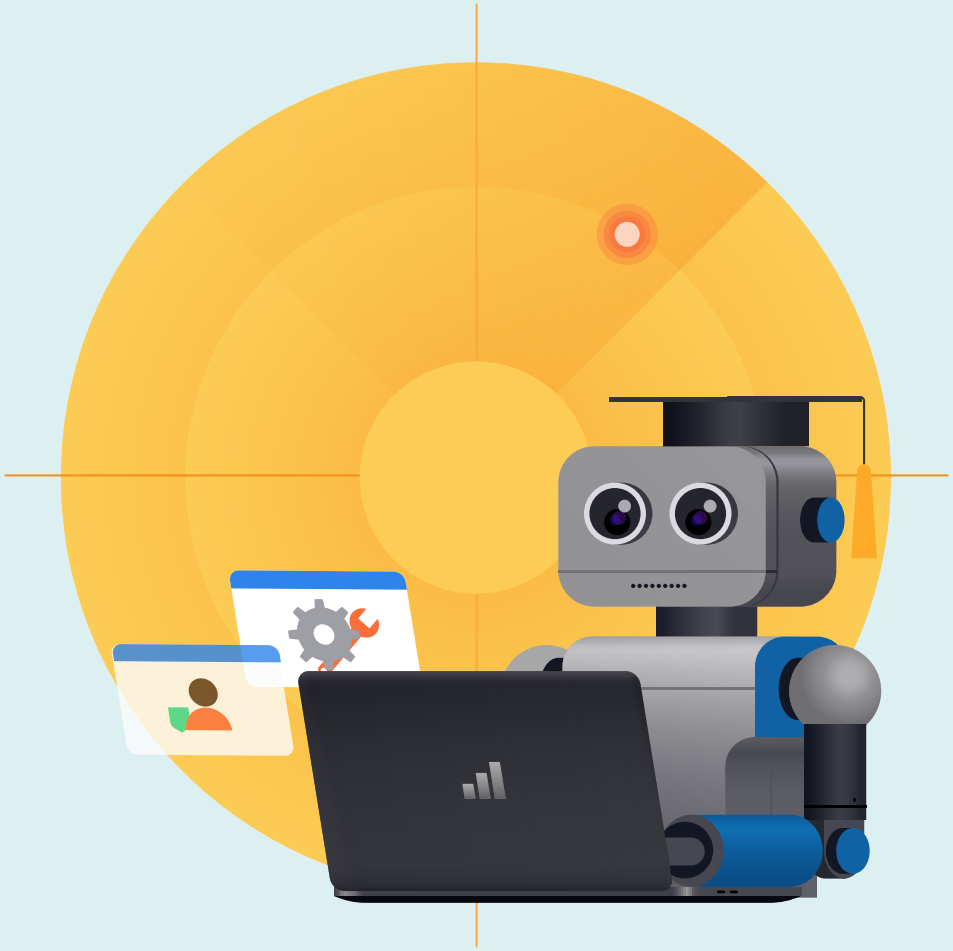
When a partner requires access to these credentials, they log in to PAM360 and request the necessary privileged credentials from the admin. The admin reviews the request and shares the credentials in an encrypted format via PAM360 without revealing them in plaintext. Once the credentials have been shared, the partner can launch a one-click connection to the asset they need to access.

Each privileged session is automatically recorded from start to end. If needed, the admin can use the shadowing option to monitor the session in real time from their desk. The tool also gives the admin the power to terminate a privileged session if needed.

Once the partner checks in the credentials after use, PAM360 automatically resets them. This allows partners to gain access to the resources they need when they need them without compromising on the integrity of these credentials.

The admin can also use PAM360 to designate individual technicians as password administrators, and allow them to add and share passwords with other technicians and end users to streamline the account consolidation process. They can restrict access to passwords based on job roles, which helps establish tight access controls. They can also create request-release workflows, which help enforce an additional layer of control over sensitive passwords.

SIEM: Rapid response threat detection and investigation



Strong network perimeter, endpoint, and access control security measures are key to mitigating and reducing the risk of a cyberattack.

However, with the sheer number of potential attack vectors that exist in today's world, no organization can be made completely secure. Security teams should know that despite their best efforts, their organization may still be breached, so it's important to be prepared for this possibility to ensure complete protection of the organization.

In such cases, the security team needs tools to help them detect and respond to incidents and breaches as swiftly as possible. This is where SIEM solutions can help.

SIEM solutions equip organizations with real-time threat detection using tools like user and entity behavior analytics (UEBA); security orchestration, automation, and response (SOAR) capabilities; forensic analysis; and more, allowing IT teams to rapidly identify and respond to internal and external threats.

These solutions allow security teams to:

- Monitor their entire network infrastructure, including all network devices, systems, and applications in real-time.
- Analyze all network activity, and use SOAR capabilities to detect and defend against a variety of internal and external cyberthreats.
- Get real-time alerts complete with timelines and logs when an incident is detected, and automate the incident response with intuitive, predefined workflows.
- Identify anomalous behavior from users and network entities using UEBA to identify insider threats, account compromise, data exfiltration attempts, and more.
- Detect communication with malicious sources outside your network using threat intelligence.
- Ensure compliance with data privacy regulations and security best practices.

UEBA: A brief explanation

What is UEBA?

UEBA is a system that continuously monitors user and device activity. During the course of normal operations, UEBA learns about each user and device and creates a baseline of regular activities for every user and network entity.

Any activity that deviates from this normal is flagged as an anomaly. IT admins can then investigate the underlying issue and take steps to mitigate the risk. Since AI systems are powered by machine-learning, the more experience a system gains, the more effective it becomes at detecting anomalies.

How does UEBA help with threat detection?

The UEBA system calculates a risk score for each user and entity in the organization after comparing their current actions with their baseline of regular activities. The score can range from 0 (no risk) to 100 (maximum risk). The score can vary based on a variety of factors like the impact of the action, the extent of deviation, frequency of the deviation, and more.

If an IT admin feels a particular user or entity's risk score is too high, they can investigate it further and stop any potential incidents.

Learn more about UEBA

Below are a few use cases with examples showing how ManageEngine's SIEM solution, Log360, can help organizations meet these requirements.

01

An IT admin for an organization that handles high volumes of sensitive information needs to discover and secure all instances of sensitive data within their organization's network. The admin also wishes to protect this data from unauthorized access and transfers.

The IT admin uses Log360 to scan their organizations' systems for PII stored in any device across the network.

Log360's data scanner uses specific keywords, numerical structures, or a combination of both to discover highly sensitive data like credit card numbers, Social Security numbers, names, ages, locations, online identifiers, and more. It also has a range of predefined rules to discover PII, which can be customized based on the organization's requirements. In case the PII the admin needs to scan for is not predefined, they can set the parameters and create their own rule.

Once the data is located, Log360 tracks all activity in the folders containing this sensitive data, and sends alerts to the admin in case of unauthorized access.

In addition to this, Log360's machine learning (ML) algorithms help preempt attack scenarios like data theft by constantly analyzing the behavior of all users and entities in a network. Any deviation from the baseline in terms of time, pattern, or count is registered as an anomaly and a risk score is added.

For instance, if a user copies many files or accesses information they have never accessed before, it will be logged as a pattern anomaly, and a certain risk score will be added. Users with high risk scores will be automatically placed on a watch list and their actions will be closely monitored by the system. This insight can give you the edge you need to stay a step ahead of potential threats inside and outside your network perimeter.

02

The IT admin for an organization wants to protect their organization against compromised systems and accounts. They need to detect these attacks and take immediate action to mitigate the damage.

The IT admin uses Log360 to aggregate the data from intrusion detection systems, intrusion prevention systems, devices, firewalls, and the Active Directory infrastructure.

Log360 analyzes this data in real time and alerts the admin of any possible intrusion attempt immediately. Once an intrusion is detected, the admin can investigate it further based on the source, destination, and severity. The admin can also use Log360 to automate their response to security events with workflows that minimize critical response time during an attack.

When a system is compromised, it often comes under the control of an external command-and-control server. If a system compromise goes undetected at first, another opportunity to spot it is when the infected system attempts to communicate with the external server.

Log360 corroborates data from reputed threat feeds to alert the admin when a system makes multiple attempts to connect to a malicious source. After flagging a malicious source, the system gives the admin additional details such as the reputation score, age, and geolocation of the domain to aid their analysis.

In addition to this, Log360 comes with a UEBA add-on that can detect anomalies in user behavior and spot account compromises. This add-on uses unsupervised ML algorithms to ascertain the normal behavior of users and entities, then detects any deviations or anomalies from that.

The Log360 UEBA add-on detects account compromises by taking into account multiple factors, such as anomalous logins, malicious software installations, and abnormal file changes. The key factors that can indicate possible account compromise are grouped under three categories: Logon Failure Anomalies, Malicious Software Installation, and Other Account Compromise Anomalies.

To help in the investigation of account compromise, Log360 provides the admin a complete timeline of all user activities to discover what occurred and who the culprit was. Its exhaustive reports and the graphical dashboards help the admin investigate a specific event and the associated incident to determine if there was a compromise in a user account.

Apart from account compromises, Log360 can also spot data exfiltration, insider threats, and other advanced persistent threats. The solution's intuitive security analytics dashboard provides admins with the insights on the users and entities with the highest risk scores, behavioral trends, watch-listed users, and more. It also helps them quickly drill down and investigate anomalous events.

03

An IT admin for an organization wants to ensure granular auditing of changes to security controls in their network infrastructure. For this, they need to monitor multiple environments and keep track of any critical changes.

The IT admin uses Log360's exhaustive range of reports to audit critical changes in their Active Directory, Microsoft 365, AWS, and Azure Active Directory in real time. The moment any policy change or modification to users, groups, OUs, computers, Group Policy Objects (GPOs), sites, or FSMO roles is detected, an alert is raised immediately, allowing the admin to react promptly.

To ensure complete protection, the admin sets Log360 to also audit the organization's applications, servers, databases, and network devices for critical changes in security policies.

Log360's built-in analytical dashboard enables the admin to granularly track critical changes in each of these devices. For instance, they can track changes to firewall access control lists (ACLs) and rules for incoming traffic. In applications like SQL, write access is usually restricted to a few privileged users to prevent unauthorized changes to the organization's database.
A user suddenly gaining write access through underhanded means could have serious implications for data security.

Log360's reports and dedicated dashboards can monitor such changes in user privileges and enable admins to react to these immediately.

This ensures that the organization's security controls stay intact, freeing up the admin's time for other critical operations.

UEMS: Securing endpoints against vulnerabilities and other threats

The digital transformation of organizations has led to an exponential growth in the number and variety of connected enterprise endpoints, including computers, smartphones, and even IoT devices. The shift to cloud solutions, remote and hybrid work models, and adoption of policies like BYOD mean that many users expect to be able to access their organizational data and complete their work using any device, from any location, at any time.

IT departments need to provide hassle-free management of both corporate and personal devices. IT administration needs to be location agnostic, provide around-the-clock services, and enable employees to use their own devices for work.

Meanwhile, data security and privacy concerns mean that IT teams need to ensure complete confidentiality of sensitive information on these devices. This is where UEMS solutions come into play.

UEMS solutions enable organizations to provide their users with the freedom to work from anywhere, at anytime without compromising on security or regulatory requirements.

These solutions allow IT teams to:

- Manage, monitor, and secure all their endpoints including smartphones, tablets, laptops, and desktops along with their users, apps, content, and data — all from a central console.
- Enforce IT policies and apply configuration updates while keeping pace with the rapidly increasing number of devices.
- Protect devices against exploits by identifying and deploying patches for high-risk vulnerabilities in operating systems (OSs) and third-party applications.
- Protect device data and reduce the risk of corporate data leakage by using containment technology to compartmentalize work and personal space.
- Provision, back up, and restore entire systems remotely, from the OSs to applications.
- Safeguard against the threat of data loss and malware intrusions through removable devices using trusted device lists, file transfer restrictions, and more.

Below are a few UEMS use cases with examples showing how ManageEngine solutions can help organizations meet these requirements.

01

An IT admin for an organization wants to secure their organization against vulnerabilities. To ensure effective patching, they need to identify the most critical vulnerabilities and patch them on priority. They also need to find a way to protect against vulnerabilities that don't have a direct fix or where a fix may lead to undesirable outcomes.

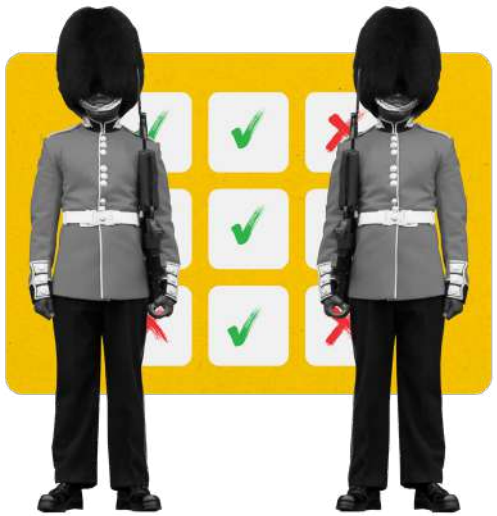
The IT admin uses Vulnerability Manager Plus' risk-based vulnerability assessment capability to prioritize vulnerabilities based on exploitability and impact. The admin can then remediate them across an environment of any size by deploying the latest patches using the built-in patching function.

The admin can also automate and customize the entire cycle of patching, starting with detecting missing patches, downloading them from vendor sites, testing them for stability, and deploying them to all your endpoints irrespective of their whereabouts using Vulnerability Manager Plus' automated patch management capability. This helps them keep Windows, Mac, Linux, and over 350 third-party applications continuously up to date while clearing the IT staff's schedule so they can focus on other critical tasks.

Vulnerability Manager Plus also offers a dedicated view to swiftly identify zero-day or publicly disclosed vulnerabilities and apply work-arounds to mitigate the flaws before fixes arrive. It also keeps the admin updated on the OSs and applications that are or are about to become obsolete, meaning they'll no longer receive patches from the vendor.

With Vulnerability Manager Plus, the admin can create custom groups to isolate high availability servers and exclude less critical patches when scheduling automated patch deployments to them. The admin can also use the decline patch feature to deny problematic patches for production machines until vendors come up with revised versions of these patches.

02



An IT admin keen on minimizing the attack surface needs to restrict application access to users based on their jobs, allowing them to run only what's essential. The admin also needs to ensure users are only given the bare minimum application-level privileges needed.

The IT admin can use Application Control Plus to construct control rules for application access by building a list of trusted and blocked applications and simultaneously mapping them to target user devices. This gives the admin total administrative control over the applications that are run in each and every endpoint.

The admin can use flexibility modes and greylist resolution capabilities to observe and test out policies before laying down hard and fast restrictions.

Once the admin finalizes the array of applications that will be allowed to execute, they can then decide on the privileges on which each of them will run.

Application Control Plus lets the admin establish the principle of least privilege by giving them total control over enterprise-wide privileges and allowing them to grant privileges only when required. Instead of elevating user privileges, Application Control Plus lets admins elevate privileges specific to applications in the necessary end-user devices.

With Application Control Plus' additional just-in-time access feature, any deviations from standard requirements can also be seamlessly incorporated. The admin can fulfil temporary needs without creating permanent policies, and these extra privileges can be configured so that they're automatically revoked after the requirements are satisfied.

03

An IT admin in an organization that handles large volumes of data needs to prevent the unauthorized disclosure of critical information. To do this, the admin has to find all the sensitive data and label it accordingly. Then, they have to ensure that users are only allowed to move sensitive data through specific data transfer mediums and that all others remain blocked to proactively stop leakage or theft.

The admin uses Endpoint DLP Plus to automate the discovery of all sensitive data within endpoints using pre-defined or custom templates. Endpoint DLP Plus sifts through all files stored on organization endpoints, detects data that matches the selected templates, and classifies it as sensitive.

Once sensitive data is found and labeled, admins have to first prevent it from being transferred to unauthorized applications They can utilize Endpoint DLP Plus to mark certain apps as "trusted". Users will be able to transfer sensitive data between trusted apps, but will be prohibited from sharing it with other unverified apps. This keeps sensitive data confined to select locations, making it easier to track. Admins can also choose to have all content originating from specific apps automatically labeled as sensitive.

To control data transfer and prevent leakage via email, browsers, and apps, admins can use Endpoint DLP Plus to specify which domains or email IDs are allowed to send or receive sensitive information. They can also restrict the web domains, browsers, and cloud apps to which sensitive information can be uploaded.

Endpoint DLP Plus or Device Control Plus can be used to limit which peripheral devices can access sensitive information by marking specific devices as "trusted". All other devices are blocked by default. Trusted devices can be given varying levels of data access based on the employee's role. When granting copy permission to a device, admins can restrict the type and size of files that can be copied. For documents that need to be printed, admins can limit which printers are allowed to print sensitive files and ensure all printed documents are watermarked.

These tools are equipped with a self-service portal. Employees can use this to report false positives, or request policy exemptions. Third-party users, like consultants, can ask for temporary device access through the Endpoint DLP Plus self-service portal. Admins can review these requests and grant permissions and exemptions as needed.

Network security: Preventing network downtime and intrusions

Networks are the backbones of any modern organization's operations. They support a wide range of critical daily activities including information sharing, production activities (for example, controlling assembly lines in manufacturing plants), customer transactions, communication with vendors, and more. These are even more important in a remote work scenario, where employees don't have physical access to mission-critical files or systems and the network is the only means of getting their job done.

Apart from these internal considerations, there's also the case of the new age customer — advances in technology mean that this customer now expects the information and services they need to be available whenever they want them. They seek reliability from their service providers, and a robust organizational network plays a key role in providing them the reliability they seek.

The compromise of an organizations' network can also expose sensitive information including PII, ePHI, transaction information, intellectual property, and more to malicious actors. Besides this, any unplanned downtime in an organization's network can disrupt its daily operations, preventing customers and employees alike from accessing the services they need. This can harm an organization's reputation, affect their bottom line, and even lead to regulatory action. This is why it's vital that organizations work to ensure integrity and uninterrupted availability of their corporate networks.

Network security solutions enable organizations to detect common attacks and intrusions, protect the network against them, and ensure

They equip IT teams with the ability to:

- Continuously monitor the network security infrastructure and help identify internal and external threats.
- Analyze firewall security and traffic logs for anomalous events.
- Track configuration changes made to the network and network security devices.
- Discover and configure devices in the network from a centralized console, and automate the life cycle of device configuration management.
- Automate network configuration backups, and quickly restore these configurations when needed to make the network disaster-proof.
- Restrict access to network controls with role-based access control, secure the network with easy firmware updates to protect against vulnerabilities, and more.
- Perform network behavior analysis for real-time threat detection and network surveillance.
- Detect and get instant alerts on rogue device intrusions in the network and block unauthorized access.

Below are a few use cases with examples showing how ManageEngine's Network security solutions can help organizations meet these requirements.

01

The security admin wants to continuously track network usage and prevent internal threats in their organization. They also need to be alerted about any security and traffic anomalies in real time.

The security admin uses Firewall Analyzer's log analysis capability to monitor the Internet usage of all employees both within the network and outside of it connecting through a VPN. The admin can easily schedule log reports on a periodic basis and send them to the management team. Security admins can also set alert triggers for both traffic and security events, and get notified when any set metric with a trigger alert is exceeded.

Next, the admin uses NetFlow Analyzer's Advanced Security Analytics Module (ASAM) to perform in-depth network behavior analysis. This network-flow-based security analytics and anomaly detection tool helps in detecting zero-day network intrusions, DDoS attacks, and suspicious traffic using the state-of-the-art Continuous Stream Mining Engine™ technology and by classifying the intrusions to tackle network security threats in real time.

The ASAM offers continuous overall assessment of network security with actionable intelligence to detect a broad spectrum of external and internal security threats. NetFlow Analyzer also has a set of predefined algorithms and thresholds based on which security attacks and events are classified. These existing criteria can be customized to create alert profiles that will notify you via email and SMS every time there's a violation.

Finally, the admin also uses OpUtils' Rogue Detection feature to continually scan and list all the newly discovered and unmanaged devices in the network. OpUtils enables the admin to verify and mark these devices as rogue in the case of unauthorized devices. By combining its capabilities with those of the Switch Port Mapper, it displays the port to which the rogue device has connected. These endpoints can be blocked or unblocked within OpUtils.

02

The IT admin wants to keep track of all configuration changes made to the devices in the network ecosystem and get notified on the changes made. Apart from this, they also want to manage device configurations from a central location.

The IT admin uses Network Configuration Manager's change management capabilities to manage and instantly get notified of all configuration changes in their network devices. What's more, the IT admin can set up user roles using the solution's role-based access control capability to restrict access to devices. Using this feature, the admin can ensure that network operators and users can access only devices that are necessary for their work, thereby preventing unauthorized changes being made to network configurations.

The IT admin can also manage network configurations from a remote location using the tool's configuration backup capabilities. This helps them build a repository of configuration backups, which they can use to revert configuration errors and prevent network outages.

Next, the admin uses Firewall Analyzer's change management capabilities to track configuration changes made to the firewall. Additionally, Firewall Analyzer's configuration change management reports help find who made what changes to the firewall configuration, when, and why. Finally, admins can also schedule configuration backups for their firewalls to help with disaster recovery.

03

The IT admin wants to check for various compliance mandates for both network and network security devices.

The IT admin and the compliance team can readily check their network configurations for compliance with internal and industry standards using Network Configuration Manager. The solution comes with built-in policies for standards like PCI DSS, SOX, Cisco IOS, and HIPAA. The IT admin can create custom policies for internal purposes and instantly generate all compliance check reports. The IT admin can even fix compliance violations using configuration script templates.

Next, the admin can easily adhere to various security mandates by running compliance checks using out-of-the-box compliance reports generated by Firewall Analyzer. The solution comes with built-in security standards for PCI DSS, ISO 27001, SANS, NIST, NERC CIP, SOX, HIPAA, and the GDPR. Finally, the admin performs security audits and identifies configuration loopholes in their firewall.

Data security: Safeguarding organizational data against breaches

Data is the foundation on which organizations operate. Whether it affects customer information, trade secrets, or other sensitive data, a data breach can cause a lot of harm to an organization. Breaches can damage organizations' reputations and lead to major financial losses (as per a Ponemon Institute report, the average total cost of a data breach is 3.86 million US dollars).

Data breaches can be the result of a variety of things ranging from failure to store and secure data properly to social engineering attacks like phishing. This is why it's vital that organizations safeguard themselves against every possible threat using a comprehensive data security solution.

Data security solutions enable organizations to ensure the confidentiality, integrity, and availability of their data at all times.

They equip data security teams with the ability to:

- Identify and classify files containing PII, PCI, ePHI, IPs, and other sensitive organizational information.
- Gain complete visibility into their storage environment with insights on file permissions and security for sensitive files; disk space usage; redundant, obsolete, and trivial (ROT) files; and more.
- Ensure the integrity of information by monitoring all critical files, folders, and shares in real-time, and receive instant alerts on any unauthorized access or changes in sensitive files.
- Detect ransomware intrusions and other threats, and automate instant responses to protect data.
- Prevent the unauthorized transfer of sensitive files via email, external storage devices, printers, web applications, and more.

Below are a few data security use cases with examples showing how ManageEngine's solution can help organizations meet these requirements.

01

An IT admin wants to gain complete visibility into their storage ecosystem to optimize storage and identify potential security issues in their file permissions.

The IT admin uses DataSecurity Plus' file analysis capability to analyze their storage ecosystem.

The tool examines file permissions throughout the organization's storage environment to detect security vulnerabilities like broken inheritances and files owned by dormant users. It also detects and alerts the admin about files with excessive permissions such as those accessible by every user or those allowing unrestricted access. As an additional security measure, the tool also tracks harmful ransomware-infected files using a predefined library of over 50 ransomware file types to help eliminate them from the organization's file servers.

02

The IT admin wants to audit all file activity in their storage environment.

To track all file activity, the admin uses DataSecurity Plus' built-in file auditing feature to gain real-time insight into all file activity in their storage environment.

The tool tracks all activities (read, write, copy, delete, move) to give the admin insight into all user activities. It alerts the admin to critical events such as unauthorized or unusual file changes, file modifications after business hours, user activity in sensitive files, multiple failed access attempts, and more. The admin can create custom scripts for each of these scenarios to automatically shut down an attack. It also allows them to generate reports to check compliance with various IT regulations like the GDPR, PCI DSS, HIPAA, and more.

03

The IT admin believes there is a credible risk of data leak from internal sources. They want to protect against this and prevent data theft from disgruntled or malicious employees.

The admin uses DataSecurity Plus to classify files based on their sensitivity as Public, Internal, Confidential, or Restricted. They then set restrictions on copying and sharing sensitive files (files marked as Internal, Confidential, or Restricted) over email, web applications, or external storage media.

These restrictions can range from using prompts to educate users on organization policies on copying and sharing sensitive data to completely disabling the ability for users to copy sensitive files to external storage media or attach them in emails. Users who attempt either of these will be unable to carry out this operation and will be shown a warning message instead.

The admin can also create custom scripts to handle critical data usage policy violations by automatically taking a number of actions, including deleting or quarantining files and blocking file transfers.

Compliance: Staying on the right side of the law with cybersecurity solutions

As discussed in the introduction to this guide, there exists a regulatory requirement for organizations to implement strong cybersecurity programs. Governments across the world are enacting legislation to protect the privacy of their citizens in the digital space. Failure to comply with these regulations can lead to stiff fines for offending organizations.

This brings us to yet another point discussed earlier in this guide: data security is a prerequisite for data privacy. You can't have data privacy without first ensuring data security. This means, to ensure the privacy of their users' personal information and other sensitive data, an organization must implement a strong cybersecurity program.

One thing to remember is that each privacy regulation has complex requirements. No single solution can address all the requirements of every regulation. However, with the right processes and tools, any organization can make complying with these regulations easier.

At ManageEngine, our goal is to simplify IT for our customers. That's why we've created helpful guides on how organizations can use our solutions to simplify compliance with key requirements of major privacy regulations.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) was designed to protect the protect the data of all European Union (EU) residents and applies to any organization that handles the data of EU residents.

Complying with the GDPR will benefit organizations by simplifying their processes and applications. Unifying all their data repositories and having a clear understanding of the types and purposes of data collection will help organizations easily facilitate data access and modification requests, which will lead to enhanced security.

In addition to this, compliance will show the organization's customers that they take data privacy seriously, offering them a competitive edge in an increasingly privacy-focused world.

On a financial note, GDPR violations can lead to fines of up to 20 million euros or 4 percent of the organization's total global turnover of the preceding fiscal year, whichever is higher.

So what role does IT play in this? With 40 articles to follow, complying with the GDPR is a multi-step process, and many of its requirements are long and complex. While there is no single solution that can address the entire regulation, there are many compliance requirements in the GDPR that can be simplified with the right IT tools.

Visit our GDPR solutions page to take a look at some of the GDPR's articles and how our solutions can help you satisfy those requirements.

Explore our GDPR solutions

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) went into effect on January 1, 2020. It aims to empower Californian consumers with the privacy rights they need to take back control of their personal information.

Companies don't have to be based in California or have a physical presence there to fall under the law. They don't even have to be based in the United States. The CCPA is applicable to a company if it collects or processes data of California residents and falls into at least one of the following three categories:

- Has annual gross revenues in excess of $25 million
- Possesses the personal information of 50,000 or more consumers, households, or devices
- Earns more than half of its annual revenue from selling consumers' personal information

To give power back to the consumers, the CCPA guarantees ten basic rights to all California residents including the right to know all personal data collected, the right to say no to the sale of their information, the right to sue companies in the event of a data breach, and more.

The CCPA's requirements may seem confusing or daunting at first, but the right solutions and configurations can greatly simplify an organization's compliance journey. As with any of these regulations, there is no single solution that can address the entirety of its requirements. However, there are many stipulations in the CCPA that can be made easier with the right processes and IT tools.

Visit our CCPA solutions page to take a look at some of the CCPA's requirements and how our solutions can help you satisfy them.

Explore our CCPA solutions

Protection of Personal Information Act (POPIA)

The POPIA is a regulatory mandate aimed at safeguarding the PII of South African citizens. It provides conditions for the lawful collection and processing of personal data of the citizens by all public and private organizations residing both in and outside the Republic of South Africa.

POPIA compliance requires protecting the PII of employees, vendors, suppliers, and partners in addition to customer data. POPIA defines personal information as religious beliefs; race; gender; ethnic origin; medical, financial, educational, or criminal records; trade union membership; political persuasion, and more.

Complying with POPIA will help organizations improve their reputation, gain a competitive advantage through customer trust, and even enhance their security - the measures taken for POPIA compliance can act as a stepping stone to comprehensive protection against data breaches. Failure to comply, on the other hand, can result in either imprisonment of up to 10 years, a fine of up to R10 million, or both.

POPIA can be broadly categorized into eight conditions. The requirements for these conditions are vast, and they might seem complex and baffling. Adherence to these conditions requires a combination of strict organizational policies and technical measures to be in place. By adopting the right processes and IT products, POPIA compliance can be made a lot easier.

ManageEngine has a comprehensive suite of IT management solutions to help organizations comply with the data security, documentation, and audit requirements of POPIA. Visit our POPIA solutions page to see how we can help your organization comply.

Explore our POPIA solutions

Best practices: Guidelines on ensuring comprehensive security coverage

Cybersecurity is a vast field and finding solutions to each potential threat and issue can be a daunting task. To simplify this process, various organizations have released frameworks and guidelines that simplify the process of ensuring cybersecurity by offering organizations a systematic checklist of process to follow.

The NIST Cybersecurity Framework is one example. There are also other guidelines like the Critical Security Controls created by the Center for Internet Security® (CIS), the Essential Eight Maturity Model developed by the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), and more.

Implementing these models can help organizations develop a solid foundation to build their security program on.

To make the implementation of these frameworks easier, we've created helpful guides that walk readers through the recommendations of each model and list the ManageEngine products that can help them meet these requirements.

CIS Controls®

CIS Critical Security Controls are a prescriptive, prioritized set of cybersecurity best practices and defensive actions that can help prevent the most pervasive and dangerous attacks and support compliance in a multi-framework era. These actionable best practices for cyberdefense are formulated by a group of IT experts using the information gathered from actual attacks and their effective defenses.

Implementing CIS Critical Security Controls can help organizations develop a foundation for their information security program and a framework for their security strategy. It ensures that they follow a risk-management approach to cybersecurity with proven real-world effectiveness. As an bonus, implementing these controls makes it easy for organizations to comply with other frameworks and regulations, including the NIST Cybersecurity Framework.

CIS Critical Security Controls comprises a set of 20 cyberdefense recommendations surrounding organizational security and split into three distinct categories: basic, foundational, and organizational. Each of these categories and the 20 CIS Controls in them are further divided into Sub-Controls. In addition to the basic, foundational, and organizational controls, the controls are prioritized by Implementation Groups (IGs).

Each IG identifies which Sub-Controls are reasonable for an organization to implement based on their risk profile and their available resources.

ManageEngine's suite of IT management solutions can help organizations meet the discrete CIS Control requirements, helping them carefully plan and develop a best-in-class security program to achieve better cyberhygiene.

Visit our CIS Controls page to learn more about CIS Critical Security Controls and how we can help your organization implement them.

Learn more

Essential Eight Maturity Model

The Essential Eight maturity model is a set of strategies developed by the ACSC to help organizations mitigate common attack vectors. The Essential Eight is divided into three main objectives, which are then further divided into eight strategies.

Preventing malware attacks

- Controlling application
- Patching applications
- Hardening user applications

Configuring Microsoft Office macro settings

- Limiting the extent of cybersecurity incidents
- Restricting administrative privileges
- Implementing MFA
- Patching OSs

Recovering data and system availability

- Taking daily backups

Organizations can determine the maturity of their cybersecurity approach based on three maturity levels that have been defined for each mitigation strategy mentioned above. The maturity levels are defined as:

1. **Maturity Level One:** Partly aligned with the intent of the mitigation strategy
2. **Maturity Level Two:** Mostly aligned with the intent of the mitigation strategy
3. **Maturity Level Three:** Fully aligned with the intent of the mitigation strategy

The right solutions and configurations can greatly simplify the process of reaching the highest maturity level. Although there is no single solution that can address all the strategies an organization needs to implement, the right combination of processes and IT tools can make reaching Maturity Level Three easy.

Visit our Essential Eight solutions page to learn more about the model, how our solutions can help organizations meet its requirements, and how to achieve Maturity Level Three.

Learn more

About ManageEngine

ManageEngine crafts the industry's broadest suite of IT management software. We have everthing you need — more than 120 products and free tools — to manage all of your IT operations, from networks and servers to applications, service desk, Active Directory, security, desktops, and mobile devices.

Since 2002, IT teams like yours have turned to us for affordable, feature-rich software that's easy to use. You can find our on-premises and cloud solutions powering the IT of over 280,000 companies around the world, including nine of every ten Fortune 100 companies.

As you prepare for the IT management challenges ahead, we'll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers.

And as a division of ZohoCorporation, we'll continue pushing for the tight business-IT alignment you'll need to seize opportunities in the future.

ManageEngine

www.manageengine.com

ManageEngine ManageEngine ManageEngine