ManageEngine's blueprint for endpoint management and a future-ready workforce

Featuring:

- Our endpoint journey: The before-after story of our endpoint management strategy
- A modern blueprint for future-ready endpoint management
- Integrating management with security to handle our device fleet effectively
- How our IT teams are improving employee experiences during the new normal

Glossary of terms

BYOD	Bring Your Own Device
CCPA	California Consumer Privacy Act
COBO	Company Owned/Business Only
COPE	Company Owned/Personally Enabled
COSU	Company Owned/Single Use
CYOD	Choose Your Own Device
EMM	Enterprise mobility management
GDPR	General Data Protection Regulation
ITSM	IT service management
MDM	Mobile device management
PDPA	Personal Data Protection Act
UEM	Unified endpoint management

What's inside?

Introduction

The 2000s can be called the decade of change. A lot happened in ten years. The world population crossed six billion, America saw its first African American president, and Bill Gates was the richest man alive for eight years. Most importantly, the 2000s also gave us the biggest tech change in our lifetime: the smartphone boom.

In 2009, Intel formally introduced a BYOD policy after a significant rise in employees bringing their own smartphones and laptops and connecting them to the corporate network. This revolutionized the workplace. Over a decade later, smartphones are now irreplaceable. Businesses are scrambling to find a system that allows personal devices and corporate information to coexist.

With remote work becoming the new norm, the road map for digital transformation is solely dependent on the choices we make now. Endpoint management has helped millions across the globe create a limitless workplace, covering every aspect of device management from PCs to smartphones. However, is it enough? How do you know if the measures you're taking can protect your organization from future risks? Technology is growing faster than we can handle it. How do you keep up with the changes and provide your brand with an ecosystem in which it can thrive?

Why do you need this e-book?

A recent survey by Deloitte revealed that companies spend about 10 percent of their IT budget on cybersecurity. But does higher spending always mean a better cybersecurity maturity level?

Let's say you're going skydiving. You're all strapped up and ready to go. Just as you're about to jump, the instructor tells you there's a 95 percent chance the parachute will work. Would you still jump out of the airplane? Would you leave that five percent to fate? Device management isn't all that different. One small opportunity is all it takes to destroy years of effort.

Poor device management spares no one. It affects everyone from the CEO to tech support. As an organization, you have a lot at stake and not much room for error. Each year, companies lose millions to data breach lawsuits. This kind of crisis can be easily averted if you're proactive in your efforts to manage employee devices. With the global launch of 5G paving the way for next-gen technology, you need to be prepared, if not one step ahead, with your endpoint strategy.

If you're reading this, chances are you're looking for a better endpoint system for your business. This e-book covers ManageEngine's path to discovering the right device management plan—our achievements, mishaps, and everything in between. We'll talk about the evolution of device management, the rise of BYOD, some real-life scenarios, and how we navigated through uncharted waters in the wake of COVID-19. We'll also briefly discuss the future of mobility. Let's dive in!

Chapter 01

Our journey so far

Doing things our way

There's a saying that goes "It takes a wise man to learn from his mistakes, but an even wiser man to learn from others." Organizations spend years on market analysis, assessing trends, competition, risks, and opportunities before jumping into the market. ManageEngine isn't any different.

Instead of diving in headfirst trying to be the first of our kind, we learned from others' mistakes and meticulously tested our products in-house before their release. Playing it safe? Maybe. Nevertheless, the most secured plans come with a set of challenges. We started out with basic client management tools, moved to MDM, and finally created a comprehensive UEM system. During this period, we changed plans, locations, and even our name! It took years to reach where we are today, and we're nowhere near done. We are constantly trying to accommodate every need and create a holistic product that gives us exactly what we're looking for. We're trying to redefine management.

Why did we do that? Did it work?

ManageEngine's device management through the years

1996
Adventnet inc.

Where it all began

COBO devices are used. Sysadmins monitor inventory and update systems individually.

2006
CMT

Beginning of client management tools

BYOD starts gaining popularity. client management tools, including MDM, help maintain inventory, update devices and monitor hardware and software purchases.

2015
ManageEngine's strategy

The rise of endpoint management

The smartphone becomes a workplace staple. ManageEngine enforces a COPE device strategy. EMM envolves from MDM to monitor the surge in number of smartphones.

2018
Pillars of security

Evolution of UEM

A combination of client management tools and EMM is used to monitor COPE devices. Uniform updates applied on all systems and endpoint security increases overall.

2020
Covid-19

Modern management and beyond

COVID-19 accelerates remote work. We switch to cloud-based management to enable business continuity. Remote access tools created to ensure employees can access information surely from any location.

Mistakes, losses, and a whole lot of repairs

Poor device management structure is your Achilles' heel. In spite of your overall strength, your business functions can collapse if you're unable to make sense of your management strategy. At ManageEngine, external devices were not a cause for concern up until about five years ago. Most employees used COBO devices so we didn't focus on creating a device management plan. With the introduction of BYOD, devices became smaller and smarter, people took their work on the go, and security threats were larger than ever.

The biggest problem with a BYOD system is the lack of security. Employees might use unsecured Wi-Fi or mobile data, which leaves them vulnerable to attacks. If an employee loses their device, you've lost valuable, confidential information. That's a lawsuit waiting to happen! Malware, compatibility issues, support costs, you name it—there are so many hurdles. One misstep can cause thousands of dollars in damages or worse, loss of trust and reputation. There's nothing worse than losing a customer's faith in your brand. Like they say, trust takes years to build and seconds to destroy.

We faced a number of challenges like:

- Unauthorized usage of apps and data sharing: Employees would often download apps that were not verified or approved by the company, and there was no way for us to monitor that. This also includes the use of hardware such as USBs to share information.
- Unknown devices entering the corporate network: Following a "trust but verify" system does reduce the risk of attacks, but it does not eliminate threats altogether.
- Device disparity: Corporate devices are usually procured from a predetermined list of original equipment manufacturers (OEMs). This usually consists of two to three vendors. In a BYOD setup, we had to be able to accommodate a wide variety of devices and ensure our applications were compatible with all of them. This removed the element of uniformity we craved.
- Difficulty in troubleshooting remotely
- Inability to deploy software and updates at once: Having to do it manually took up too much time, costing us valuable man-hours.
- Failure to conduct a remote wipe when an employee's device was missing
- Most importantly, we did not have a centralized way to monitor activities. How would we know if we were compliant with data protection laws? Was customer information secure?

While these problems are neither unique nor universal, minimal device control and operational inefficiency definitely kept our Sysadmin team (and Legal and Compliance!) on their feet at all times. It started to look more like a never-ending battle with minor issues. Surely there had to be a better way to tackle this.

Next, we discussed requirements and strategy. When an employee walks out the door with sensitive information, it's important to have an airtight device management plan in place. Once we saw a steady rise in device numbers, we decided to create a customized plan that worked for us. First we had to ask ourselves, *What are we trying to fix? What are our goals?* We came up with a list of requirements that would make device management easier.

Our plan should facilitate:

- Access control for deployment.
- Patch management.
- Automated processes to reduce admin workload.
- Remote access to devices.
- Restricted access—controlled admin privileges.
- Controlled use of external hardware (USBs).
- Power management.
- App restrictions and app blocklisting.
- Desktop and mobile integration.
- Geotracking for managed devices.

We picked company-issued devices to promote uniformity and cut down on operational costs in the long run. Now, how do we manage the devices? By creating a product that meets all our expectations. UEM with MDM as a built-in feature was the obvious choice. It gives us control over all our endpoints. We can monitor and carry out tasks almost effortlessly, not to mention the hours saved. For example, with endpoint management, IT admins get enrollment done in a third the time it would take to individually enroll devices. OS updates, which would usually be a week-long task, now only take a fraction of the time. A tool that we found to be particularly useful was Wake on LAN, which allowed us to schedule booting of Windows systems in the network remotely.

Finally, damage control. Devices go missing from time to time. When the inevitable occurs, we need a safety net. If an incident involving an end user occurs, it's mandatory to file a report at the nearest police station. This is for any lost or stolen device at that particular location. The Sysadmin team issues a remote wipe, and records are updated accordingly. Our end goal during these circumstances is to be able to say "We've got it covered."

Why now?

When we first started out, we had our endpoint management system with an integrated MDM module. But as BYOD's undeniable popularity increased, it became evident that we were going to need a separate system to monitor gadgets, smartphones in particular. And we weren't the only ones who saw the BYOD boom. Major players in the cloud software market, like VMware and SOTI, created their own systems. By 2012, there was an emerging market for MDM. In 2015, we released MDM as a separate product for customers and implemented that same solution within our organization.

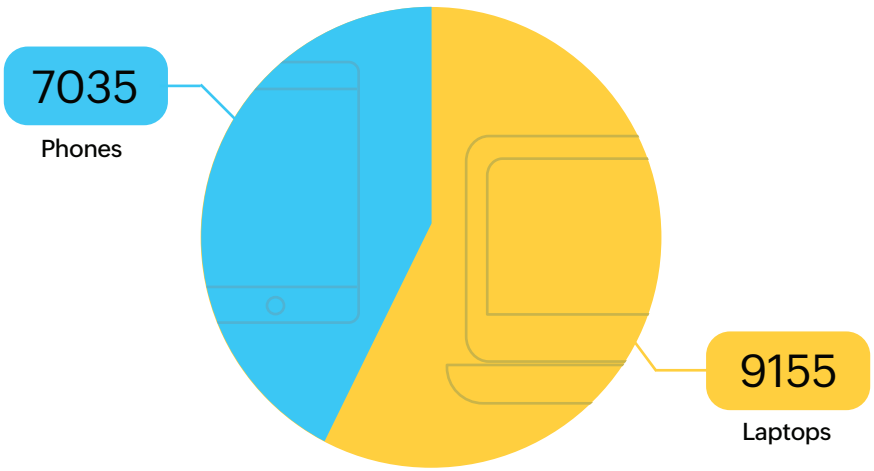
MDM enhances network security and provides a centralized platform, especially for MSPs with a large number of devices. The ease of management using MDM is also what pushed us to consider COPE instead of BYOD. Having an in-house device management application, it just made sense to go with company-issued devices. We never have to worry about increasing costs to outsource device management or periodic renewals, and it's far easier to push apps and updates to devices.

The steep rise of BYOD led to yet another step in endpoint evolution: EMM. Enterprise management solutions help secure corporate data while providing employees the flexibility of using their personal devices for work as well as the benefits offered by enterprise mobile management. The terms EMM and MDM are often used interchangeably. Both point to the idea of enhancing employee productivity by providing real-time management of employee devices to troubleshoot or configure. While MDM focuses on the device, EMM is a sophisticated version that protects not just the device but the information on it too.

One size does *not* fit all

ManageEngine follows a COPE approach. Employees are provided with a list of preapproved devices that meet the organization's procurement standards (e.g., budget, availability, or business requirements), giving them the freedom to choose while maintaining a level of uniformity. An employee can also personalize their device, avoiding the need for two different devices. This way, the organization retains ownership. Company-issued devices are great for organizations with heavy security compliance requirements. They can exercise more control over mobility while respecting employees' privacy. Moreover, because each device is preconfigured with the necessary security measures before it's assigned to an employee, there's less risk of a security breach and it isn't a burden on the Sysadmin team. It makes repairs or replacements easier when compared to other approaches.

Our biggest challenge with COPE was keeping up with technology. Devices have to be frequently updated, more so for us, as we need to keep testing our products for compatibility across multiple platforms. After thorough evaluation, we stuck to a mid-range budget for employee devices that meets all our performance requirements and is supported by the OEM without breaking the bank. Luckily, the market today is flooded with a wide variety of smartphones, laptops, and peripherals at competitive prices. High-end devices are purchased exclusively for product testing.



Number of devices in Zoho Corporation

Chapter 02

Creating a system that works

A learning curve

When we first started out, we manually inventoried our devices and installed updates on each device. For a start-up, that's not exactly an issue. But what happens when you have 1,000 employees? 5,000? A traditional inventory system is time-consuming and labor-intensive. As our organization grew, there were too many devices and not enough people to handle them. We decided to switch to a unified system before things got out of hand. Having an effective plan helps you save time and money. Zoho Corp's Sysadmin team handles internal processes from employee onboarding to software updates efficiently. Being able to do all those things (and more) in a uniform manner helps reduce redundant tasks. The administrative team can then focus on other important incidents.

Each device has to go through a number of teams before approval, including:

Help desk:

Monitors requests raised by employees, conducts asset availability checks to issue devices, and periodically updates records

Compliance:

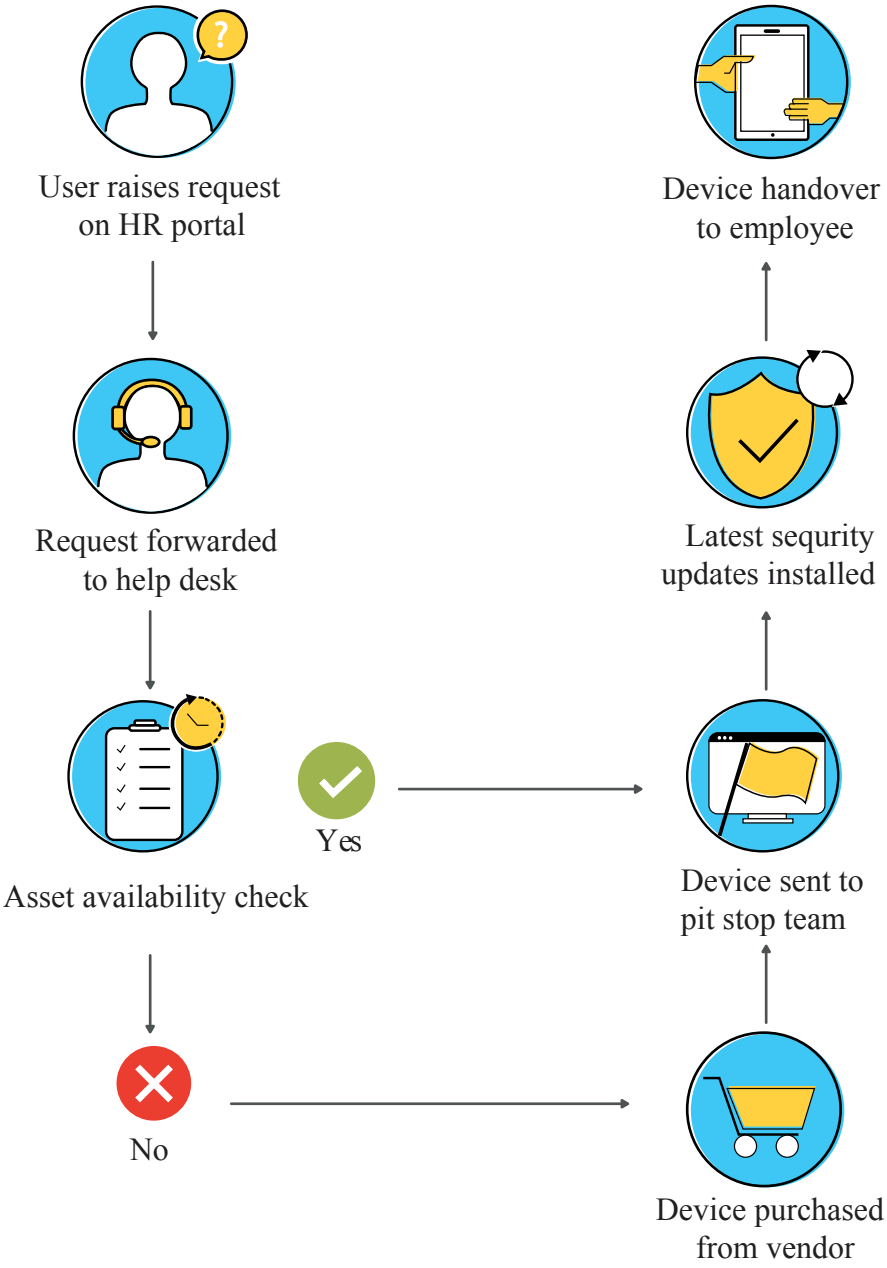
Ensures device compliance with organizational and international security policies

Procurement:

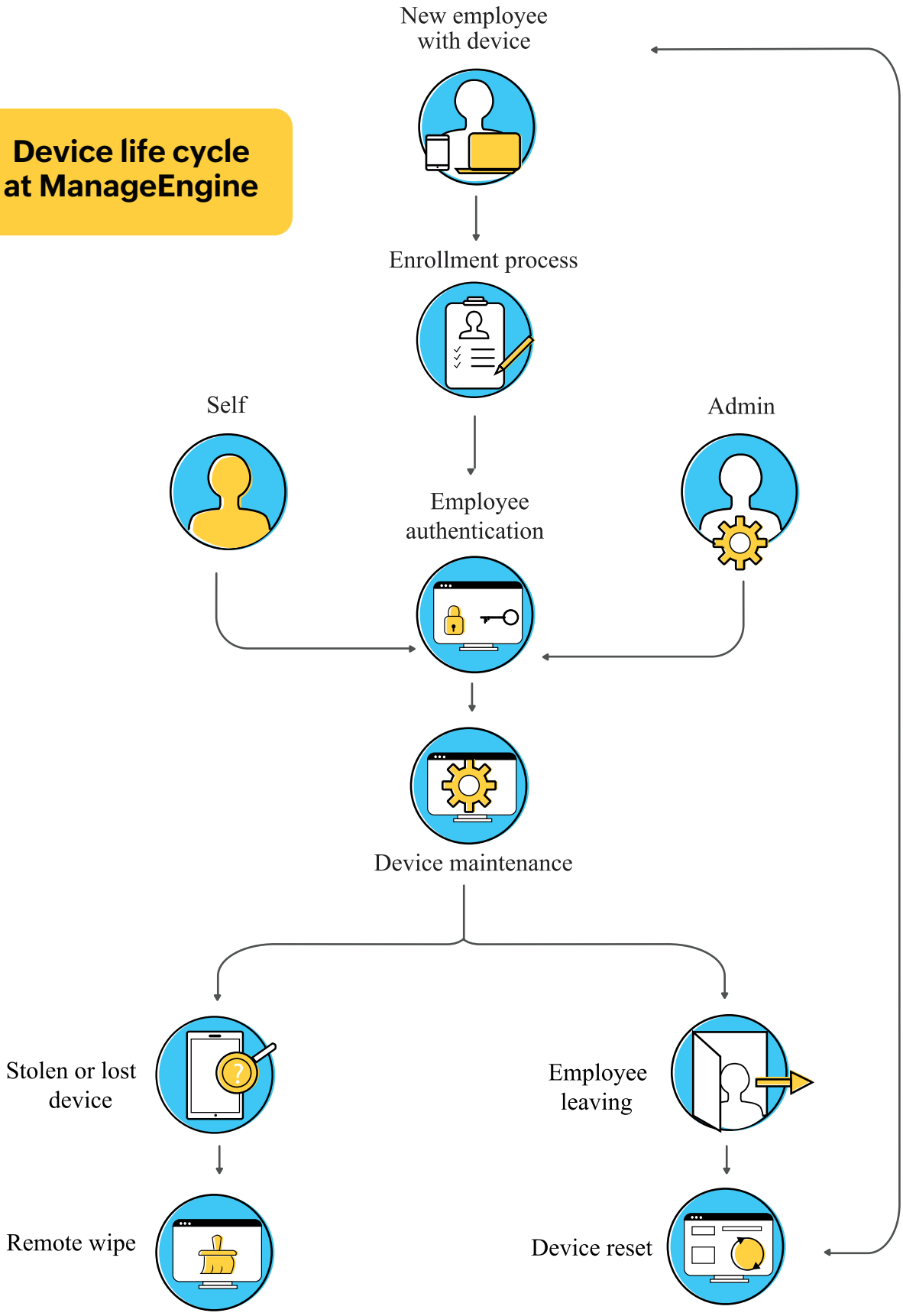
Conducts performance evaluations, hardware selection, cost and vendor analysis, and vendor purchase negotiations

Pit stop:

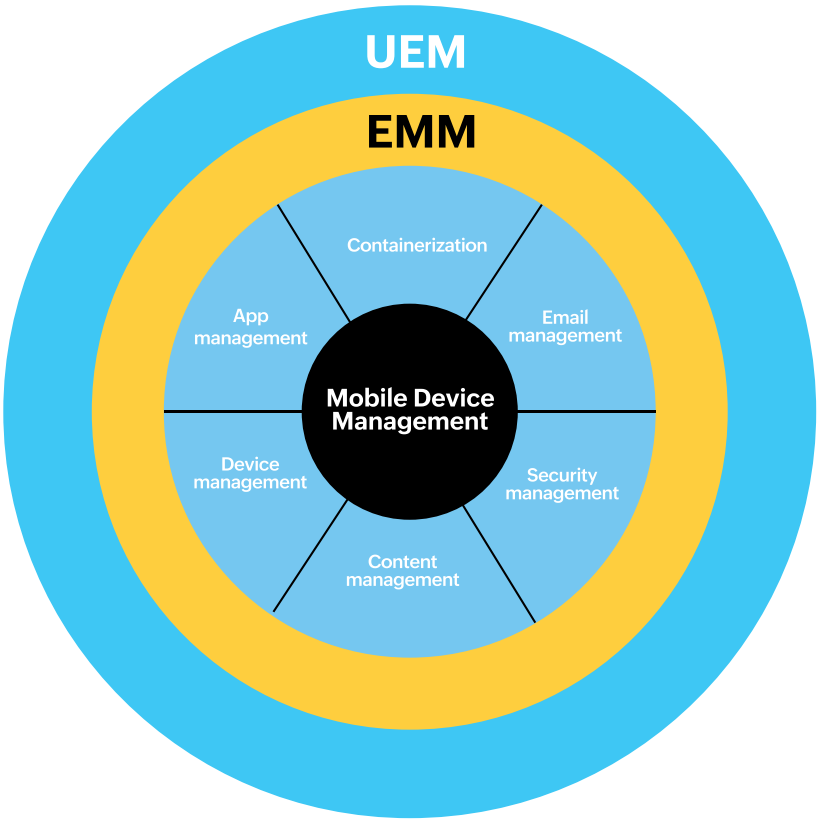
Installs the latest security updates on devices before handover to the Sysadmin team


User raises request on HR portal
Request forwarded to help desk
Asset availability check
Yes
No
Device sent to pit stop team
Device purchased from vendor
Latest sequrity updates installed
Device handover to employee

Device life cycle at ManageEngine



An umbrella approach



UEM encompasses a broader aspect of device management where instead of just addressing the mobile device, it caters to any endpoint, like laptops, desktops, servers, phones, and single-purpose devices like displays. It might sound complicated, but really it's just a combination of EMM and preexisting client management tools. UEM wasn't really a thing until 2018, when tech research giant Gartner released its first-ever Magic Quadrant for UEM. Gartner evaluated popular UEM vendors based on their EMM capabilities.

UEM has been in place at ManageEngine for two years now. If you've spent time researching UEM, you've come across the phrase a "bird's-eye view" on every blog, website, and product description—and rightly so! UEM allows you to manage, control, configure, and monitor macOS, Android, iOS, Windows, and Linux devices from one console. This single-handed approach towards application management, device management, data security, and compliance is perfect for organizations with a constantly growing number of endpoints. It offers a number of benefits, including enhanced visibility over network devices with end-user support, improved SLA resolution time, and boosted productivity when integrated with ITSM tools.

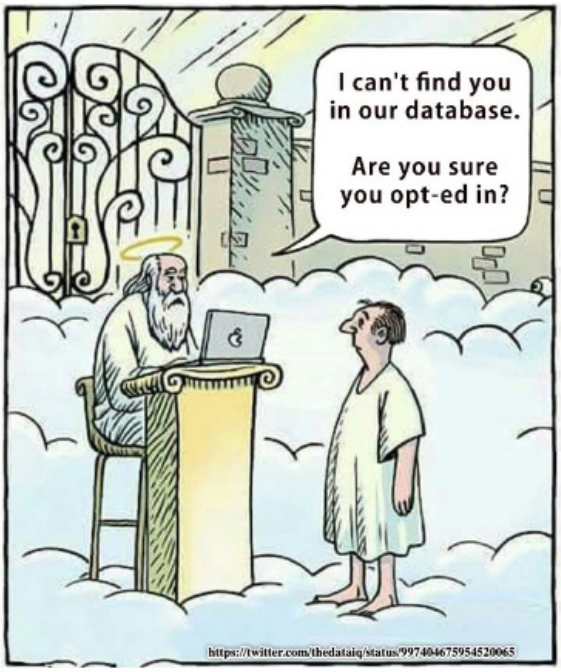
UEM is a boon if your company has legacy apps. It acts as a bridge between modern and legacy management, encouraging technological diversity. A big drawback when you rely solely on EMM is organizational fragmentation. UEM overcomes that drawback and provides administrative privileges control.

By the time we had a full-fledged endpoint management system, we learned what worked best for us. After multiple rounds of revisions, testing, and additions, we had a large-scale application that could handle a significant number of devices and scale up as needed. Our UEM tool is now one of the biggest players in the market. From the business point of view, UEM turned out to be the major requirement for evaluators, customers, and analysts alike. We are capable of managing multiple connections to mobile devices, IoT devices, and desktops from a single platform through APIs on desktop and mobile operating systems. Clients are more than happy to invest in a plan that has been tested in-house with over 9,000 employees.

In July 2018, only 11 percent of organizations adopted UEM. By November, that number had jumped to 18 percent, and by April 2019, it reached 25 percent. That means over the course of nine months, UEM adoption in the enterprise more than doubled!

Behind the scenes

What is data security without laws? Rightfully, each country has its set of rules and regulations, protecting citizens' personal information. From Singapore's PDPA to California's CCPA, maneuvering through these laws can be tricky. While the PDPA is regarded as relatively business-friendly, there's one mega law dictating the rules of the game worldwide: the GDPR. This is one of the strictest laws of data protection and privacy that a company must abide by. Although it's an EU mandate, the GDPR impacts most organizations worldwide. Regardless of whether your company deals with clients or employees in the EU or not, it's advised to be proactive and be compliant with their laws. If you have to take on employees or customers from the EU tomorrow, you shouldn't have to make drastic changes to company policies last minute. A PwC survey showed that 92 percent of US companies consider the GDPR a top data protection priority.



In our book ***A CIO's guide to rethinking compliance***, we discussed Zoho's approach to tackling the GDPR.

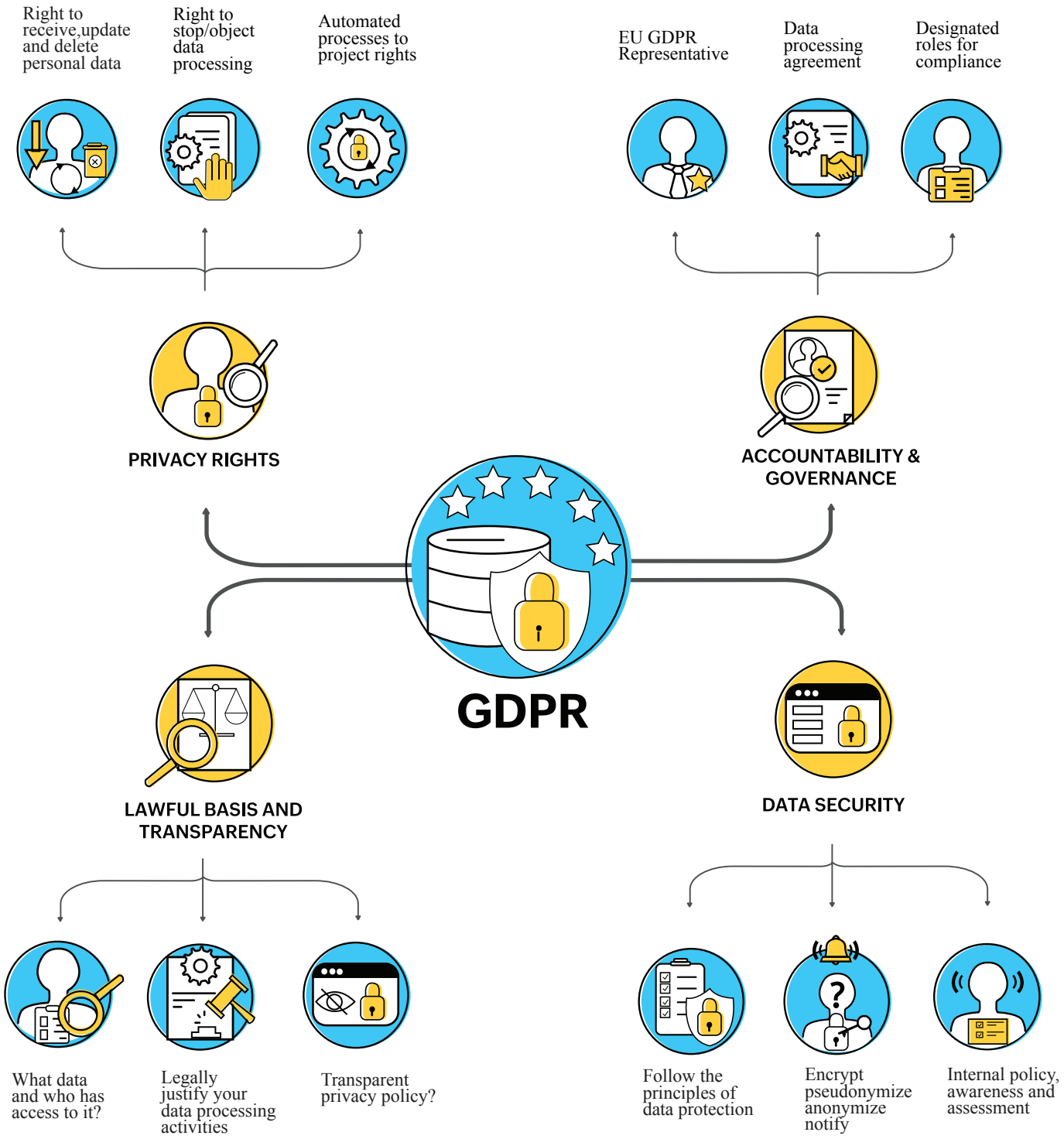
Some of the changes we have made include:

- Standardized policies and procedures for all operations.
- Increased audits to ensure compliance.
- Data protection impact assessments: Privacy reviews for new products and processes.
- Internal data protection scores to monitor teams and their data practices.
- Privacy awareness sessions for all employees.

Following x number of principles is not a one-time change. It takes weeks to implement and requires consistent monitoring. The GDPR might seem like an inconvenience, but it pushes organizations to the understanding that the data they collect is not just a random collection of words and numbers—it is sensitive information belonging to real people. Not treating that information with the utmost care and privacy can result in an equally real threat. As a company, ManageEngine has always taken privacy very seriously. To further demonstrate our continuing commitment to privacy, we extended the GDPR data usage rights to users worldwide.

Pillars of security

The GDPR is based on four fundamentals that protect users.



Time and ~~tide~~ crime wait for none

Non-compliance can lead to hefty fines. In the first half of 2020, European supervisory authorities issued at least 114 administrative fines totaling over €50 million. In 2019, Google made headlines when it was slapped with a whopping €50 million fine in France for insufficient transparency, control, and consent over the processing of personal data. That wasn't the tech giant's last negative encounter with the GDPR. In 2020, it was fined (twice!) for violating EU citizens' right to be forgotten.

Violation	Consequence
Severe violation Infringements of articles: • 5 (data processing principles) • 6 (lawfulness of processing) • 7 (conditions for consent) • 9 (processing of special categories of data) • 12 – 22 (data subjects' rights) • 44 – 49 (data transfers to third countries or international organizations)	Fine up to €20 million or, in the case of an undertaking, up to four percent of the total global turnover of the preceding fiscal year, whichever is higher
Less severe violations Infringements of articles: • 8 (conditions for children's consent) • 11 (processing that doesn't require identification) • 25 – 39 (general obligations of processors and controllers) • 42 (certification) • 43 (certification bodies)	Fine of up to €10 million or, in the case of an undertaking, up to two percent of the entire global turnover of the preceding fiscal year, whichever is higher
Likely infringement	• Warning notice • Temporary or permanent ban on data processing • Data protection inspections directed by the EU commission

Chapter 03

Your BYOD plan - savior or security threat?

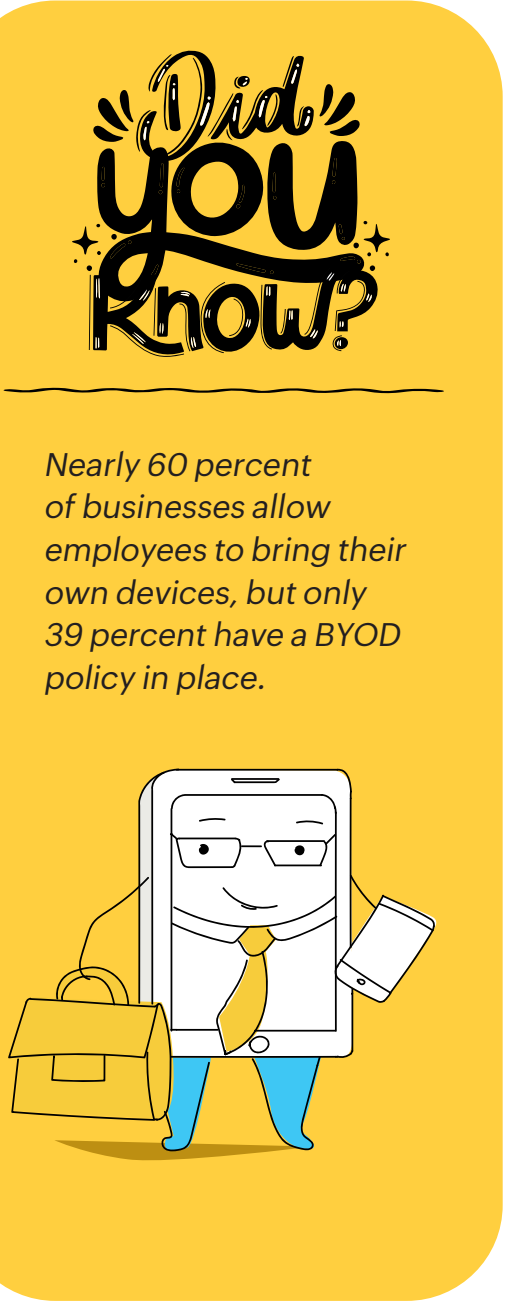
Expanding your mobility horizon

BYOD=smartphones. Smartphones can take your business to new heights or be the security threat you've been dreading, depending on how you play your cards. With so many cons, you might be wondering if it's even worth bringing up a BYOD policy. Take it from us, it's worth the hassle. Like it or not, BYOD is here to stay. If you're running a small or medium-sized business, your tight budget probably limits you from spending large amounts on company-issued devices. This is where BYOD (if executed properly) can benefit you.

BYOD can save your company nearly $350 per employee, per year. And it's not just about cutting costs. It's about increasing efficiency and keeping employees happy. BYOD increases employee productivity by aligning with existing behavior. Workplace flexibility inevitably results in job satisfaction. Using their own devices instead of learning how to use a new one saves time and is more convenient. Employees love the ease of working, and employers love the money they save. So jump on the wagon and get ahead of it while you can! The solution is in your hand (literally).

For any device management plan to work, you need a multifaceted approach. There are three key areas that need attention:

1. A system to make it work
2. A crew behind the scenes
3. A team that plays by the rules

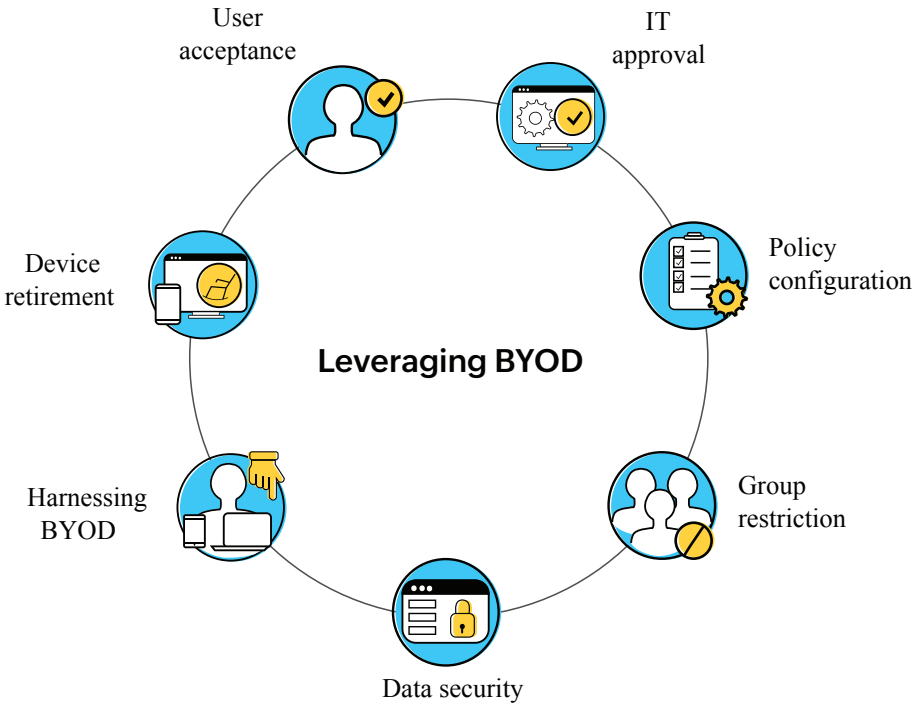


1. Erasing micromanagement from the top

Nearly 60 percent of employees worldwide use personal phones for work-related tasks, and about 90 percent of them continue to do so after work hours. With these numbers, it's no surprise that BYOD has cemented its existence in the workplace. Instead of fighting BYOD, welcome the change—with a set of rules. Before creating a framework, assess the situation and evaluate your needs. A BYOD policy outlines critical security considerations, such as the type of devices that are sanctioned by the organization, the data that can be accessed, and the employees who will be accessing corporate information from these devices. The success of the BYOD trend in an organization completely depends on how the BYOD policy is designed and implemented. In our white paper ***Leveraging BYOD***, we discussed some of these areas of consideration.

Frameworks such as COBIT 5, ISO 27001, NIST 1, or ENISA 2, regarded as general cybersecurity frameworks, are popular among many organizations worldwide. However, case studies reveal that COBIT 5 and ISO 27001 don't directly address BYOD security concerns. NIST 1 and ENISA 2 explicitly address BYOD security. To ensure harmony, choose a protocol that meets all your requirements.

Without a clear set of rules, employees are faced with ambiguity. A strong policy makes the do's and don'ts of using their own devices at work abundantly clear for employees. Who pays for what? What information can employees access? What happens if a device is lost or stolen? Is personal information monitored? Answering these important questions can liberate users from little challenges that hold them back.

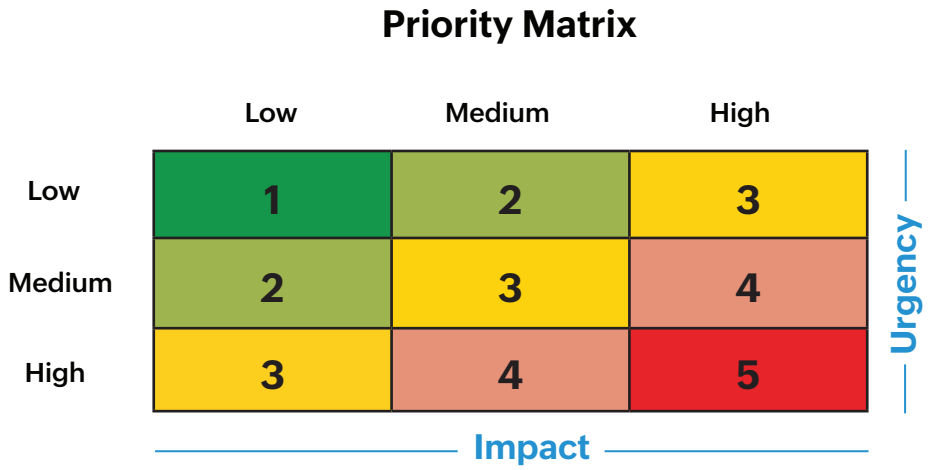


2. The M-team

The mobility team. The unsung heroes of the IT department, holding down the fort rain or shine. At Zoho Corp, the Sysadmin team handles all internal activities and takes measures to prevent incidents. They work around the clock to provide support to employees around the world. We also have a smaller support team in the US. A team of 50 managing the devices of over 9,000 employees is no small feat. It's safe to say our endpoint strategy is tried, tested, and triumphant! How do we pull it off?

During a Q&A session with author Nora Roberts, a reader asked, "How do you balance writing and kids?" She said that the key to juggling is to know that some of the balls you have in the air are made of plastic and some are made of glass. If you drop a plastic ball, it bounces, no harm done. If you drop a glass ball, it shatters. So you have to know which balls are glass and which are plastic and prioritize catching the glass ones. This can be applied to almost every aspect of life, including device management.

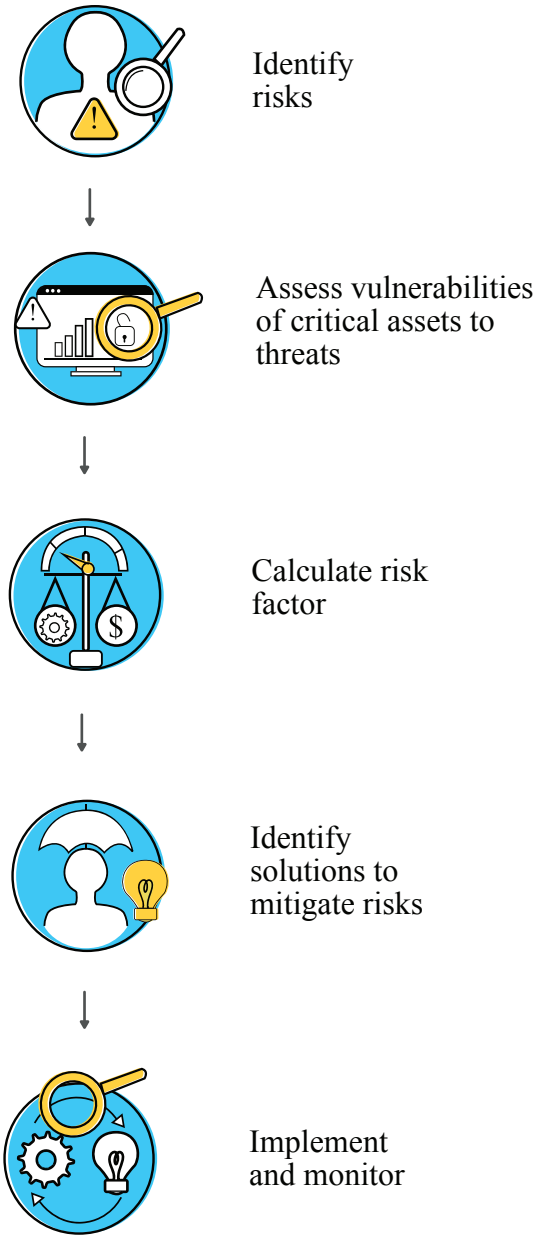
To make things easier, our Sysadmin team uses a priority matrix. It helps us weigh different factors and assign tasks to Sysadmin agents. An ITIL®-recommended priority matrix can categorize tasks based on impact and urgency. System administrators can design a matrix that works best for them.



A request may affect the functioning of an organization, a department, a group, or an individual. Can you afford to delay a user maintenance request? Yes. But a software update? Or deploying a patch? Those are glass balls. The Sysadmin team gets hundreds of tickets every day, and it's impossible to attend to all of them immediately. Knowing how to prioritize tasks can be a game-changer. We opted to integrate our help desk with endpoint management to allow employees to raise requests.

Risk management,

another key concept in device management, follows a similar structure. The idea of addressing troubles as they arise is divorced from reality and will leave you constantly putting out small fires. If you're lucky, you escape. Risk management shields your organization from data loss and cyberattacks and reduces operational costs. It's also a big time saver. Having proof of compliance will make your life easier during audits.



Stages of risk management

Your risk management strategy can be flexible and include as many stages as required to make sure you've covered all the bases. A standard plan often contains five stages:

1. Identify risks

How can you be affected? How can an intruder get into sensitive corporate data? Identify potential risks and analyze the likelihood of it occurring within your organization. This is one of the few places where pessimistic thinking may actually work in your favor. Professional red teams are constantly trying to figure out loopholes and gaps in device security that they can take advantage of.

Risks can be identified from any of these factors:

- Threats and vulnerabilities identified from external or internal sources
- Internal or external issues
- Requirements of interested parties
- Assets
- Incidents

Some common threats associated with devices include malicious software, gaining access to a device that has been lost or stolen, negative end-user behavior like jailbreaking, and corporate data leakage. ManageEngine uses a data security tool to monitor risks, which is strongly recommended to keep stakeholders in the loop.

2. Assess vulnerabilities

What's at stake? Determine what can be classified as an asset and how it can be used by adversaries. Assets may be physical, digital, or even people. In our case, a physical asset is the device itself; a digital asset is the information in it; and the asset can also be the device owner or a sysadmin. An asset valuation scale determines the importance of each asset and its impact on the functioning of the organization in terms of confidentiality, integrity, and availability. Vulnerabilities can be exposed by anything from APIs to Bluetooth. Data can be transmitted over Wi-Fi, or files can be accessed when using third-party apps. Identify these vulnerabilities associated with assets and evaluate the ease with which they can be exploited.

3. Calculate risk

How bad is it? In our book ***How Zoho Corp handles natural disasters and does business as usual,*** we discussed in detail the criteria an incident needs to meet to be categorized as a risk and how risk is calculated.

Risk Calculation

Impact \ Likelihood	Low (0)	Low (1)	Medium (2)	High (3)
Low (0)	0	0	0	0
Low (1)	0	1	2	3
Medium (2)	0	2	4	6
High (3)	0	3	6	9

4. Identify solutions

How do we fix it? There are many ways to mitigate risks. Based on the situation, pick a path that best addresses its needs and will reduce the likelihood of these unpleasant surprises.

Risk acceptance:

Also known as risk retention, it simply refers to an organization's ability to accept risks. Risks are identified but no action is taken to reduce the said risk due to its minimal impact. For example, not being able to issue a device for new employees during the pandemic is a problem, but it has minimal risks. The organization limited the procurement period and issued devices as soon as possible. Based on the risk rating, the severity of the risks is categorized as LOW (0 to 3), MEDIUM (4 to 6), and HIGH (7 to 9). Zoho's risk acceptance criteria is LOW (0 to 3).

Risk avoidance:

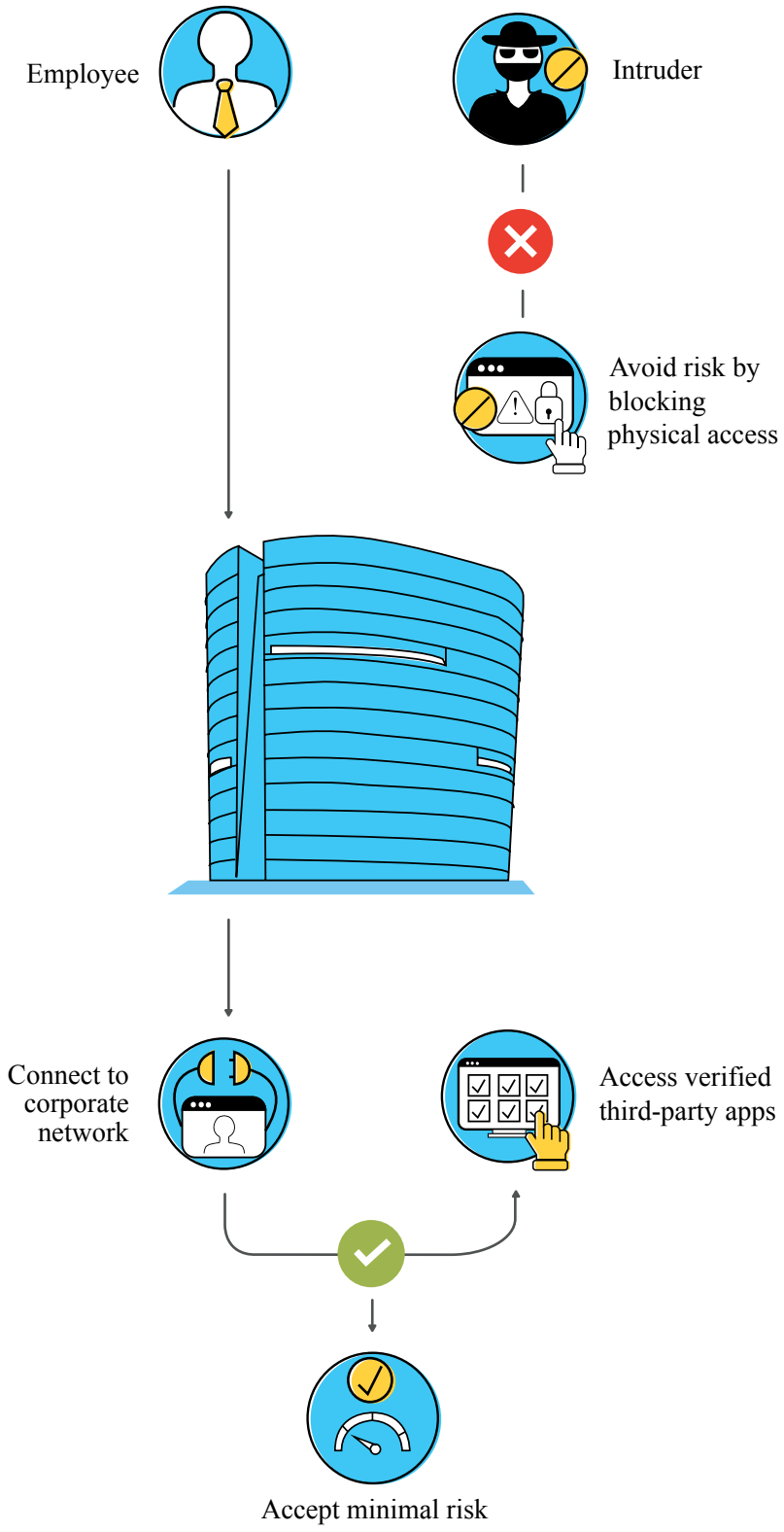
When you decide to terminate an activity that leads to risk, you can choose risk avoidance or termination. Establishing policies that prevent any risk-causing activities even before they are initiated is one way of avoiding risk. For example, by making company-issued devices mandatory, we avoid the risk of having unknown devices within our network.

Risk transfer:

In some scenarios, you can transfer or share the risk with a third party. Sharing the burden often also means sharing control, especially if the risk is something your organization cannot take charge of. This can help reduce future damage. Take the example of insurance. Some organizations opt for corporate gadget insurance that covers accidental damage, theft, loss, and manufacturing defects.

Risk reduction:

When the risk can be controlled by taking action, it is called risk reduction or modification. Businesses can assign a level at which risk is acceptable, which is called the residual risk level. Risk reduction is the most common strategy because there is usually a way to reduce risk. Root cause analysis plays a significant role here. If risk modification is chosen, we have to test and monitor the effectiveness of the implemented controls. We can then derive the revised risk score (i.e., the score calculated from the impact and likelihood after applying the control). Taking steps to facilitate secure application, like patch updates, and conducting periodic audits can warrant compliance in the workplace and minimize the threat of cyberattacks.



5. Implement and monitor

You cannot just implement a one-time solution and close the case. That's like putting a band-aid over a bullet hole. The trick is to make sure you're always prepared to tackle these risks and protect your organization. Repeating and continually monitoring the processes can help ensure maximum coverage of known and unknown risks. You avoid impulsive reactions and being in firefighting mode at all times to rectify problems that could have been anticipated. The result? Happy employees and customers, and a resilient organization.

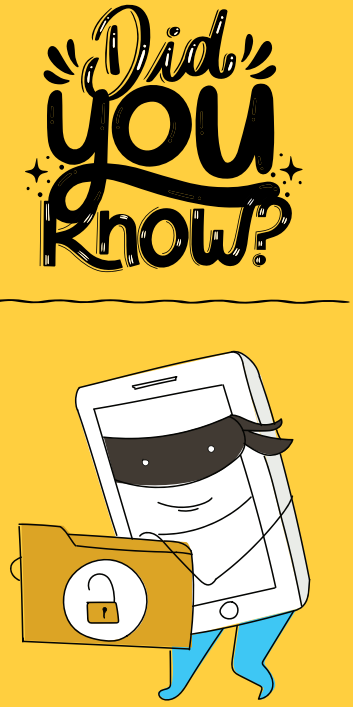
So now you have policies that meet your requirements, and a framework to make it work. What's next? A well-structured Sysadmin team is the last piece of the puzzle. For all the parts to fit and make sense, you need to assign roles. When your Sysadmin team has clear responsibilities, there's no room for confusion. It allows them to tackle requests and tasks efficiently.

Role or team	Responsibility
Manager	• Handles Level V requests and escalations • Implements new IT infrastructure • Manages the entire Sysadmin team • Communicates with vendors
Leadership	• Handles Level III and IV requests and escalations • Implements new setups • Coordinates with the Sysadmin team
IT Services (24x7)	• Uses a shift-based system to respond to Level II and III requests like maintaining servers and application servers, monitoring services and alerts, and configuring backups
Pit stop	• Responds to tickets submitted by employees • Handles issues like configuring applications, troubleshooting applications and hardware, providing or upgrading laptops, OS re-installation, and licensing software
IT Asset & Compliance	• Manages assets such as laptops, phones, monitors, and other peripherals • Provisions devices to the Pit stop team based on employee requests

3. Fostering a culture backed by tech

"Culture eats strategy for breakfast." Does this mean strategy is not crucial? No. It means strategy is secondary. It means a rich and powerful culture paves the way for success in an organization. Before you use a product, it's important to take into account what the end user (in this case, employees of ManageEngine) might think. It's crucial to consider their feelings and not make them feel like the company is tracking them 24/7 or invading their privacy. We knew we needed to monitor devices while they were on our network. However, it wouldn't be right to access employees' personal apps. An employee might be reluctant to have UEM on their device since features such as geolocation are active, and many may be reluctant to be followed on their free time or have their call history seen.

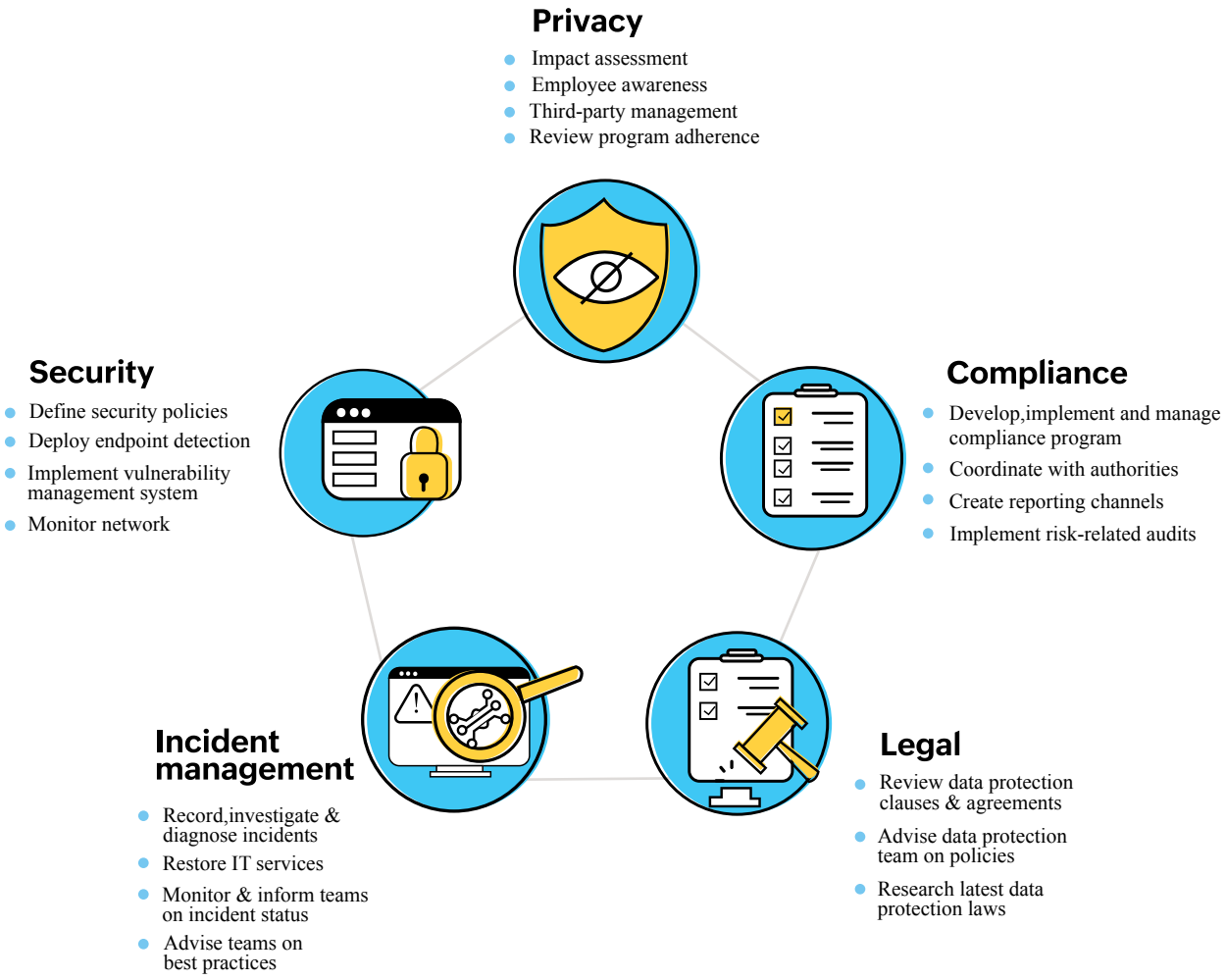
This is where containerization came in. Containerization aims to secure a portion of a device's resources (for example, application, storage, or network access) from other applications and systems running on the same device. It ensures that enterprise data and an employee's data are completely isolated from one another. The flow of data in and out of the container is prohibited, thereby securing corporate data and giving users complete control over their personal data. Win-win!



In 2019, human error was the cause of over 21 percent of data breaches in corporations.

While we're discussing employees, remember that you're only as strong as your weakest link. A posh, high-tech, secure device management plan is meaningless if employees don't know the rules. Focus not just on the device but the person using it. Employees should be aware of company policies as well as laws pertaining to their clients and countries. ManageEngine has always put emphasis on being a privacy-first organization, eliminating third-party trackers and "backdoor deals." It is mandatory for employees to undergo privacy awareness training (PAT).

Every new employee gets #giveyourselfPAT and information security management system training to ensure they are aware of data protection practices and their responsibility towards them. This gives employees the information necessary to perform their duties without compromising the security and privacy of the organization. To reinforce the importance of data security and privacy, we also have an annual security and privacy awareness training session for all employees. Each session sheds light on the focal points of security: the what, why, where, and how. It takes a village to make sure an organization is prepared for any threats. At Zoho, we have five teams working hand in hand to stay on top of any risks.



Chapter 04

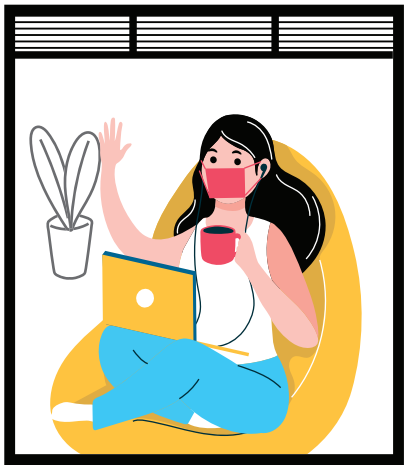
Covid-19 - Adapting to new normal

Challenges in the work-from-home era

At the onset of the COVID-19 pandemic, Zoho Corp issued a work-from-home policy long before nationwide lockdowns. When you think about a global crisis that has a major impact on organizations, it goes without saying that you need to prioritize—and fast. Where do you start? Your first goal should be to protect the welfare of your employees. This one's a no-brainer. We knew we had to ensure their safety before we moved forward. By early March, 8,000 people working in one office quickly turned into 8,000 offices. While there has been a considerable increase in productivity, the transition was not seamless. Remote work came with a unique set of challenges.

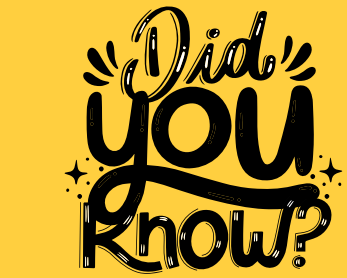
Our second priority was business continuity. We need to be able to deliver the products that customers need to run their businesses. How can all the departments work together with customers and ensure there is no disruption in services? Employees need to have access to information.

They need to be able to communicate regardless of their location. How do we enable that? When employees are working from the comfort of their home, they often use their own Wi-Fi or mobile data, which is often unprotected or at least not as protected as an enterprise VPN. This becomes an issue when handling sensitive data. How do we ensure the security of company information?

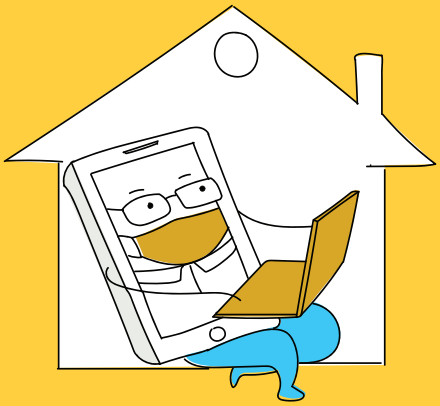


We can't rely solely on endpoint management, especially during the pandemic when employee devices aren't on the corporate network. By using VPN, productivity is boosted since access to corporate resources can be granted to the employees working from anywhere without having to compromise on data security.

Idle session timeout, session expiration, and mandatory two-factor authentication for our VPN login further strengthened our cybersecurity. We have further opted to provide end users with a self-service portal to install licensed software required for day-to-day operations.



In a poll assessing the impact of COVID-19, over 47 percent of InfoSec and IT professionals admitted to facing new challenges due to the sudden shift to remote work.



Before the pandemic, we relied extensively on our on-premises endpoint management tool to manage employee data. Since the shift to remote work, we've started managing everything through a cloud-based system. The cloud version of our UEM product was launched in August 2020. Although we faced multiple hurdles in a short span, our excellent Sysadmin team was able to find a work-around quickly and help employees find a balance between productivity and security.

Zoho's CEO Sridhar Vembu has often talked about rural revival—empowering the rural community by providing work opportunities. True to his vision, he launched the "hub and spoke" model offices in the lesser known parts of South India. As of 2020, we have 12 spoke offices and more coming soon. COVID-19 has made it difficult for large corporations to function, but our spoke offices with limited capacity have turned out to be a viable solution in uncertain times. If anything, the pandemic helped us accelerate their opening.

For instance, our Puthucode office was inaugurated in October 2020. It is situated 18 miles from Palakkad (370 miles from Zoho Corp's Chennai office) and only has 21 employees. Employees working at a spoke office raise a device issue request to the administrative team back at the Chennai branch (our Indian headquarters). The admin team reviews and approves the request. The required gadgets are sent over by post within two weeks. It's that easy! Moving to a cloud-based system has made it simpler for the Sysadmin team. They can now process these requests in a hassle-free manner, regardless of where the employee is. Whether we're three or three hundred miles away, providing devices is no longer an issue.

Office with a view: Employees are immersed in nature while they get their work done. Better than any top-floor office!

As the saying goes, the show must go on. Remote work has not stopped ManageEngine's growth. We continue to hire on an ad hoc basis. Onboarding employees turned out to be a big hurdle. Normally employees would complete their onboarding process in person (read: get their pictures taken) and get their devices immediately. This is better for the employee as well as the company because it's important to carry out official work on a protected device. With the lockdown, we were unable to provide devices right away. Here, we had no choice but to provide flexibility. Employees used personal devices for a short while. OneAuth, our in-house multi-factor authentication app, ensured that accounts could not be accessed by anyone other than the employee. They received their work-approved devices when the postal services resumed.

We have also upped our product game to find solutions to these unprecedented challenges. In April, we introduced two features to our applications. First, a Direct Download feature to our UEM system. This allows "roaming" agents who are working from home to download the required files directly over cloud rather than from the server. We also block removable storage devices, including USBs, on all laptops. Second, we added remote work tools for our internal communication channel. This includes a virtual check-in/check-out, "At Work/Away" status updates in real time, as well as meeting and call updates to see department members' availability.

Our main focus was to create tools that help organizations build multiple layers of security to enable remote access to critical systems. One such remote access product facilitated access to user desktops for providing technical assistance and servers inside the corporate network for regular operations. The access management tool, on the other hand, enabled remote connections to critical business systems like servers, applications, and network devices.

Once again, ITSM saves the day. Device control is only half the picture; you still need to deal with risk mitigation, which is where ITSM plays a significant role. Traditionally, business and IT have always been viewed as two separate entities. The pandemic has helped businesses understand that IT isn't just a supporting element but the backbone of the organization's success. ITSM turned out to be the need of the hour. It has worked just as efficiently, if not more, during the pandemic, emphasizing its importance in the workplace. ManageEngine's ***The State of ITSM in the COVID-19 Pandemic survey*** report showed that over 72 percent of participants responded positively to the effectiveness of ITSM in remote scenarios.

We faced multiple hurdles as we transitioned from different types of endpoint management over the years, and it's likely that you will too. Expect hiccups when switching to a new device management plan, especially if you're incorporating remote work in your organization. You might experience a sudden influx of tickets or VPN issues, but if you've done your homework and picked a tailored plan, the system should fall in place in no time, allowing you to deliver meaningful customer and employee experiences.

Challenges with endpoint security
(and best practices to overcome them)

Challenge #1: Cost

A solution that actually works won't be free. Implementing UEM in the workplace comes with implementation and renewal costs, not to mention the costs involved in buying hardware and software. Devices, licenses, antivirus, apps—it can definitely burn a hole in your pocket! Luckily, there are a few penny-pinching hacks to make sure you spend only on the necessities.

Best practice: Automate and evaluate

Automate processes to reduce overhead costs. Think of automation as an investment rather than an expense. Your admin team shouldn't be on defense mode all the time. If you're busy solving minor issues, some significant issues might slip through the cracks. Automation can free sysadmins from the shackles of redundancy and let them work proactively. For optimized resource utilization, automate your processes. You can identify unused hardware and software, reassign unused devices, and remove malicious apps. Plus, security features are embedded in automated workflows. Embedded security capabilities provide remote management and control of endpoints and guarantee that all employee devices are enrolled and deployed with the latest security updates. Automated patch management, application management, and policy deployments are some of the key focus points where we implemented automation.

Unleash your inner Marie Kondo and take a good look at your devices' utility. Far too often companies shell out thousands on unnecessary licenses and apps. Spend only on what you need and get rid of the rest. Companies often overlook some of the features no longer in use. Most of the products in use at ManageEngine are in-house products, so that's a big saver for us. We conduct periodic evaluations of various products and third-party applications based on the latest technology. If the product features meet our requirements, we buy those products and integrate them with our own. The legal team evaluates licenses. Based on their input, we make the necessary investments.

Challenge #2:
Too many devices and types

Regardless of the industry, policies, and security framework, monitoring the number of devices and implementing a plan that is suitable for every type has been a constant headache. It's even tougher with BYOD! Upgrading phones is no longer based on needs, it's a trend. And every time there's a new device, you need to start all over with the authentication. How do you keep up with the sheer volume?

Best practice:
Invest and inventory

Your plan needs to be versatile. Invest in a solution that allows a wide variety of devices and supports platforms like Windows, macOS, Android, and iOS. UEM is a holistic approach to enterprise device management. A cross-platform visualization of all endpoints is a must-have. Manage from a single console. Manage your entire IT infrastructure from a single pane of glass using agent-based or agentless support.

Tip: Integrate with other ITSM tools to stay on top of your IT game. To maximize its potential, we've integrated our UEM system with our in-house products:

- Help desk software to ensure smooth communication between employees and the Sysadmin team and respond to tickets raised
- Enterprise security manager to secure browsers across networks
- Asset management software to keep track of our assets across all branches of Zoho Corp
- Analytics software to study data and create insightful reports and dashboards for informed decision-making

Challenge #3: Security

With the dawn of the 5G era comes a new wave of security threats. Distribution of responsibilities among manufacturers, network operators, and service providers increases the number of parties involved in providing the 5G service. This may cause risks in data processing and ambiguity in sharing responsibilities. As if endpoint management wasn't complex enough already! For every benefit, there's a potential threat. Downloading large amounts of data in a fraction of a second? Great! What if it contains malicious data? Not so great.

As 5G becomes a dominant presence, there will be a significant increase in deployment of Internet of Things (IoT) devices. Experts predict that this will be the perfect gateway for distributed denial-of-service attacks. Even if you don't choose to adopt 5G technology right away, you should keep up and ensure you're not at risk.

Best practice: Rules and regulations

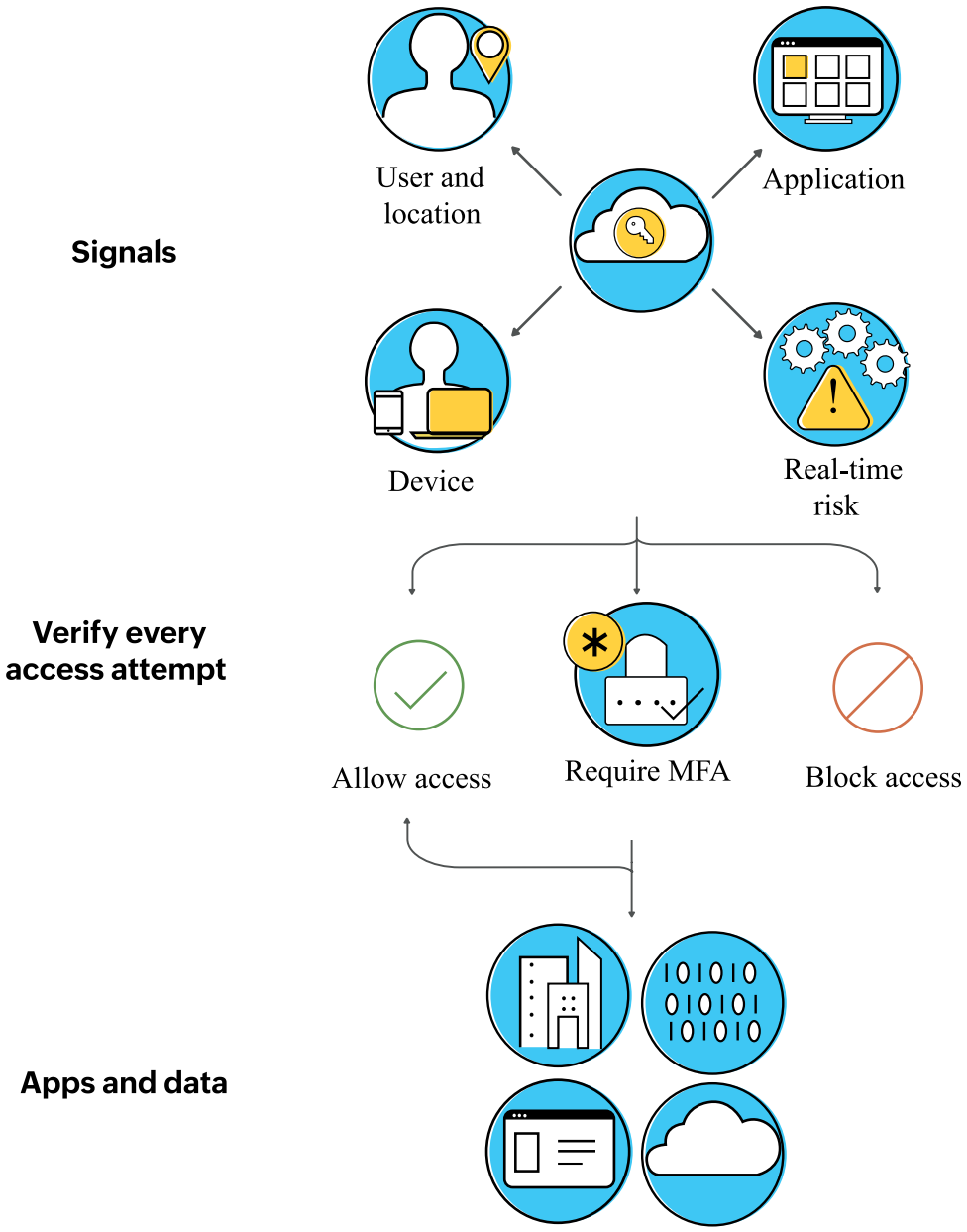
Complying with regulations is a full-time job. Lay down the law! Employees should be made aware of what they can do and what is beyond limits. Accessing confidential information and performing any other tasks involving the organization must be carried out over a VPN. Make sure people have a way to report security issues, especially in a remote work scenario. Employees don't have the privilege of showing up at work for a quick solution, so it's up to you to find a way to make it work.

We have in-house products to facilitate communication between employees and sysadmins. Our help desk tool is a platform for raising requests to the Sysadmin team. Employees can monitor the ticket status and alert the team in case of urgent issues like theft or a security breach. Our communication tool allows employees to stay in contact with the rest of the organization remotely and at work. It helps to know who is available at any given point in time to assist employees with their device-related troubles.

Zero Trust framework

A Zero Trust framework, as the name suggests, is a data security protocol that implies that all devices and entities within or outside of a network boundary are not to be trusted unless thoroughly verified by the system administrator. Zero Trust relies on multi-factor authentication, analytics, encryption, and file-system-level permissions; it includes dynamic enforcement of access rules, not only for a user's identity but also for their device and the context in which they're attempting access. Simply put, nobody enters or makes a move inside the network without your permission. You have full control over your organization's network and can cut off system access should any action fall outside of the predetermined range of allowed activities. The result is that users are given the minimum amount of access to accomplish a specific task.

Mobile devices are at the core of Zero Trust security. Traditional cybersecurity follows a "trust but verify" model that isn't exactly suitable for modern technology. Working on the assumption that everyone inside a network can be trusted may result in insider attacks. A continuously monitored real-time security framework is a protective shield, especially in organizations that have BYOD in place. A great example is Microsoft's Zero Trust framework.



Microsoft's Zero Trust framework

Challenge #4:

Complexity

Time is money! You could lose out on thousands of dollars if employees don't understand the system. If your system is too complex, employees may spend more time trying to figure out how they can submit a device request or access information than actually getting work done. If employees are not satisfied with the endpoint solution, they may avoid using those devices for work, completely defeating the purpose of investing in such a tool. How do you balance protecting information and boosting productivity?

Best practice:

Choose a user-oriented solution

Users first. To quote Steve Jobs, "Start with the customer experience and work backward to the technology." It's important to protect corporate data, but it shouldn't be at the cost of your employees' productivity. Choose a solution that works best for your employees and your brand and work around it. Employees are at the core of our plan. Employee experience is just as valuable as customer experience.

Assess your needs and test out different solutions before you pick "the one." Do you want an in-house solution, or will you outsource your ITSM operations? What do you aim to achieve by implementing endpoint management? What are your organization's pillars of security?

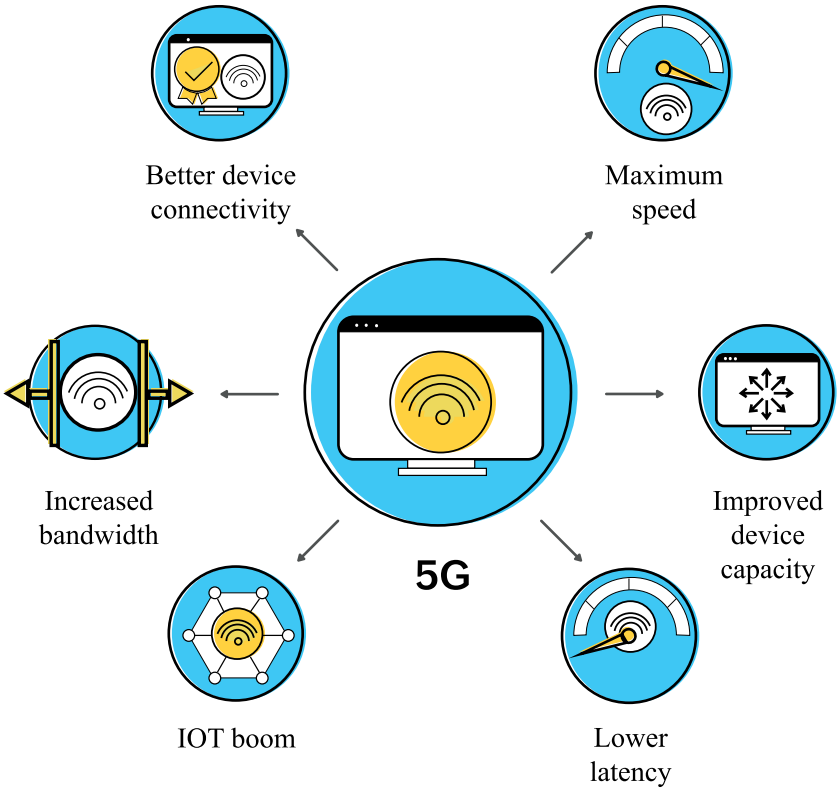
The future of mobility

Endpoint management is not a one-time process. It's constantly evolving—and that's a good thing! You cannot stick to the status quo and expect your brand to grow. You should be able to control your endpoints at any point in time no matter the size of your organization. Be prepared to go with the flow and scale up as needed. Update your systems. If your organization has a machine or device running outdated software without the latest patches installed, your risk of experiencing a security threat increases significantly.

Before you implement a plan, ask yourself whether it ensures protection. Does it provide a cohesive user experience? Investing in a plan that checks all your boxes right from the start will strengthen your cyber resilience, and you'll reap its unparalleled benefits in the long run.

The 5G era

The future of mobility will be revolutionized by the introduction of 5G technology. Despite its challenges, the benefits of 5G outweigh the cons. What's in it for you?



Better device connectivity:

Ever faced trouble with spotty service in a crowded place? Or in the middle of nowhere? Not anymore! Connectivity in hard-to-reach places is critical now that remote work has become the norm. 5G also allows organizations to implement virtual networks and create subnets. Network slicing provides connectivity more tailored to organization-specific needs. Improved device connectivity is a blessing in the workplace, facilitating calls and presentations in real time without network problems. You no longer have to spend the first five minutes of your Zoom call saying "Can you hear me?"

Maximum speed:

The 5G experience promises speeds of 1Gbps to 10Gbps, which is a significant shift from 4G LTE, maxing out at 1Gbps. While some claim 5G could theoretically reach 20Gbps, it's too early to predict real-world performance. Nevertheless, this makes downloading information and communication with cloud platforms faster and easier. This in turn will improve productivity, saving time and money. It would take you longer to tie your shoes than it would to download a movie!

Increased bandwidth:

For businesses, using 5G provides deeper insight on their customer base. More connections, more information. A large portion of digital businesses rely on data. Big data analytics can help turn volumes of data into actionable knowledge. You can benefit from a vast wealth of information and transform your business like never before. They don't say data is the new oil for nothing!

Every sector you can think of stands to gain with the widespread introduction of 5G. While it may take a couple of years to see its full potential (and perils), that shouldn't stop you from stepping up your endpoint strategy now.

Improved device capacity:

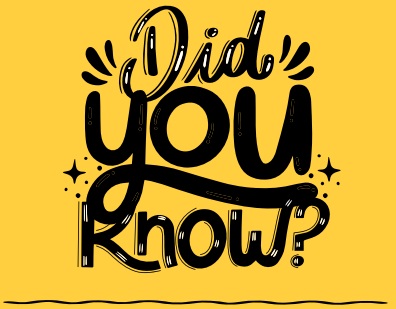
5G is expected to enable mass connectivity. We're talking millions. One million devices per cell. People from every corner of the planet connected in an instant. It also helps that 5G is an addition to our existing system rather than a complete replacement. When a 5G connection is established, the device will connect to both the 4G network to provide the control signaling and to the 5G network to help provide the fast data connection by adding to the existing 4G capacity.

Lower latency:

With 5G, latency (time taken for a device to carry out a task) could drop from 50 milliseconds to just one millisecond. Deutsche Telekom achieved a latency of three milliseconds with the first practical 5G trials in Germany. This means there's virtually no delay in sending and receiving emails, Googling information, or downloading files.

IoT boom:

Machine-to-machine communication will revolutionize every field. IoT is the cherry on top in the smart world. Smart cities rely extensively on 5G and IoT to create immersive experiences. Businesses can expect an increase in wearables like smart watches and even drones. Next-gen tech will make room for innovative products and services and improve our way of life, similar to the rise of cloud services.



Experts predict that IoT will account for a quarter of the 41 million global 5G connections in 2024.

Final thoughts

Through this book, we've uncovered ManageEngine's long but fruitful journey in device management. We've had our ups and downs. We've faced struggles and gained so much in the process, and that's the purpose of this book. We want to share our knowledge in hopes that others can grow from it. The most important takeaway from this book is that there is no such thing as one right policy or approach. We have many options to choose from, so make the best of it! The future of mobility is full of promises. Although we can't predict what's in store to a T, one can be cautiously optimistic about the exciting road ahead. We hope this book inspires you to take charge, to lead the change in your field and become a pioneer of innovation in your own way.

Mahanya Vanidas
Author | Content writer
ITSM customer education
ManageEngine

ManageEngine

a division of ZOHO Corp.

For more information:

www.manageengine.com

sales@manageengine.com