ESEVEL

BUILDING A SOLID IT INFRASTRUCTURE

The 5+1

Essentials for Growing Companies

INTRODUCTION

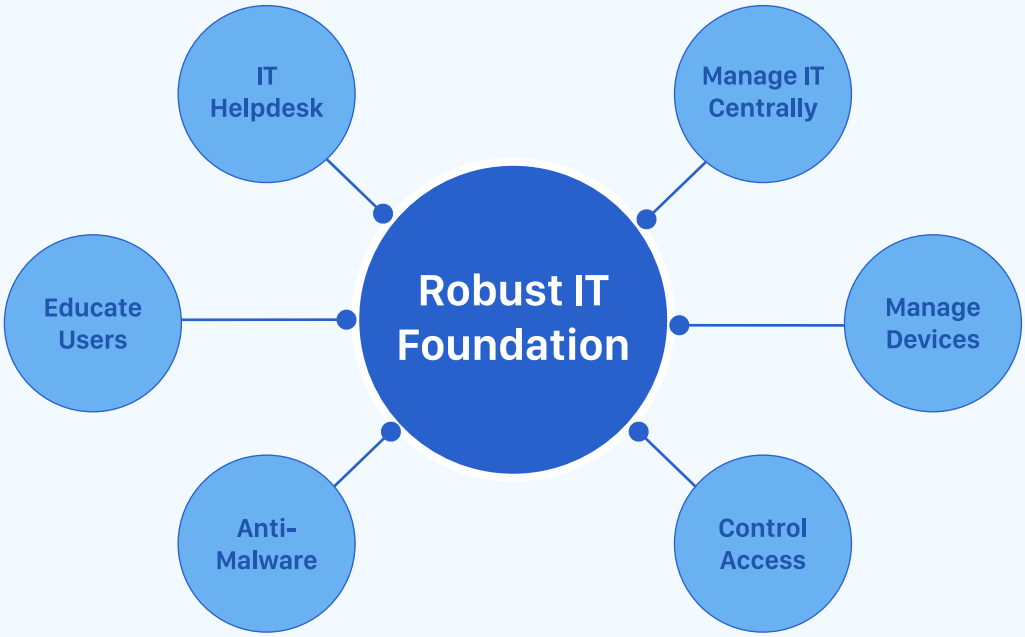
In today's fast-paced business world, having a solid IT foundation is crucial for growing companies. As your business expands, so do your IT needs.

A strong IT infrastructure ensures smooth operations, protects sensitive data, and boosts productivity. Investing in IT now can save you from costly problems later.

You might think your business is too small or it's too early to build an IT foundation, but that's a dangerous misconception.

Small to medium-sized businesses (SMBs) are prime targets for cyberattacks, with 43% of attacks aimed at them, according to Verizon. Many SMBs never recover from these attacks due to financial losses and damage to their reputation.

Building a solid IT foundation not only enhances your security but also attracts larger clients who need vendors with secure IT. This opens up significant revenue opportunities for your business.



This guide will cover the key aspects of building a robust IT foundation

Centralized IT Management: Why centralizing your IT processes is essential and how to do it effectively.

Device Management and Security: Best practices for securing and managing your devices.

Access Management: The importance of controlling who has access to what and how to implement strong policies.

Anti-malware: Tips on choosing and implementing effective anti-malware solutions.

End-User Cyber Hygiene Education: How to educate your team on cyber hygiene to reduce human error and enhance security.

+1 IT Helpdesk

The importance of having a dedicated IT helpdesk and how it supports your IT foundation.

By the end of this guide, you will know how to build and maintain a strong IT infrastructure that supports your company's growth and success.

Centralized IT Management

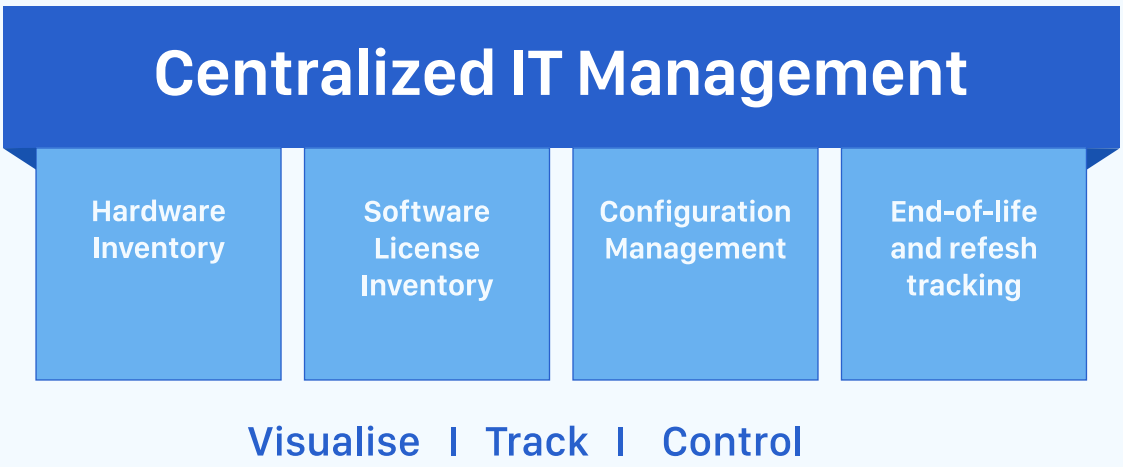
What Is Centralized IT Management?

Centralized IT management is like having a single control center for all your IT systems. Instead of using different tools to manage hardware, software, and security, you use one unified system. This makes it easier to see and control everything at once.

Why Centralize Your IT Management?

Centralized IT management is crucial for growing companies. It helps you see and control all your IT assets, ensuring security and efficiency as you expand.

By putting all IT processes into one easy system, you can easily track everything. This means every piece of hardware, software license, configuration, and tech refresh cycle is monitored and accounted for.



Remember, you can't manage what you don't track. Centralizing IT management makes tracking simple and efficient.

Benefits of having all IT processes managed centrally.

Centralized IT management has many benefits.

First, it makes things more efficient. When all your IT assets are tracked in one place, you can quickly find and fix problems. This reduces downtime and boosts productivity.

It also gives you better control over your IT environment. You can enforce policies consistently, ensure compliance, and reduce security risks.

Remember that outdated and unsupported hardware and software are risky because service providers usually stop providing patches, including those for security issues, after the end-of-life (EOL) date.

Improved efficiency and better control.

Centralizing IT management makes your work smoother and more efficient.

With one system to monitor and manage everything, you get rid of the inefficiencies of using different tools and manual tracking. This means faster response times, lower costs, and a more proactive IT approach.

You also gain better control with consistent policy enforcement, easier compliance, and a clear view of your IT setup. This helps you make better decisions and plan strategically.

Steps to Centralize IT Management

Assessing current IT infrastructure.

The first step in centralizing your IT management is to check what you currently have. Make a complete list of all your hardware and software licenses. At this stage, an Excel sheet will do.

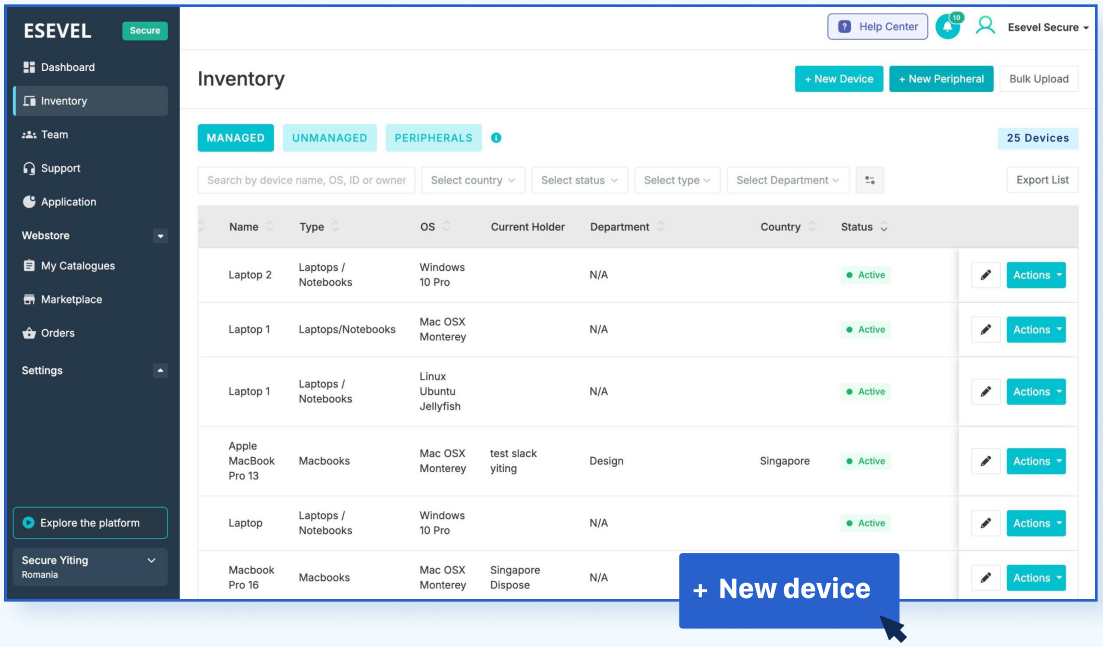
This list will be the base for your centralized system, giving you a clear view of what you own and what needs to be managed.

Choosing the right tools and platforms.

Once you have a complete inventory, the next step is to choose the right tools for centralized management.

Look for solutions that offer inventory management, configuration management, and end-of-life tracking. These tools should work well with your existing systems and give you real-time updates on your IT assets.

If you are on a budget, you can start with something as simple as an Excel spreadsheet, but you will need to designate someone to consistently update it. For more robust options, consider paid asset management tools like Zluri, ServiceNow, or ManageEngine.



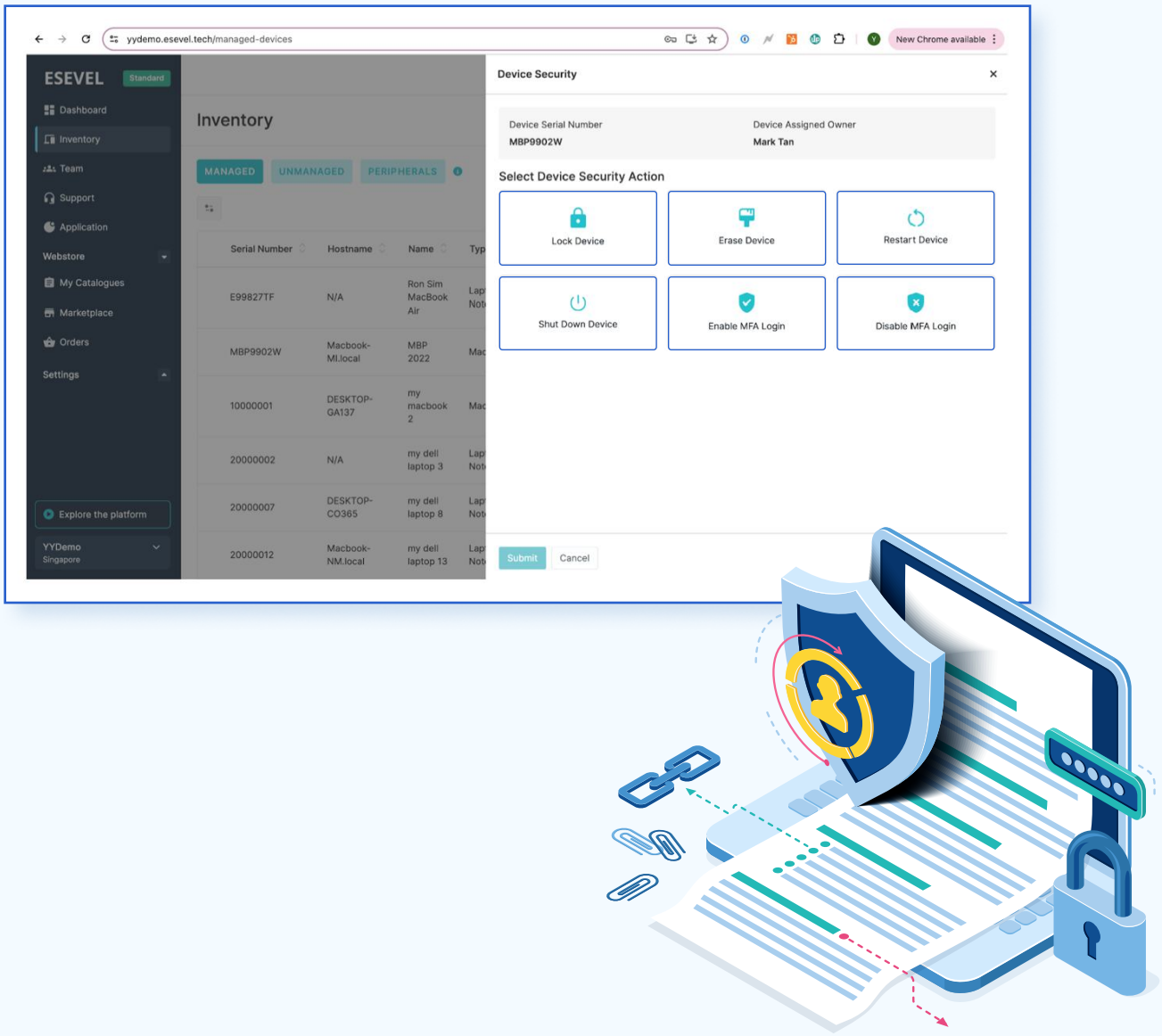
For a comprehensive solution, check out Esevel, which offers IT management and is free with any paid plans.

Implementing centralized policies and procedures.

With the right tools in place, it's time to set up centralized policies and procedures.

Create clear rules for tracking and managing hardware and software, including regular updates and tech refresh cycles. Designate someone to be in charge of IT and ensure they understand these procedures and their importance.

A standardized approach will ensure consistency, boost security, and improve the overall stability of your IT environment.

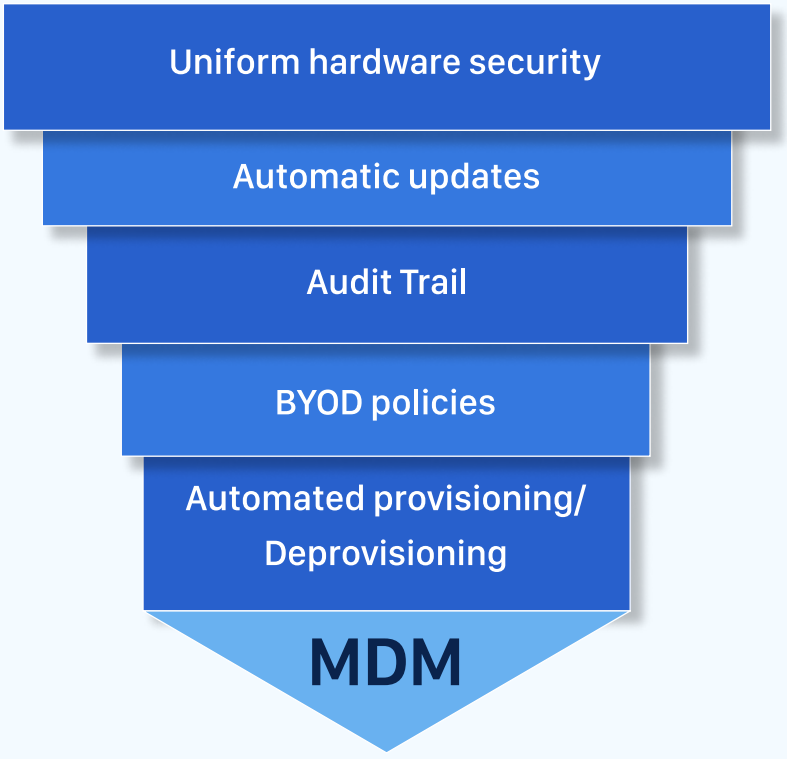


Device Management and Security

What is Device Management and Security

Device management and security involve overseeing and protecting all the devices used in a company, such as computers, smartphones, and tablets.

It ensures that these devices are properly configured, regularly updated, and secure from threats. This includes managing hardware, installing software patches, enforcing security policies, and securing personal devices used for work (BYOD).



The goal is to keep devices safe, control access to sensitive data, and prevent security breaches.

Securing Your Devices: The Basics

Importance of device management and security.

Device management and security are essential to protect your company's data.

Proper security ensures that all devices are in a secure state before they access corporate resources.

This helps control remote access to sensitive data, provides user authentication, and allows for remote wiping of lost or stolen devices. Keeping devices up-to-date with software patches also prevents security vulnerabilities.

Common threats to device security.

> Common threats to devices include malware, unauthorized access, and data breaches. Without proper management, devices can easily become entry points for cyber threats, putting your company's data at risk.

> The rise of hybrid and remote work exposes devices to even more threats, as they are often used outside the secure company network.

Implementing Device Management

Tools for managing devices (MDM solutions)

To manage devices effectively, use Mobile Device Management (MDM) solutions.

Popular MDM solutions include JumpCloud (our top choice), Jamf, and Microsoft Intune.

These tools help you track hardware, ensure software updates, and enforce security settings across all devices. They also automate aspects of provisioning and deprovisioning laptops for onboarding and offboarding staff, reducing the manual time spent on IT tasks.

Additionally, MDM is excellent for applying policies to personal devices used for work (BYOD).

If you need an easy-to-manage MDM system that is fully supported with a service desk, consider using the Esevel solution. Esevel uses JumpCloud, a premier MDM solution, and places it on an intuitive interface specifically designed for non-IT users.

Best practices for device security

Use your selected MDM solutions to implement the following:

Uniform Hardware Security

Ensure all hardware is secured consistently.

Automatic Updates:

Set operating systems and software patches to update automatically.

Change Management:

Implement an audit trail for all changes to track and manage alterations.

BYOD Policies

Secure personal devices with storage encryption, lock and wipe capabilities, and enforced authentication.

By following these practices, you can maintain a secure IT environment, reduce risks, and ensure that all devices accessing your company's resources are safe and up-to-date.

Access Management

Controlling Access: Keeping Data Safe

The importance of managing who has access to what.

Access management is crucial for protecting your company's data.

By controlling who has access to specific applications and files, you reduce the risk of identity theft, data breaches, and unauthorized access to sensitive information.

It ensures that only the right people can see and use the data they need, maintaining confidentiality and security.

Risks of poor access management.

Poor access management can lead to serious security issues.

If access rights are not properly granted, changed, or revoked, it can result in unauthorized users gaining access to sensitive data. This increases the risk of data breaches and identity theft.

Additionally, without proper logging and monitoring, it's difficult to track who has accessed what, making it harder to spot and respond to security threats.

Setting Up Access Management

Role-based access control (RBAC)

Implementing Role-Based Access Control (RBAC) is a key step in setting up effective access management. RBAC allows you to assign access rights based on roles within the company.

This means employees only have access to the data and applications they need for their job, following the principle of least privileged access.

Tools and technologies for effective access management.

To effectively manage user access, you need the right tools and technologies. Here are some essential practices:

Anti-Malware Solutions

Protecting Your Systems from Malware

Overview of malware threats and their impact

Malware, or malicious software, includes viruses, spyware, ransomware, and other harmful programs.

Malware can cause serious harm to your IT systems and data by stealing sensitive information, corrupting data, and even rendering your systems unusable.

The impact can be devastating, leading to data breaches, financial losses, and damage to your company's reputation.

Why anti-malware solutions are essential

Anti-malware solutions are crucial for protecting your IT environment.

They provide proactive, real-time protection by scanning networks and data for malware.

If malware is identified, these solutions can remove it before it causes damage. This proactive approach helps safeguard your systems and data, ensuring business continuity and security.

Choosing and Implementing Anti-Malware Solutions

Features to look for in anti-malware software

When selecting anti-malware software, look for these key features:

Real-Time Protection

The software should continuously scan for and block malware threats.

Automatic Updates

Ensure the software can update itself automatically to protect against the latest threats

Comprehensive Scanning

It should scan all files, emails, and web traffic for potential threats.

Endpoint Protection

The solution should cover all devices, including computers, smartphones, and tablets, ensuring complete protection.

Popular anti-malware solutions include Bitdefender (our top choice), Crowdstrike and Microsoft Defender.

Steps to implement and maintain anti-malware protection

After you have selected the right anti-malware solution for your business needs:

1. **Install on All Devices:** Ensure that the software is installed on all endpoints, including desktops, laptops, and mobile devices.
2. **Configure Settings:** Set up real-time scanning and automatic updates to ensure continuous protection.
3. **Regularly Update Software:** Keep the anti-malware software updated to protect against the latest threats.
4. **Monitor and Review:** Assign someone in your company to regularly check the software's logs and reports to ensure it's effectively identifying and removing malware.

By following these steps, you can proactively defend against malware threats and ensure your business remains secure.

End-User Cyber Hygiene Education

Why Cyber Hygiene Matters

The role of employees in maintaining IT security.

Employees are the frontline defenders of your company's data.

With 70% of data breaches involving human error, it's clear that even the best security systems can't do it alone.

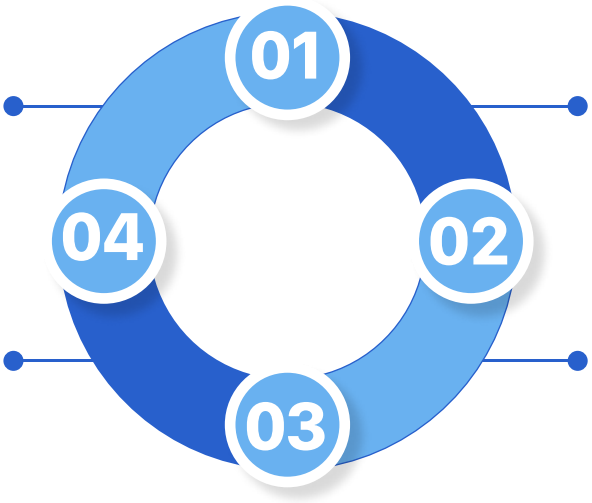
Proper training helps employees recognize and respond to potential threats, protecting your sensitive information from cyber attacks.

Common cyber hygiene practices everyone should follow.

Everyone in the company should follow these basic cyber hygiene practices:

Use Strong Passwords: Create complex passwords and change them regularly.

Update Software: Keep all software and systems up-to-date to protect against vulnerabilities.



Avoid Phishing Scams: Be cautious of suspicious emails and links.

Use Multi-Factor Authentication: Add an extra layer of security to your accounts.

Educating Your Team

Effective ways to educate employees on cyber hygiene

To effectively educate your employees on cyber hygiene:

Annual Training	Interactive Workshops	Regular Updates
Provide all end users with at least annual training on cyber threats, security policies, and standards.	Use interactive workshops and simulations to make learning engaging and practical.	Keep employees informed about new threats and best practices through newsletters or briefings.

Planning these training programs can be challenging. At Esevel, we specialize in organizing comprehensive cyber hygiene training for our clients. Reach out to us, and we'll handle it for you.

Creating a culture of security awareness

Creating a culture of security awareness involves:

Training Management: Ensure that management receives training on tech risks and tech risk management practices.

Encouraging Open Communication: Foster an environment where employees feel comfortable reporting potential security issues.

Recognizing Good Practices: Reward and recognize employees who follow good security practices.

+1. IT Helpdesk

Importance of having a dedicated IT helpdesk.

A dedicated IT helpdesk is crucial for preventing IT problems from causing delays or work stoppages.

It ensures smooth business operations and keeps employees focused on their core tasks. With a reliable helpdesk, issues are resolved quickly, minimizing downtime and boosting productivity.

How a helpdesk supports your IT foundation.

An IT helpdesk is the backbone of your IT support system. It provides immediate assistance to end users, solving technical problems and answering IT-related questions.

This support helps maintain the stability and efficiency of your IT environment, ensuring that all other IT management aspects function seamlessly.

Setting Up an Efficient IT Helpdesk

Key features of an effective IT helpdesk.

- **Ticketing System:** Streamlines issue tracking and ensures no problem goes unresolved.
- **Knowledge Base:** Provides users with self-help resources to solve common problems quickly.
- **Multi-Channel Support:** Offers assistance through various channels such as email, phone, and chat.
- **Skilled Technicians:** Employs knowledgeable staff who can diagnose and fix a wide range of issues.

Tools and best practices for IT helpdesk management.

- **Helpdesk Software:** Use tools like Zendesk, Freshdesk, or ServiceNow to manage support tickets efficiently.
- **Regular Training:** Ensure helpdesk staff are well-trained and up-to-date with the latest technologies and troubleshooting techniques.
- **Performance Metrics:** Track key metrics like response time, resolution time, and customer satisfaction to continually improve helpdesk performance.
- **User Feedback:** Collect feedback from end users to identify areas for improvement and ensure high-quality support.

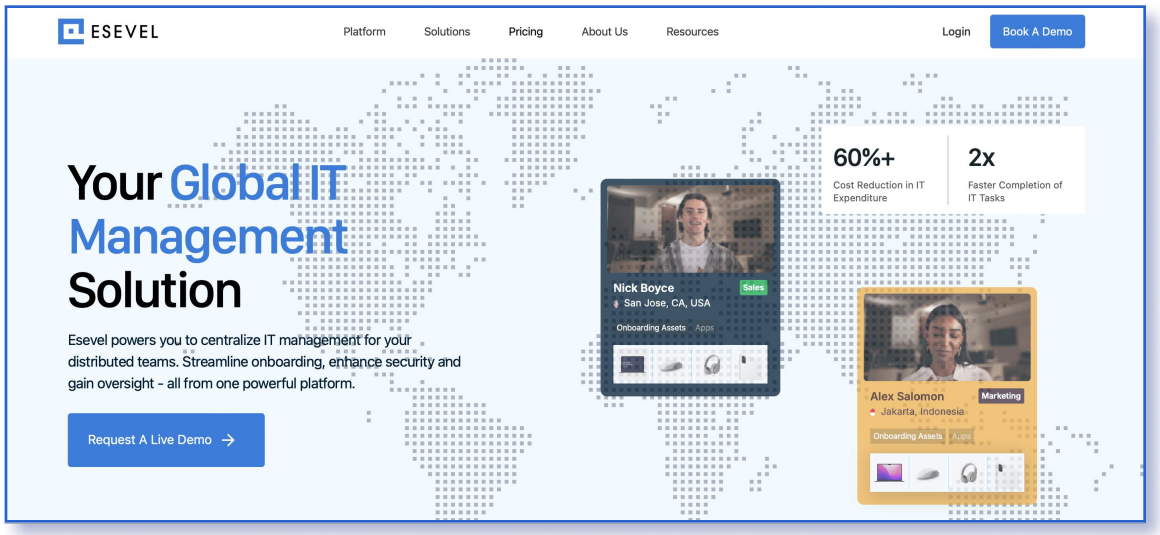
For 24/7 professional IT helpdesk support, consider Esevel. Esevel offers experienced IT engineers, built-in helpdesk software that integrates with systems like Slack, and has served thousands of users worldwide. Ensure your team gets the support they need, whenever they need it.

Esevel: Your Partner in IT Management

For growing companies without an IT department, managing IT can be overwhelming.

Esevel offers a managed IT service with an easy-to-use platform specifically designed for businesses like yours.

Our service helps you seamlessly implement all 5+1 aspects of a solid IT foundation:



Anti-Malware	Centralized IT Management	Device Management and Security	End-User Cyber Hygiene Education +1 IT Helpdesk	Access Management

What sets Esevel apart is our automated workflows, which drastically reduce the manual effort involved in IT management.

We aim to simplify IT and make it accessible for smaller and growing companies.

With Esevel, you can focus on what you do best—growing your business—while we take care of your IT needs.

Discover how Esevel can transform your IT management, boost your security, and help you scale with confidence.

Conclusion

Building a solid IT foundation is essential for growing companies. Let's recap the 5+1 aspects we've covered:

- Centralized IT Management: Centralize your IT processes for better control and efficiency.
- Device Management and Security: Secure and manage all your devices effectively.
- Access Management: Control who has access to what and implement strong policies.
- Anti-malware: Choose and implement robust anti-malware solutions.
- End-User Cyber Hygiene Education: Educate your team to reduce human error and enhance security.
- +1 IT Helpdesk: Ensure smooth operations with a dedicated IT helpdesk.

Final Tips

- **Automate Where Possible:** Use tools to automate repetitive tasks and reduce manual work.
- **Regularly Review Policies:** Keep your IT policies up-to-date to address new threats and challenges.
- **Invest in Training:** Ensure your team is well-trained and aware of best practices.

Next Steps

Don't wait for IT issues to disrupt your business. Start implementing these strategies today to build a robust IT foundation that supports your company's growth. Proactive planning is key.

Ready to simplify your IT management? Partner with Esevel and let us handle your IT needs. Reach out now to build a secure, efficient, and scalable IT environment. Your future success starts with the right IT foundation.

Resources for Further Reading and Tools:

Esevel For professional IT helpdesk and cyber hygiene training.

Verizon Data Breach Investigations Report:
To understand more about cyber threats targeting SMBs

NIST Cybersecurity Framework
A comprehensive guide to building and maintaining a strong cybersecurity posture.