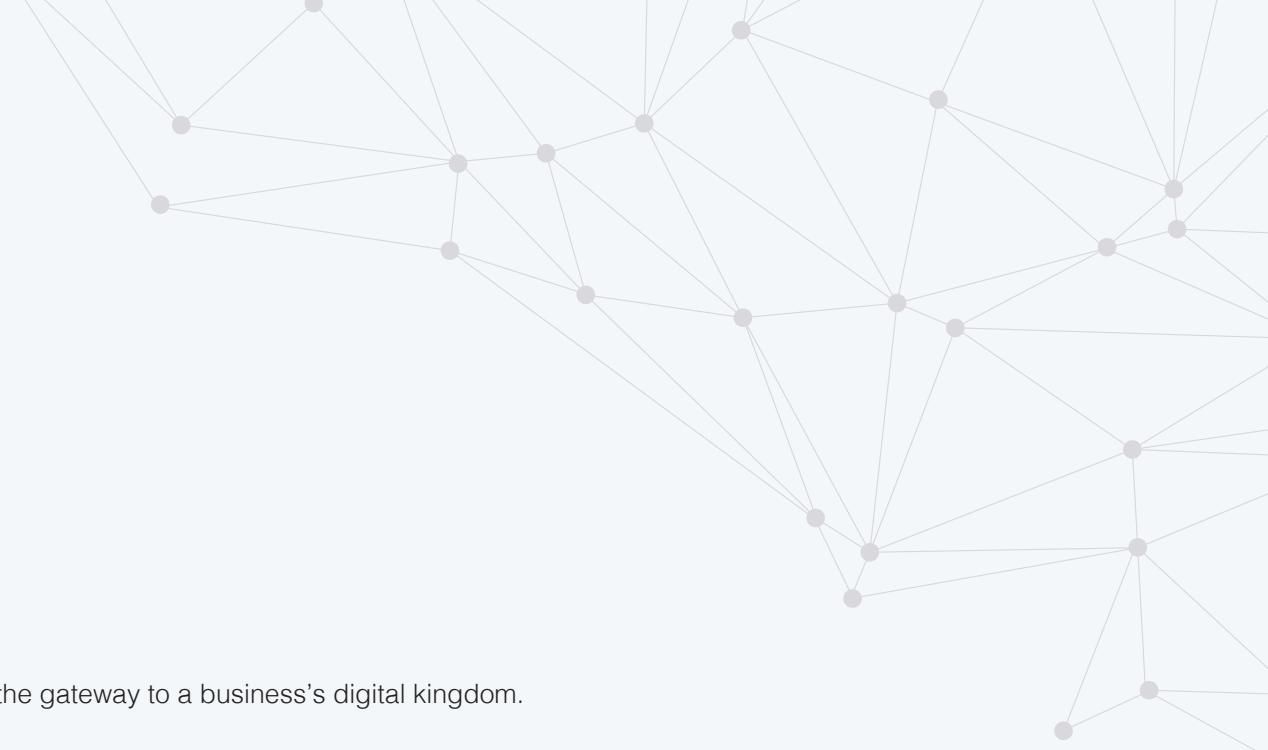




10 Endpoint Security Tips You Should Know

In partnership with
 **HUNTRESS**





Introduction

Connectivity is king in the digital world, and endpoints are the gateway to a business's digital kingdom. Because of this, they're one of hackers' favourite targets.

According to the IDC, 70% of successful breaches start at the endpoint. Unprotected endpoints provide vulnerable entry points to launch devastating cyber attacks. And with businesses needing to protect more endpoints—and more kinds of endpoints—than ever before, that perimeter becomes harder to defend.

You need to improve your endpoint security, but where do you start? This guide can help.

We've curated the top 10 must-know endpoint security tips that every business should have in their arsenal. From identifying entry points to implementing EDR solutions, we'll dive into the insights you need to defend your endpoints confidently.

Know Your Endpoints: Identifying and Understanding Your Entry Points

Tip 1

Understanding your network's endpoints is like creating a map for your cyber security strategy. Start by taking stock of all the endpoints that could serve as gateways for cyber threats.

Conduct a thorough inventory and categorise endpoints based on their sensitivity and criticality. This will help you tailor your defences to address specific vulnerabilities associated with each device.

Pro Tips



Utilise asset management tools to maintain an updated inventory of all endpoints.



Categorise endpoints based on their functions and importance to the organisation.



Prioritise security measures for critical endpoints.



What is an endpoint?

Endpoints are physical devices that connect to a network, such as desktop computers, laptops, mobile devices, virtual machines, printers, servers, etc.

Develop a Proactive Patch Strategy

Tip 2

The bedrock of endpoint security is regularly updating operating systems and applications. Developing a proactive patch management strategy ensures that known vulnerabilities are promptly addressed, reducing the risk of exploitation by cyber criminals. By building a systematic and timely patch process, you can ensure that endpoints are updated with the latest security patches, which can prevent potential incidents that could compromise sensitive data or disrupt operations down the line.

Pro Tips



Streamline updates with automated patch management tools, or seek out managed security solutions to reduce this burden on your team.



Prioritise patches based on their severity and potential impact.



Test updates in a non-production environment before rolling out more widely.



Schedule patches during off-peak hours to minimise disruptions.

Add an Extra Layer of Defence with MFA

Tip 3

Implementing multi-factor authentication (MFA) adds a layer of protection against unauthorised access to endpoints. You can significantly enhance your endpoint security by requiring users to provide multiple forms of identification— like a password, security token, or facial recognition.

Encourage users to adopt MFA across all devices to strengthen authentication mechanisms. Educate them on its importance and how it can deter cyber criminals even if they obtain their login credentials.

Pro Tips



Enable MFA for all user accounts, especially those with access to sensitive information.



Regularly audit MFA settings to ensure ongoing effectiveness.

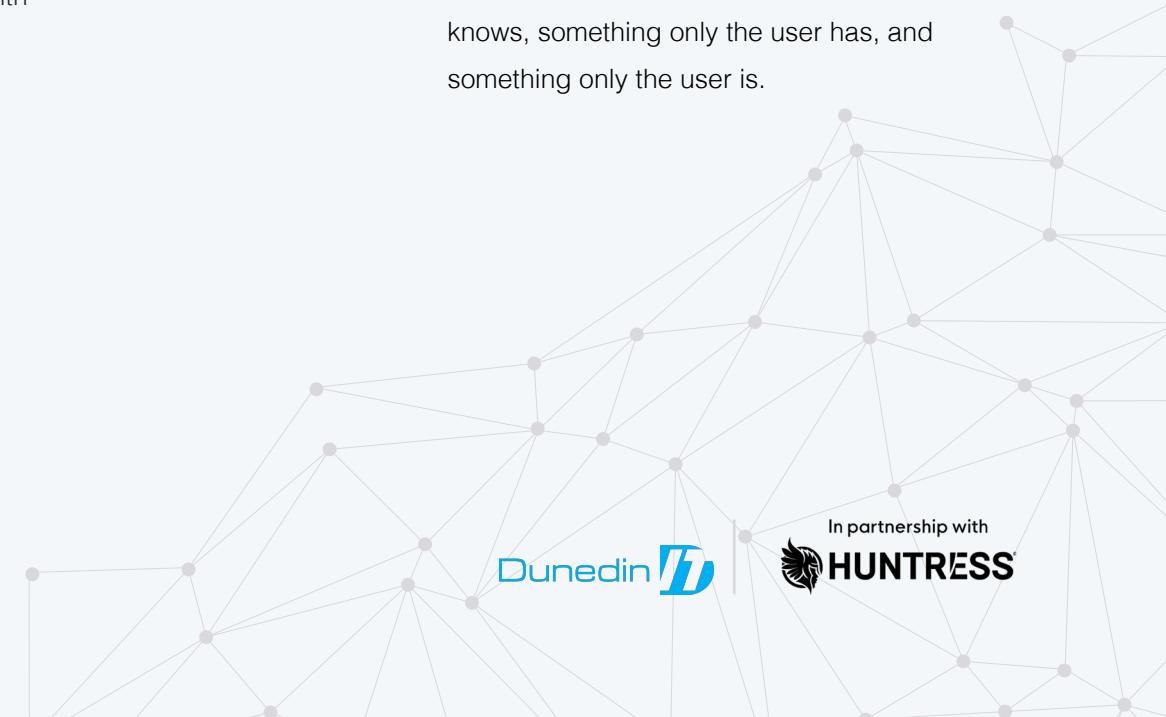


Pair MFA with single sign-on (SSO) to balance convenience and security.



What is MFA?

Multi-factor authentication, or MFA for short, is an authentication method that requires users to provide two or more verification factors before granting access. These factors typically include something only the user knows, something only the user has, and something only the user is.



Embrace the Principle of Least Privilege

Tip 4

Adhering to the principle of least privilege can help you strike the right balance between security and functionality. The principle of least privilege works by allowing only enough access for a user, program, or process to perform its function.

Limiting user access to the bare minimum needed for their roles reduces the risk of unauthorised access to endpoints. Make sure to review access permissions regularly to maintain security without slowing down day-to-day operations.

Pro Tips



Audit the access rights of users, programs, or processes to identify and minimise unnecessary privileges.



Use role-based access controls to align permissions with job responsibilities.



Set up regular reviews to keep the principle of least privilege effective over time.

Layer Up Your Endpoint Defences

Tip 5

Imagine building a fortress with multiple layers of defences. That's the concept behind defence-in-depth.

Combining firewalls, antivirus software, endpoint detection and response, and intrusion detection creates a robust security posture for endpoints and the broader network. This approach ensures that even if one layer is breached, others remain intact, providing a holistic defence against whatever hackers throw at you.

Pro Tips



Defence-in-depth usually involves a combination of physical security controls, technical security controls, and administrative security controls.



To determine what layers you need, look for gaps between system components where adversaries could find their way in.



Consider a managed cyber security solution to deploy and manage these multiple layers of defence.



What is defence-in-depth?

Defence in depth is a security strategy that leverages multiple layers of security to avoid a single line of defence and a single point of failure.

Prioritise Real-Time Endpoint Insights and Visibility

Tip 6

Speed and precision are critical in catching potential incidents early. The best way to have time on your side is to invest in endpoint security solutions that provide real-time monitoring and telemetry.

Real-time telemetry offers deep insight into the conditions and behaviours of all endpoints and the activities happening on them. This level of visibility can help reduce the risk of blind spots, detect abnormal patterns and behaviours, and catch threats that have circumvented other preventive solutions (like antivirus and firewalls). It can also serve as an early warning for potential security incidents.

Pro Tips



Look for security tools or managed solutions that have real-time monitoring capabilities.



Set up alerts to trigger when suspicious activities and anomalies are detected, or seek out solutions backed by a security operations centre (SOC) that can triage these alerts for you.



Regularly analyse telemetry data to identify trends and enhance your threat detection capabilities.



Did you know?

The global median dwell time is 16 days.

That means an attacker could be present in a target's environment for two and a half weeks before being detected!

Implement an EDR Solution

Tip 7

Endpoints are the new battleground for cyber attacks. To stand a fighting chance, you need the ability to detect known and unknown threats and respond to them quickly and efficiently. That's where an endpoint detection and response (EDR) solution can help.

EDR is designed to offer real-time monitoring and threat detection on the endpoint level, enabling businesses to respond quickly when suspicious activity is detected. Choosing an EDR solution can enhance your endpoint defences and provide helpful context like who, what, where, when, and how an attack may have occurred. That's what sets EDR apart from antivirus, firewalls, or other preventive solutions and why it's a complementary layer in any security stack.

Pro Tips



When choosing an EDR solution, keep your specific needs and budget in mind.



Look for an EDR solution that offers real-time detection and alerting, is easy to roll out and use, and plays nice with your other tools.



EDR solutions aren't "set it and forget it." Think about whether you have the right skill sets and ability to manage a solution on your own.



Evaluate if an unmanaged or a managed EDR solution is right for you.



What is EDR?

EDR stands for endpoint detection and response. EDR is an endpoint security solution designed to continuously monitor, detect, and enable investigations and responses to cyber threats.

Establish a Clear BYOD Policy

Tip 8

As employees bring their own personal computers, smartphones, or other devices into the workplace, this means more endpoints for you to defend and more potential entry points to fend off attackers. Establishing a bring-your-own-device (BYOD) policy can help mitigate potential risks while maintaining the flexibility and convenience of personal device use. A well-defined BYOD policy enforces guidelines for personal device use and ensures devices comply with security standards and are regularly monitored.

Pro Tips



Craft a comprehensive BYOD policy outlining usage and security requirements for personal devices in the workplace.



Look into mobile device management (MDM) tools to help enforce policies.



Regularly audit BYOD devices for both compliance and security adherence.



What is BYOD?

BYOD stands for bring your own device. An organisation's BYOD policy allows employees to use their own computers, smartphones, or other devices for work purposes.

Empower Your First Line of Defence with Regular Cyber Security Training

Tip 9

Users and employees are your organisation's first line of defence. Regular cyber security training sessions empower them with best practices for protecting endpoints and educating them about threats.

It's easy to create a culture of awareness without every employee needing a master's degree in cyber security. Security awareness training programs provide consistent education to help employees learn how to recognise and report potential security threats.

By turning employees into active participants in your security efforts, you can strengthen the human element of your defence at the endpoint level and beyond.

Pro Tips



Conduct regular security awareness training sessions for all employees.



Provide clear guidelines on recognising and reporting security incidents.



Put your employees' knowledge to the test through phishing simulations to check the effectiveness of your training or identify users who need more education.



Foster a culture of continuous learning, adapting training content to evolving threats.

Conduct Regular Risk Assessments and Audits

Tip 10

Think of risk assessments and audits as your cyber security health check-ups. Regular assessments are critical for evaluating the effectiveness of your endpoint security measures and contributing to a healthy security posture.

Regular assessments identify potential weaknesses and areas for improvement, while audits ensure compliance with security policies. This continuous improvement cycle allows you to adapt your strategies based on your findings, keeping your endpoint security strong and effective.

Pro Tips



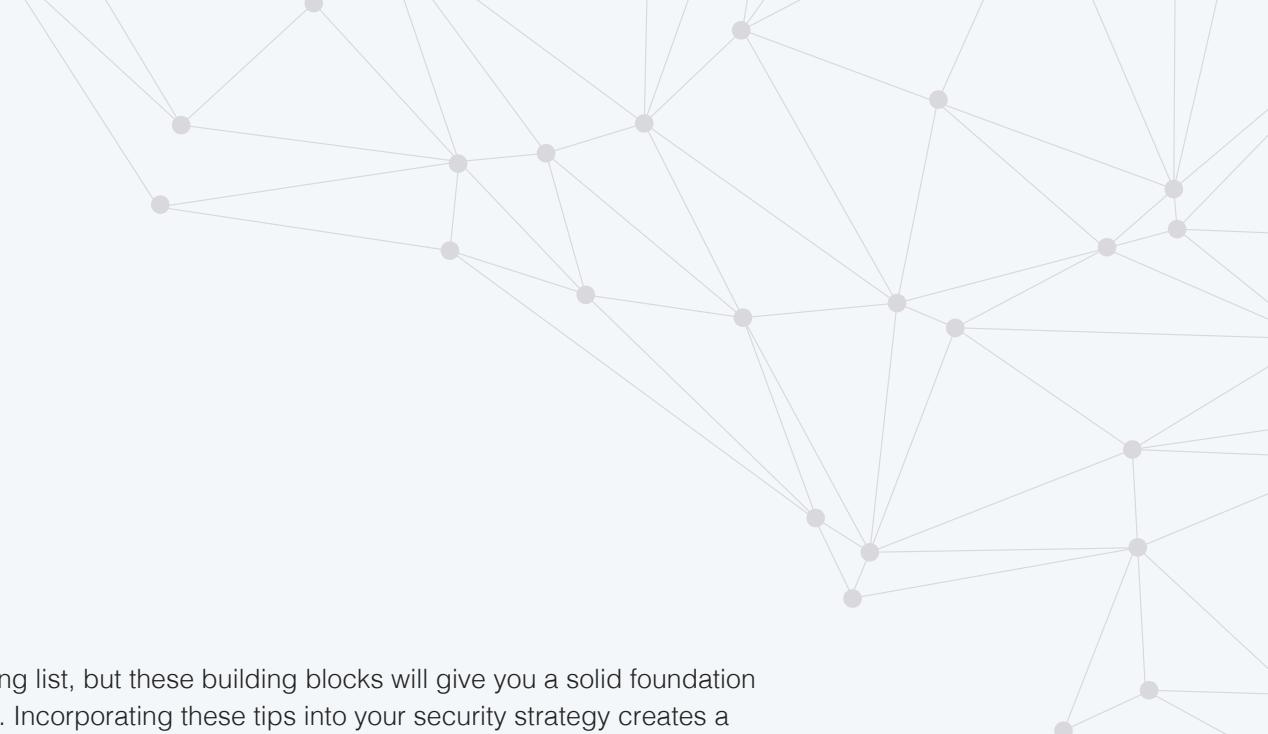
Schedule regular risk assessments to evaluate the effectiveness of your security measures, including endpoint security, network security, incident response, and more.



Perform thorough audits of endpoint security policies, configurations, and user compliance.



Establish a feedback loop to implement improvements based on assessment and audit findings.



This isn't an all-encompassing list, but these building blocks will give you a solid foundation for your endpoint security. Incorporating these tips into your security strategy creates a resilient defence so your organisation can confidently navigate today's threat landscape.

Contact us for more cyber security tips.

Contact Us

Website <https://www.dunedinit.co.uk>

Email sales@dunedinit.co.uk

Phone Number **0330 058 1701**

Dunedin 

In partnership with
