10 Endpoint Security Tips You Should Know

HUNTRESS

Introduction

In today's digital world, where connectivity is king, endpoints serve as the gateway to a business's digital kingdom. But because of this, endpoints are one of hackers' favorite targets.

According to the IDC, **70% of successful breaches start at the endpoint.** Unprotected endpoints provide vulnerable entry points to launch devastating cyberattacks. And with IT teams 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 even start? That's where this guide comes in.

We've curated the top 10 must-know endpoint security tips that every IT and security professional 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 with confidence.

Tip 1

Know Thy Endpoints: Identifying and Understanding Your Entry Points

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

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

Pro Tips

- Utilize asset management tools to maintain an updated inventory of all endpoints.
- Categorize endpoints based on their functions and importance to the organization.
- Prioritize 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.

Tip 2

Develop a Proactive Patch Strategy

Regularly updating operating systems and applications is the bedrock of endpoint security. Developing a proactive patch management strategy ensures that known vulnerabilities are promptly addressed, reducing the risk of exploitation by cybercriminals. 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.

Prioritize 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 minimize disruptions.

Tip 3

Add an Extra Layer of Defense with MFA

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

Encourage users to adopt MFA across all devices to strengthen authentication mechanisms. Educate them on its importance and how it can deter cybercriminals 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.

Tip 4

Embrace the Principle of Least Privilege

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.

By limiting user access to the bare minimum needed for their roles, you reduce the risk of unauthorized access to endpoints. Make sure to regularly review access permissions to maintain security without hindering day-to-day operations.

Pro Tips

Audit the access rights of users, programs, or processes to identify and minimize 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.

Tip 5

Layer Up Your Endpoint Defenses

Imagine building a fortress with multiple layers of defenses. That's the concept behind defense-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 defense against whatever hackers throw at you.

Pro Tips

- Defense-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 cybersecurity solution to deploy and manage these multiple layers of defense.

What is defense-in-depth?

Defense in depth is a security strategy that leverages multiple layers of security measures to avoid a single line of defense and a single point of failure.

Tip 6

Prioritize Real-Time Endpoint Insights and Visibility

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.

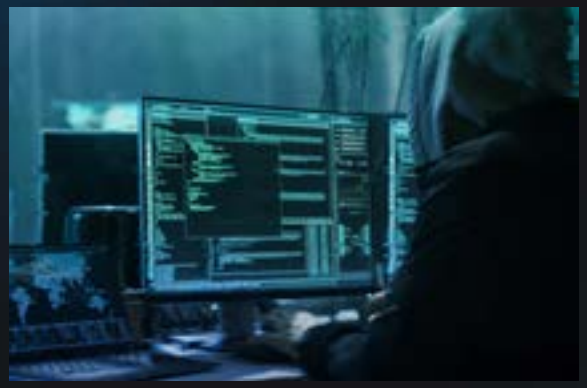
Real-time telemetry offers deep insight into the conditions and behaviors of all endpoints as well as the activities happening on them. This level of visibility can help reduce the risk of blind spots, detect abnormal patterns and behaviors, and catch threats that have circumvented other preventive solutions (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 center (SOC) that can triage these alerts for you.

Regularly analyze 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!

Tip 7

Implement an EDR Solution

Endpoints are the new battleground for cyberattacks. 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 IT teams to swiftly respond when suspicious activity is detected. Choosing an EDR solution can enhance your endpoint defenses and provide helpful context like who, what, where, when, and how an attack may have occurred. That's really what sets EDR apart from antivirus, firewalls, or other preventive solutions and why it's a complementary layer in any security stack.

Pro Tips

- 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.

Tip 8

Establish a Clear BYOD Policy

As employees bring their own personal computers, smartphones, or other devices into the workplace, that means more endpoints 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. A BYOD policy allows the employees of an organization to use their own computers, smartphones, or other devices for work purposes.

Tip 9

Empower Your First Line of Defense with Regular Cybersecurity Training

Users and employees are the first line of defense in any organization. Regular cybersecurity training sessions empower them with best practices for protecting endpoints and knowing what threats they should look out for.

It's easy to create a culture of awareness without every employee needing a master's degree in cybersecurity. Security awareness training programs provide consistent education to help employees learn how to recognize and report potential security threats. By turning employees into active participants in your security efforts, you can strengthen the human element of your defense at the endpoint level and beyond.

Pro Tips

Conduct regular security awareness training sessions for all employees.

Provide clear guidelines on recognizing and reporting security incidents.

Put your employees' knowledge to the test through things like phishing simulations to check the effectiveness of your training or see which users could use some more education.

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

Tip 10

Conduct Regular Risk Assessments and Audits

Think of risk assessments and audits as your cybersecurity health check-ups. Conducting regular assessments is 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. By incorporating these tips into your security strategy, you'll create a resilient defense and ensure your organization can confidently navigate today's threat landscape.

Want even more cybersecurity tips and expertise? Check out the Huntress Blog or peruse our library of educational resources.

About Huntress

Huntress is the leading cybersecurity partner for small- and mid-sized businesses (SMBs) and the managed service providers that support them. Combining the power of the Huntress Managed Security Platform with a fully staffed 24/7 Security Operations Center (SOC), Huntress provides the technology, services, education, and expertise needed to help SMBs overcome their cybersecurity challenges and protect critical business assets. By delivering a suite of purpose-built solutions that meet budget, security, and peace-of-mind requirements, Huntress is how SMBs defend against cyberattacks.

Founded in 2015 by a group of former National Security Administration (NSA) operators, Huntress has more than doubled over the past couple of years to protect more than 2 million endpoints, supporting 3,800 partners and more than 115,000 organizations. The company recently closed a $60M series C led by Sapphire Ventures. For more information, visit huntress.com or follow Huntress on social media at @HuntressLabs on Twitter, Facebook, or LinkedIn.

HUNTRESS.COM

HUNTRESS