ABSOLUTE®

Best Practices for Endpoint Visibility

absolute.com

Endpoints — they are literally everywhere (and multiplying by the day).

In fact, 74% of information workers use at least two devices, and 52% use three or more. From laptops and mobile devices to virtual desktops and IoT systems, today's enterprise environment is more connected and distributed than ever. But connectivity comes with great risk.

Cyberattacks are increasingly targeting endpoints as the weakest link, and without consistent visibility, organizations are vulnerable. So, how do you track and secure all these devices?

This is why endpoint visibility is mission-critical in today's world. Your IT and security teams need to be able to detect rogue devices, identify policy drift, and respond to threats confidently. A solid endpoint visibility strategy gives you the real-time insight you need to stay in control.

Let's walk through seven proven best practices for improving endpoint visibility across your organization — so you can reduce risk and protect your data at scale.

74%

of information workers use 2 or more devices

52%

use 3 or more devices

What Is Endpoint Visibility?

Endpoint visibility is the ability to continuously monitor, analyze, and secure all devices (laptops, mobile phones, servers, IoT endpoints) connected to your network. It provides IT and security teams with a real-time, centralized view of endpoint activity. This allows them to detect vulnerabilities, enforce security policies, and respond to threats before they escalate.

Historically, organizations relied on antivirus tools and perimeter-based defenses to secure environments. But those measures fall short in a distributed, cloud-first world. Today's endpoints aren't confined to a corporate office. They move across networks, regions, and access points. All of this introduces new layers of complexity for modern security teams.

With remote work, hybrid infrastructures, and an explosion of unmanaged and mobile devices, maintaining full visibility across all endpoints is no longer optional.

And yet, 68% of organizations say they can't see all their devices. This creates blind spots that attackers exploit.

For endpoint visibility, IT pros are now using modern solutions such as:

- **Endpoint Detection and Response (EDR)** - These tools collect continuous telemetry from endpoints to identify suspicious behavior (e.g., unauthorized access attempts) and vulnerabilities and automate responses (e.g., isolating the compromised endpoint).
- **Extended Detection and Response (XDR)** - These platforms build further on EDR technology by correlating data from endpoints, networks, and cloud services to provide broader context and faster threat response.
- **Complementary tools** - These include things like asset management systems and SIEM platforms, which help aggregate and analyze this data to provide real-time insights.

Resilient endpoint visibility is now a foundational requirement for modern cybersecurity Without it, it's nearly impossible to track assets, enforce compliance, or contain threats.

Why Endpoint Visibility Matters for Cybersecurity

By 2030, more than 125 billion connected devices are expected to be online. Without full visibility, organizations are effectively operating in the dark.

Remote work and BYOD policies have only increased the urgency. A recent study found that **84% of organizations globally** have adopted BYOD, but **only 52%** have official policies in place. That means many employees use personal devices to access corporate resources without clear guidelines or proper oversight. These unmanaged devices often lack basic security controls (like up-to-date software or strong access management).

Endpoints are now the frontline of cyber defense — and the prime target for attackers. The ability to monitor, secure, or respond to threats across a sprawling attack surface early is critical. But here's the truth: **you can't protect what you can't see**.

Endpoint visibility provides the continuous telemetry and real-time insight needed to identify issues before they turn into full-scale breaches. It gives IT and security teams the control and context they need to maintain system integrity across every device.

Challenges for Modern Endpoint Visibility

Achieving full endpoint visibility is increasingly complex. Beyond the growing volume of endpoints and evolving cyber threats, several operational and technical challenges make visibility a moving target. Understanding these obstacles is the first step toward building a stronger, more resilient security posture.

Shadow IT and Unmanaged Devices

Employees often introduce unauthorized devices or applications into the environment (a practice known as shadow IT). While it's convenient for users, these unmanaged endpoints create blind spots that traditional monitoring tools can't track. Without visibility into these endpoints, attackers can easily exploit those blind spots.

The Rise of Remote Work and BYOD Policies

The rise of remote work and bring-your-own-device (BYOD) policies has significantly expanded the attack surface. During the COVID-19 pandemic, cyberattacks on remote workers surged by 238%. Employees now access corporate data from personal laptops, tablets, and smartphones — often over unsecured networks. This decentralization makes it harder for IT teams to enforce consistent policies and maintain visibility across all endpoints.

Gaps in Legacy Security Tools

Many legacy tools were not designed to achieve real-time visibility across today's distributed environments. They often lack the telemetry, automation, and integration needed to detect and respond to threats at scale. But without continuous endpoint monitoring and analytics, gaps may remain undetected until it's too late.

Wide-Ranging Endpoint Ecosystems

Today's IT environments are more diverse than ever. An organization's tech stack may span Windows, macOS, Linux, mobile OSs, IoT devices, and cloud-hosted workloads. Achieving visibility across such a broad range of devices requires security solutions that can adapt to different infrastructures and integrate with various technologies.

7 Best Practices for Achieving Endpoint Visibility

The importance of endpoint visibility is clear. Here are 7 key strategies to overcome modern network challenges and take control of your security.

1. Implement Real-Time Monitoring

Real-time monitoring is a critical foundation for strong endpoint visibility. By continuously tracking the activity of every device (laptops, mobile phones, servers, and IoT) you can detect and respond to threats the moment they arise.

When teams catch unauthorized logins or unusual data transfers sooner, they can significantly reduce the risk of successful breaches by shrinking the window of vulnerability.

Beyond threat detection, real-time monitoring improves system performance and troubleshooting. By collecting data in a continuous stream, IT professionals identify and resolve endpoint issues with less downtime. This can improve user productivity and support compliance by making sure connected devices adhere to security policies.

But in order to achieve real-time monitoring, you need a sophisticated endpoint tracking solution. Absolute Visibility provides continuous analysis of all your devices — even if they go offline.

2. Enforce Strong Access Controls

Fortifying your access controls is a critical step in improving security across endpoints. It's about making sure that only authorized individuals have access to sensitive data and systems. Here are three key components to this strategy:

- **Role-Based Access Control (RBAC):** Assigns permissions based on users' roles within the organization. This way, employees access only the information necessary for their job functions. This enhances security and streamlines operations by reducing administrative overhead (which is costly and error-prone).
- **Multi-Factor Authentication (MFA):** Requires users to verify their identity through multiple methods — such as passwords combined with biometric verification or security tokens. MFA adds an extra layer of security which is harder for hackers to exploit.
- **Regular Access Reviews:** Audits and updates should focus on tailoring permissions periodically to align them with current roles and responsibilities. At the same time, you can set up policies to promptly revoke access for former employees or those whose roles have changed.

In addition to protecting sensitive information, implementing stringent access control measures helps your organization adhere to regulations like HIPAA and GDPR.

3. Conduct Regular Endpoint Security Audits

A regular endpoint security audit will systematically evaluate the security status of all devices connected to your network — including laptops, desktops, mobile devices, and servers. While real-time monitoring shows you what's happening *right now*, regular audits help you step back, check for problems, and make sure security policies are enforced. They help your team double-check that your systems and procedures are working the way they should be.

Here are some some basic steps for an endpoint security audit:

1. **Conduct a Complete Asset Inventory:** Maintain an up-to-date inventory of all endpoint devices so none are overlooked during the audit process.
2. **Assess Vulnerability:** Regularly scan endpoints for vulnerabilities such as outdated software, misconfigurations, or missing patches. Addressing these issues promptly reduces potential attack vectors.
3. **Review Access Controls:** Evaluate user access permissions to ensure they align with the principle of least privilege. This helps minimize the risk of unauthorized access.
4. **Verify Compliance:** Make sure all endpoints adhere to regulatory and organizational security standards, to avoid legal penalties and maintain trust.
5. **Review Incident Response Plans:** Test the effectiveness of your incident response plans related to endpoint breaches. Check for any obstructions that may prevent quick response.

4. Utilize Automated Threat Detection

Automated threat detection is a major upgrade in cybersecurity. The technology leverages artificial intelligence (AI) and machine learning to continuously monitor network activity and identify potential threats in real time. This proactive approach helps detect and respond to anomalies before they escalate into harmful security incidents.

This approach offers faster, more accurate, and cost-effective protection against cyber threats. In fact, organizations that use AI and automation can detect and contain breaches nearly 100 days faster than those relying on manual methods. These systems also reduce false positives by spotting real threats in large volumes of data, allowing security teams to focus their efforts where it matters most.

The real advantages here are speed and precision, which both improve security outcomes and lower the financial impact of breaches.

5. Train Users on Device Best Practices

Regular cybersecurity training is essential to equip employees with the knowledge and skills to protect endpoint devices against cyber threats. Human error remains a leading cause of security breaches, making it imperative for all staff to understand and implement best practices.

Device training should cover:

- **Recognizing Phishing Attempts:** Educate employees on identifying phishing emails and messages. Emphasize the importance of not engaging with suspicious links or attachments.
- **Device Security:** Teach every team member about securing both personal and work devices by keeping software updated, using strong passwords, and encrypting devices.
- **Adherence to Company Policies:** Make sure employees can aptly follow your organization's security protocols, including guidelines for remote work and data handling.

While this training should occur during onboarding, you should also establish an ongoing learning culture — to both reinforce knowledge and adapt to new threats. You can also try implementing practical simulations (such as mock phishing exercises). This helps employees put their knowledge into practice and enhances their ability to respond to real-world scenarios.

6. Encrypt Endpoint Communications

Whether it's an email, file transfer, or web traffic, encrypting endpoint communications is crucial for protecting sensitive data as it moves across network(s). By converting information into unreadable code, encryption ensures that **even if data is intercepted, unauthorized parties cannot decipher it**. This is especially important with highly-sensitive information like credit card and social security numbers, banking information, and patient medical details.

Without solid encryption, unprotected data is susceptible to interception by cyber attackers. This can lead to identity theft, financial fraud, and a loss of customer trust that can take years to rebuild.

The 2018 British Airways data breach exemplifies these risks. In this instance, attackers exploited vulnerabilities to access customer information via a malicious script which captured the personal and financial data of **nearly 380,000 customers**. This happened because the data in transit wasn't adequately encrypted (due to human error), allowing the attackers to steal it without immediately triggering alarms. Ultimately, the incident resulted in significant financial penalties and reputational damage for the airline.

To implement endpoint encryption, organizations should develop comprehensive policies that define which data requires encryption and the methods to be used (such as full-disk or file-level encryption). Likewise, secure protocols like **IPsec** ensure the authentication and encryption of data packets, which protects communications between devices. You will also want to provide encryption tools for remote and mobile devices (including removable media) to help maintain data security across all endpoints.

380k

Customers impacted by the 2018 British Airways data breach.

7. Ensure Regular Endpoint Updates and Patches

Software vendors release patches for several reasons — primarily to fix security vulnerabilities and enhance functionality. Applying these updates promptly helps protect your organization from cyber threats that exploit known weaknesses.

First, develop both a patch management policy and a regular update schedule. Establish clear guidelines outlining the processes for identifying, testing, and deploying patches. It's also a good idea to make this part of your endpoint audit schedule. The policy should define roles, responsibilities, and timelines, with critical security updates taking top priority (to mitigate higher-risk threats first).

Always test patches in a controlled environment before deployment. This helps identify potential compatibility issues and reduces the risk of disrupting work. You also don't want to deploy a patch that doesn't work or leaves you with an unknown vulnerability.

By keeping up with endpoint patches, you can significantly reduce your exposure to cyber threats and protect your reputation in your industry.

Absolute Visibility: The Key to Effective Endpoint Security

According to research from the Poneman institute, 68% of organizations experienced one or more endpoint attacks that successfully compromised data assets and/or IT infrastructure in the previous 12 months.

To mitigate these risks, maintaining comprehensive oversight of all endpoint devices is *crucial*. Absolute Visibility offers an all-in-one platform that helps organizations monitor, manage, and secure every device within their network.

Absolute Visibility empowers your team to:

- **Monitor All Devices in Real-Time on One Platform:** Gain real-time insights into each device's location, security status, and hardware/software inventory.
- **Analyze Device Usage:** Evaluate average daily device usage across various groups to detect underutilized devices or anomalous behavior.
- **Identify and Protect Sensitive Data:** Discover and manage sensitive information (such as personally identifiable information (PII) or intellectual property) across your device fleet to prevent data breaches and ensure compliance.
- **Track all Devices with Geolocation:** Maintain visibility over all enrolled devices, regardless of their connection to the corporate network.
- **Detect Threats Automatically:** Absolute Visibility automatically detects threats for you, so you don't waste time hunting them down.

Embedded in over 600 million devices, Absolute's Persistence® technology ensures continuous visibility and control — even if endpoints are tampered with or go offline.

If you're ready to empower your IT and security teams to proactively address risks, maintain compliance, and respond quickly to threats, Absolute Visibility is your answer. We secure your endpoints, so you never have to worry about gaps.

Final Thoughts

Endpoint visibility is absolutely essential in the modern device landscape. As cyber threats grow more advanced, organizations need full visibility into every device on their network to stay protected. Without it, vulnerabilities go unnoticed, and risks multiply fast.

Organizations with real-time visibility are better equipped to spot issues early and respond quickly to reduce the impact of attacks. While endpoint visibility alone isn't the whole solution, it's the foundation that enables faster detection, smarter decisions, and better outcomes when threats emerge.

Wondering how to put these practices into action? Absolute Visibility will give you the full picture of your entire device landscape, and the tools to stay ahead of threats.

Request a demo of Absolute Visibility today and take control of your endpoint security.

Request a Demo