What is Endpoint Backup and Why Do You Need it?

What is Endpoint Backup and Why Do You Need it?

Whether you experience a ransomware attack, lost or stolen device, or the accidental deletion of a file, a recovery solution is essential. Employee devices, and the network at large, carry critical business information that is often left out of company backup policies.

In these scenarios, an inadequate endpoint (PC's and laptops) backup option can result in lost data, lost time, and, more importantly, can impact employee productivity. An endpoint backup solution adds a layer of protection to prevent disruption to your business.

As the number of employees and organizations who work from home increased, so did the importance of an endpoint backup solution. The 2021 report "IDC FutureScape: Worldwide Small and Medium-Sized Business 2022", predicts that by 2023, 50% of SMBs will reorganize their company structure to remote and virtual employees. Removing employees from the physical corporate architecture leaves them open and vulnerable to attacks, mistakes, and errors on their devices.

Endpoint Risks: Why have an Endpoint Backup Solution?

In the 2020 State of Endpoint Security Risk report, 68% of IT professionals say the frequency of attacks against endpoints had increased over the past 12 months. 51% of IT professionals said they considered endpoint attacks to be successful because their endpoint security solutions don't accurately detect threats. The goal of Disaster Recovery Plans (DRPs) and backup strategies are to protect companies from the effects of disasters and attacks. These mainly focus on servers and storage, but what about endpoints? Endpoints themselves can pose a significant risk to company data.

Here are four reasons why having an endpoint backup solution is crucial for any business:

1. Protection against ransomware and other malware attacks
2. Easy data recovery in the event of a system crash or corruption
3. Reduced downtime in the event of a disaster
4. Peace of mind knowing that your data is always safe and sound

While accidental damage and theft still make up a large percentage of why users need their endpoints backed up, the limited protection offered by home networks has significantly increased the risks facing user data and company IP.

Effective Endpoint Security

Historically, endpoint protection meant using signature-based antivirus at each endpoint. However, today's threat actors have developed malware that bypasses these traditional AV solutions, driving the need for more effective endpoint security solutions.

Additionally, to protect a company's endpoints, other security precautions should be put into place, such as: Provisions for application whitelisting

- Multi-factor authentication
- Network access control
- Updated and patched software
- Advanced anti-malware software

Even with all of these protective measures in place, endpoint security is not complete without an endpoint backup solution. A key metric to any endpoint security plan is time to recovery. Having an effective and easy to use backup and recovery solution will ensure business operations are maintained with minimal disruption.

The Importance of Endpoint Data Protection

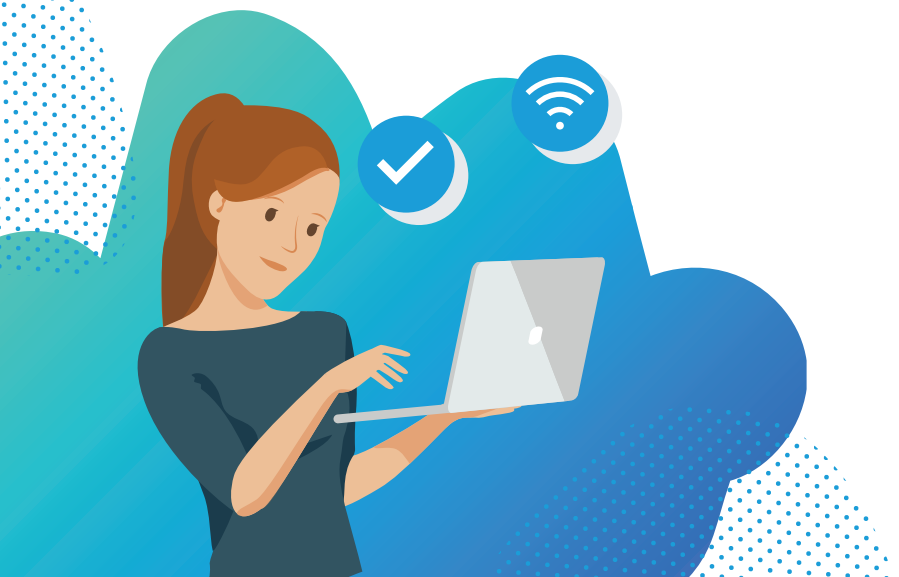
When other endpoint security measures fail—a device or data is lost, damaged, or attacked with ransomware—an updated backup of the endpoint becomes essential.

With it, the endpoint can be restored to its pre-disaster state quickly and easily.

Without it, important data is lost forever.

In industries such as healthcare, not properly securing and backing up endpoints can create a hole in regulatory compliances. In the event of a breach, this can lead to fines and damage to reputation.

Datto Cloud Continuity for PCs is an endpoint backup to assist you in your data protection strategy. Datto Cloud Continuity for PCs backups data to global data centers to ensure your cyber resiliency by protecting end users, your remote workforce, and endpoint devices.



How Endpoint Backup Solutions Work

Laptop and desktop backup solutions can range in functionality, from local hard drives, to file sync and share platforms, to file and folder only backup. Each of these options can come with shortcomings in the level of security, automation, validation, and recovery processes they offer.

Effective endpoint backup solutions protect every file on every device. They typically offer a centrally managed portal for configuration and an easy way to quickly restore backups.

The centralized management will show statuses of device backups and allow you to restore a single file or an entire system including applications, configurations, preferences and personalization quickly.
The agent on the device will back up any files that have changed since the previous backup to the cloud, limiting the exposure of the remote device.
Advanced functionality provides automatic backup checks to ensure backups are verified for a reliable recovery, validating every backup and providing an alert if there are any issues.

Endpoint Devices Should Enable Business

Allowing access to a business network from remote devices enables employee collaboration and innovation. Hindering access because of endpoint security concerns can do more harm than good. Enabling employees to access the network from their devices, while ensuring backup and protection, can empower them while protecting their data and network.

Datto Cloud Continuity for PCs offers a solution not only for the protection of endpoint business data on Windows-based computers, but also for streamlined recovery of the entire device configuration, setup, and applications. If you're ready to protect your business with an all-in-one backup and recovery solution, **contact us today.**