

Endpoint Protection for PCs & Servers



datto
A Kaseya COMPANY

Overview

Datto Endpoint Protection for
PCs

Datto Endpoint Protection for
Servers

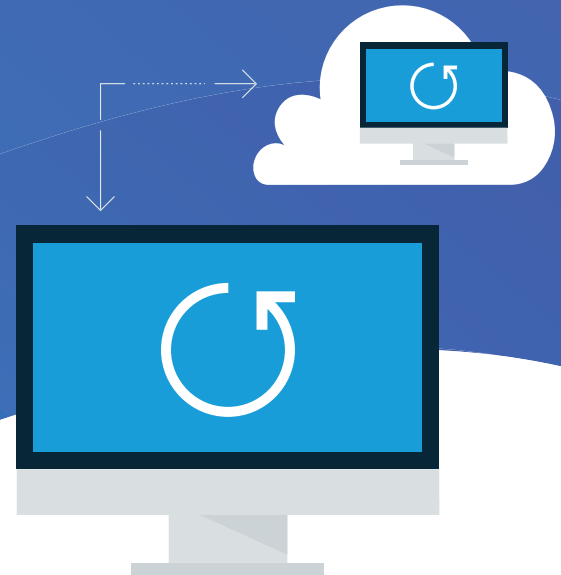
Additional Information

Datto SaaS Backup Protection
for Servers and PCs



Remote Data Backups, Inc.
Celebrating 25 Years
Datto Distributor
1.866.722.2587
sales@rdbu.com
www.remotedatabackups.com

Datto Endpoint Backup for PCs



Eliminate data loss and help your clients get their employees back up and running quickly with Datto Endpoint Backup for PCs. This reliable, image-based, all-in-one backup and recovery solution provides backup direct to the Datto Cloud, screenshot verification, and multiple layers of recovery capabilities, including Bare Metal Restore and File/Folder Recovery. In the event of a lost or stolen PC, accidental deletion, ransomware attack, or other disaster, MSPs can quickly and easily get their customer up and running, exactly as they had been before.

All-in-One Backup and Recovery for PCs

Whether it's because of a ransomware attack, lost or stolen device, or accidental deletion of a file, you can now confidently offer clients a solution not only for the protection of endpoint business data on their Windows based devices, but also for streamlined recovery of the entire device configuration, setup and applications.

- Easily restore individual files and folders
- Reliably recover from ransomware attacks
- Rapidly restore lost or stolen PCs
- Simplify admin self-service file/folder recovery for clients

Reliable PC Backups

PCs move between networks or get powered off, making it difficult to get reliable backups. Datto Endpoint Backup for PCs backup automatically pauses when the device has its connection interrupted and then automatically resumes once the connection is restored. Integrity checks, like Screenshot Verification, validate every backup and provide an alert if there are any issues. This takes the guesswork out and ensures backups are good for a reliable recovery.

Simple Deployment and Management

The Datto Endpoint Backup agent sits on the protected PC and connects directly to the Datto Cloud without the need for a local appliance. MSPs can easily purchase, manage, and monitor Endpoint Backup for PCs in the Partner Portal, the same place they do for other Datto products. Here they can pause and delete agents and view recent screenshots, as well as perform bare metal restore, point-in-time rollback, and file/folder restore.

Integrations with Autotask PSA and Datto RMM allow to streamline client billing, deploy agents and monitor backups easily and efficiently.

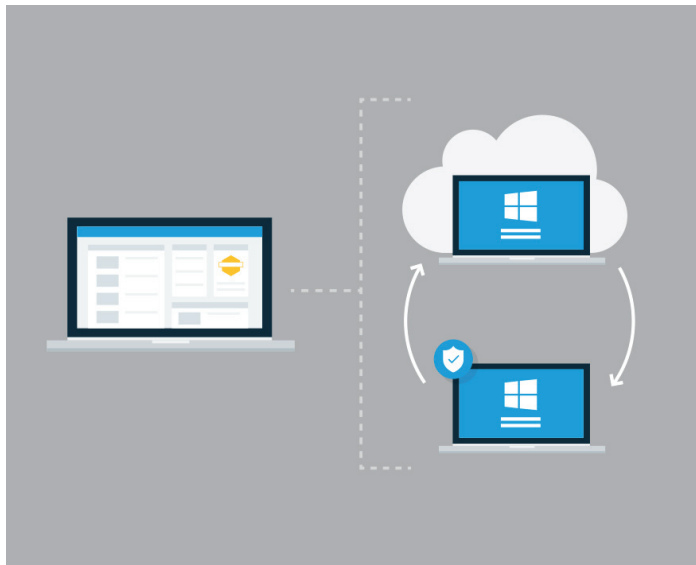
And automated Hero reports enable MSPs to easily prove the value of their services, positioning their offering as premium.

One Price, Zero Complications

Datto Endpoint Backup for PCs is designed to make it incredibly easy to resell and maintain consistent margins over time. No storage management is required, there are no surprise recovery charges, and backups are available with 1-year time-based retention (TBR) in the Datto Cloud.

Protect Business Data No Matter Where It Lives

Datto Endpoint Backup for PCs is part of Datto's entire Unified Backup product line, which includes complete protection for servers private or public cloud and SaaS data. With Datto Endpoint Backup for PCs, MSPs now have a powerful way to protect a broad range of PCs no matter where they operate from, opening up a even greater opportunity for partners to generate revenue while delivering the highest levels of business uptime.



Datto Endpoint Backup for PCs

Key Features

- Image-based cloud backup and recovery
- Automatic backup pause and resume
- Screenshot Verification
- File and folder restore
- Multi-volume support up to 1.5 TB
- Bare Metal Restore (BMR) including entire device configuration, setup and applications
- Admin self-service file and folder recovery
- No additional appliance required
- No storage management required
- One price, no additional fees
- Integration with Autotask PSA and Datto RMM

Operating System and Hardware Compatibility

- Supports Windows 11, 10 and 7 (64-bit)
- Requires 1 GB of free RAM on protected device
- Protects all selected volumes/partitions up to a combined 1.5 TB in size

Datto Endpoint Backup for Servers

Direct-to-cloud business continuity and disaster recovery solution for servers anywhere



datto
A Kaseya COMPANY

Datto Endpoint Backup for Servers is a unique business continuity and disaster recovery (BCDR) solution, designed exclusively for managed service providers (MSPs). It combines direct-to-cloud backup, powerful disaster recovery (DR) capabilities and a proven unified management portal.

Going beyond data centers

As businesses and IT infrastructures evolve, MSPs must be ready to protect and recover all critical server workloads regardless of where they are located. While it is easy to install a separate backup infrastructure in a data center, other locations may not be that simple.

Small businesses and remote locations

Whether on a bottom shelf in a mom-and-pop shop or in a utility room in a remote oil exploration site — the servers can be anywhere. It would be not feasible and sometimes may be outright impossible to put another backup device there, and the only option would be to back up directly to the cloud.

Distributed IT environments

Retail stores, restaurant chains or small customer service locations often house small servers to better serve customers. Space is at a premium, and a backup appliance may not be applicable. Direct backup to the cloud can help ensure business continuity across the entire service network.

Cloud virtual machines

Virtual machines (VMs) in the public IaaS clouds, such as Amazon AWS®, Google Cloud® and Oracle Cloud®, can be as important as on-premise servers for the continuity of your client's business. Adding backup infrastructure VMs could lead to unnecessary complexity and costs, with direct-to-cloud backup being an easy solution to protect the cloud workload.

Datto Endpoint Backup for Servers

Datto Endpoint Backup for Servers is purpose-built for MSPs. It offers direct-to-cloud backup without appliances, single pane-of-glass management, easy deployment and streamlined day-to-day operation — all delivered for a flat monthly fee.

It offers hourly replication to the secure and private Datto Cloud to provide rapid recovery during downtime, cyberattacks and outages.

Enterprise-grade protection

- **Trusted, comprehensive BCDR** built on Datto's proven SIRIS technology, delivering consistent management and protection across endpoints, servers and the cloud.

- **Secure architecture** protects each client with a single-tenant model and encrypted disks.
- **Outstanding resilience** with backup to the secure, reliable, geo-replicated Datto Cloud, which ensures better RTO and eliminates downtime risk

Rapid and reliable recovery

- **Hourly backups** to the secure Datto Cloud enable maximum redundancy and optimal RTO/RPO.
- **Rapid recovery** by instantly virtualizing a VM in the Datto Cloud or restoring it to the original or another location.
- **Streamlined restore** via a simple recovery process managed through a single, intuitive interface, allowing to recover multiple files, folders or the entire disk as required.

Built to scale for MSPs

- **Profitability and predictability** with unique, flat-fee pricing — no storage fees, no DR fees, no self-service DR testing fees, no support fees — eliminating the need to estimate costs or deal with unexpected charges.
- **Single pane of glass** to manage all Datto backups, organized in a client-centric view for consistent data protection across remote servers, data centers, Microsoft Azure, PCs and SaaS.
- **Easy deployment** and day-to-day management from a turnkey solution that is ready to use in a few clicks, increasing efficiency with smart features like screenshot verification, automated testing and email alerts.

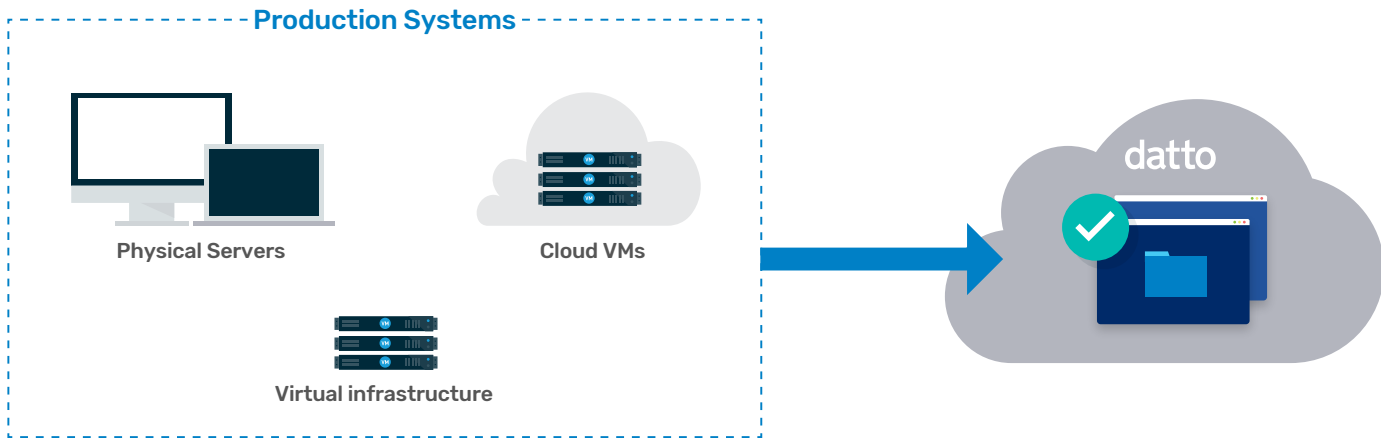
How it works

Datto Endpoint Backup for Servers backs up your clients' servers directly to the Datto Cloud every hour.

Datto Cloud

The Datto Cloud is purpose-built for cloud backup and disaster recovery. Its immutable architecture sets the standard for a secure cloud infrastructure with features like Cloud Deletion Defense.

- Multiregional presence to help you support geographically redundant backups.resilience and performance
- Consistent stack for you to protect client PCs, SaaS apps and servers.
- Cloud Deletion Defense for protection against ransomware, enabling access to deleted cloud snapshots when an agent is either mistakenly or maliciously deleted.
- Virtualization to Datto Cloud within minutes when you need to recover workloads outside of Azure.



Features and system requirements

Operating systems

- Windows Server 2022 / 2019 / 2016 / 2012 R2

Disk size

- Up to 6TB data per protected server

Instant virtualization in the Datto Cloud

- Run VMs in the Datto Cloud to simplify restore scenarios

Inverse Chain Technology™

- Send only changes to the cloud
- Get independent backups
- No rehydration, no synthetic backups, no recovery of chains link by link

Recovery options

- DR and DR testing in Datto Cloud
- Bare metal recovery (BMR) to the same or dissimilar hardware
- Export image to virtual machine format
- File/folder recovery

Single pane-of-glass management

- Monitor protected on-premises and cloud servers
- Client-centric status page with backup progress and settings
- Unified with Datto SIRIS and Datto Continuity for Microsoft Azure

Screenshot verification

- Confirm and share with clients that your backups are healthy, working and recoverable

Email alerting

- Receive alerts on the status of backups

Protecting business data wherever it lives

Datto Unified Continuity gives MSPs the comprehensive tools necessary to protect their clients' files and applications, whether they live on local servers, SaaS applications, end-user computers or the cloud. Datto offers data protection solutions built specifically for MSPs that are reliable regardless of the size of the infrastructure. With a wide array of restore options to match different recovery scenarios, Datto Continuity provides MSPs and clients peace of mind knowing critical business data can be restored in seconds and normal business operation can continue in the event of a disaster or data loss.



Datto SaaS Protection for Microsoft 365



Datto SaaS Protection ensures that MSPs can access, control, and most importantly protect their clients' Microsoft 365 data. As the leading cloud-to-cloud backup solution, SaaS Protection for Microsoft 365 offers an all-in-one backup, search, restore, and export solution for Exchange, OneDrive, SharePoint and Teams.

Microsoft 365 is Not Automatically Protected

As organizations increasingly move data into cloud-based applications, many believe that traditional best practices such as data backup are outdated. After all, SaaS applications are always available, accessible from anywhere, and highly redundant, so why is backup necessary?

An astonishing 1 in 3 companies report losing data stored in cloud-based applications. The single leading cause of this data loss? End-user error. Other common culprits include:

- Malware or ransomware attacks
- Malicious end-user activity
- Accidental data overwrites
- Canceled account subscriptions

With more and more companies depending on Microsoft 365 for collaboration and business operations, these risks are impossible to ignore. Backup is just as important in the cloud as in traditional on-premises IT systems. An independent, third-party, SaaS backup solution is the best way to protect organizations against the most common data loss pitfalls.

Protecting Your End Clients in the Cloud —A Shared Responsibility

Many organizations mistakenly believe that Microsoft 365 data is automatically protected. But, that's only partially true. Microsoft does ensure that it won't lose your data, but it does not make any guarantees about restoring data if you do. In other words, Microsoft 365 data is as vulnerable to accidental or malicious deletion, ransomware and other types of data loss as on-premises applications.

SaaS vendors like Microsoft promote a "shared responsibility" model. They are clear in recommending providers and end-users pursue third-party solutions to ensure they meet data protection, business continuity, compliance, and security requirements beyond Microsoft 365's limited native recovery capabilities.

Why SaaS Protection for Microsoft 365?

Trusted Backup

MSPs need complete confidence that clients' Microsoft 365 data is protected with a reliable, robust solution designed to reduce risk and time needed to manage backups.

- **Automated, continuous backups:** Protect Exchange, Tasks, OneDrive, SharePoint, and Teams with 3x daily backups or perform additional backups as needed at any time.
- **Streamlined client onboarding:** Get your clients' critical cloud data protected in a matter of minutes with a simplified setup and an easy click-through onboarding process.
- **Flexible retention:** Not all client environments are the same. That's why SaaS Protection offers different data retention options to meet clients' individual needs.
- **Intuitive, user-friendly management portal:** Quickly and easily determine the number of licenses in use, gauge profitability, and view clients' backup status all from a single pane of glass.

Fast & Effortless Restore

- **Point-in-time restore and export:** Quickly restore or export data from a specific point-in-time before a data loss event occurred.
- **Non-destructive restore process:** Quickly identify and recover individual objects or entire accounts with related records and folder structure intact.
- **Cross-user restore:** Restore data from one Microsoft 365 user account into another.
- **Retain user data:** Save money and effort by preserving inactive Microsoft 365 user data with SaaS Protection for as long as you need it.
- **Easy export:** Export entire accounts or specific items in standard file formats.

Effective Monitoring and Management

Have complete administrative control and proactively monitor your backup activities. Be confident in the status of all backup and recovery operations with detailed, actionable reports.

- **Backup monitoring:** Enables on-demand retrieval of events such as backup, export, or restore. Here you can see all of your successful and failed backup runs at the seat-level with error messaging around the root cause.

- **Admin audit log:** Maintain a detailed record of all administrator and user actions from your admin dashboard.
- **Multi-Admin roles:** Manage your accounts using roles such as Super Admin and multiple General Admin roles.

Predict Profitability

Build margin with bundled solutions that include protection for clients' Microsoft 365 data.

- **Simple, per-license pricing:** Deploy licenses across end clients, and redeploy them as needed.
- **Aggregated, volume-based discounting:** Discounts are based on total licenses sold across all of your clients.
- **Flexible subscription options:** Choose the best fit for each client with standard month-to-month contracts or discounted longer-term commitments.
- **Increase margins:** Build margin and add multi-layer protection for your Microsoft 365 clients by bundling Microsoft 365 and Datto SaaS Protection.

Data Protection and Compliance

Balance security and transparency with powerful controls and robust user lifecycle management. Protect valuable business data from accidental or malicious acts.

- **Security and compliance:** SaaS Protection backs up data in compliance with Service Organization Control (SOC 1/ SSAE 16 and SOC 2 Type II) reporting standards and supports your HIPAA and GDPR compliance needs.
- **Ransomware protection:** Roll-back data to a point-in-time before ransomware attacks.
- **Custom data retention:** Keep data indefinitely or adjust retention settings to meet compliance standards.



Datto SaaS Protection for G Suite



Datto SaaS Protection ensures that MSPs can access, control, and most importantly protect their clients' Google G Suite data. As the leading G Suite backup solution for MSPs, Datto SaaS Protection offers all-in-one backup, search, restore, and export for Gmail, Calendar, Contacts, and Shared Drives.

G Suite is Not Automatically Protected

As organizations increasingly move data into cloud-based applications, many believe that traditional best practices such as data backup are outdated. After all, SaaS applications are always available, accessible from anywhere, and highly redundant, so why is backup necessary?

An astonishing 1 in 3 companies report losing data stored in cloud-based applications. The single leading cause of this data loss? End-user error.

Other common culprits include:

- Malware or ransomware attacks
- Malicious end-user activity
- Accidental data overwrites
- Canceled account subscriptions

With more and more companies depending on G Suite for collaboration and business operations, these risks are impossible to ignore. Backup is just as important in the cloud as in traditional on-premises IT systems. An independent, third-party, SaaS backup solution is the best way to protect organizations against the most common data loss pitfalls.

Why Google Vault Is Not Backup

While Google Vault does include some primitive recovery capabilities, it does not protect against:

- **Data loss due to permanent deletion:** If an admin or end user permanently deletes data, files are only recoverable for a short period of time. Plus, it doesn't provide admins the granular control they need—only a restore of all deleted items in a 25 day window.
- **Data loss due to a ransomware attack:** If your business suffers a ransomware attack, Google doesn't allow you to roll-back your data to a point-in-time before the corruption occurred. If you cannot restore your data to the point before the attack happened, you end up losing not only your valuable business data, but also a hefty sum of money to criminals—without any guarantee your files will be unlocked, or any future protection from the same attack.
- **Time lost in recovering files:** The time it takes to recover data from the cloud might take longer than what your business can afford. It can take anywhere from minutes to weeks or longer to restore lost data.
- **Data loss due to inactive licenses:** As one would expect, an active G Suite license is required to access G Suite data. Unfortunately, inactive or deprovisioned user data is permanently deleted, and there is no rollback option.

Why SaaS Protection for G Suite?

Trusted Backup

MSPs need complete confidence that clients' G Suite data is protected with a reliable, robust solution designed to reduce risk and time needed to manage backups.

- **Automated, continuous backups:** Protect Gmail, Calendar, Contacts, and Shared Drives with 3x daily backups or perform additional backups as needed at any time.
- **Streamlined client onboarding:** Setup is fast and easy with a straightforward click-through onboarding process.
- **Flexible retention:** Not all client environments are the same. That's why SaaS Protection offers different data retention options to meet clients' individual needs.
- **Intuitive, user-friendly management portal:** Quickly and easily determine the number of licenses in use, gauge profitability, and view clients' backup status all from a single pane of glass.

Fast & Effortless Restore

- **Point-in-time restore and export:** Quickly restore or export data from a specific point-in-time before a data loss event occurred.
- **Non-destructive restore process:** Quickly identify and recover individual objects or entire accounts with related records and folder structure intact.
- **Cross-user restore:** Restore data from one G Suite user account into another.
- **Retain user data:** Save money and effort by preserving inactive G Suite user data with SaaS Protection for as long as you need it.
- **Easy export:** Export entire accounts or specific items in standard file formats.

Effective Monitoring and Management

Have complete administrative control and proactively monitor your backup activities. Be confident in the status of all backup and recovery operations with detailed, actionable reports.

- **Backup monitoring:** Enables on-demand retrieval of events such as backup, export, or restore. Here you can see all of your successful and failed backup runs at the seat-level with error messaging around the root cause.
- **Admin audit log:** Maintain a detailed record of all administrator and user actions from your admin dashboard.
- **Multi-Admin roles:** Manage your accounts using roles such as Super Admin and multiple General Admin roles.

Predict Profitability

Build margin with bundled solutions that include protection for clients' G Suite data.

- **Simple, per-license pricing:** Deploy licenses across end clients, and redeploy them as needed.
- **Aggregated, volume-based discounting:** Discounts are based on total licenses sold across all of your clients.
- **Flexible subscription options:** Choose the best fit for each client with standard month-to-month contracts or discounted longer-term commitments.

Data Protection and Compliance

Balance security and transparency with powerful controls and robust user lifecycle management. Protect valuable business data from accidental or malicious acts.

- **Security and compliance:** SaaS Protection backs up data in compliance with Service Organization Control (SOC 1/ SSAE 16 and SOC 2 Type II) reporting standards and supports your HIPAA and GDPR compliance needs.
- **Ransomware protection:** Roll-back data to a point-in-time before ransomware attacks.
- **Custom data retention:** Keep data indefinitely or adjust retention settings to meet compliance standards.