

Backup Buyer's Guide

Table of Contents

Introduction	3
Choosing where and how to back up your data	4
NinjaOne Endpoint Backup	6
NinjaOne Server Backup	7
Why SaaS platforms Need Backup	8
How NinjaOne delivers SaaS backup	9
Microsoft 365 Applications protected by NinjaOne SaaS Backup	10
Google Workspace SaaS Backup	11
NinjaOne Archiver	12
Why NinjaOne Backup?	13
About NinjaOne	14

Introduction

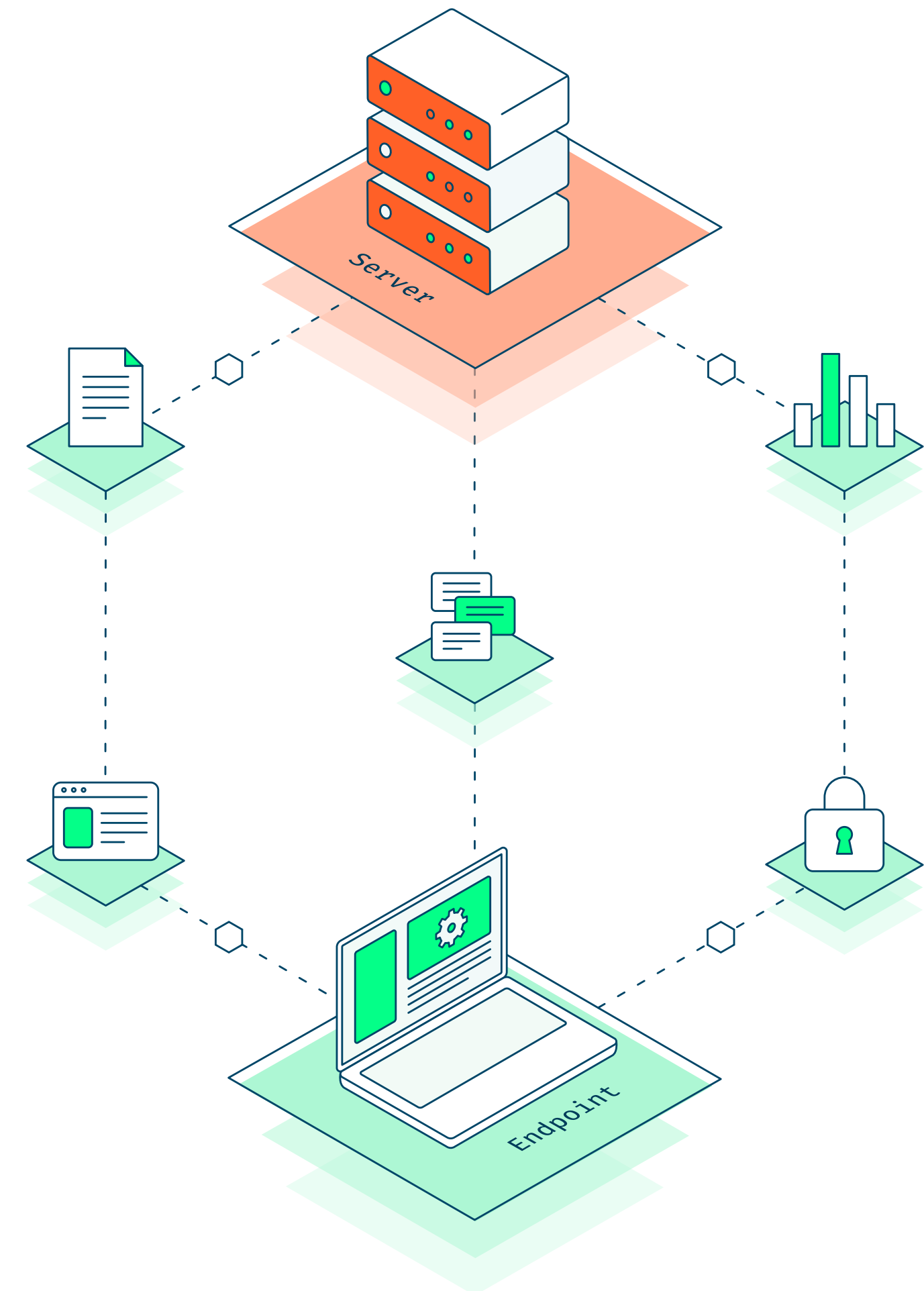
Backup isn't just about restoring lost data

It's about keeping your business running. In a world where endpoints, cloud productivity platforms, and compliance requirements are more critical than ever, you need a unified approach to backup and retention.

Modern backup solutions must cover the full spectrum of today's IT environments from user endpoints and critical servers to cloud-based productivity platforms. A robust backup strategy should include file and image-based protection for laptops, desktops, and physical or virtual servers to ensure fast recovery after ransomware, hardware failure, or accidental deletion.

Equally important is the ability to protect SaaS platforms like Microsoft 365 and Google Workspace, which often lack comprehensive, long-term backup capabilities. Businesses need solutions that offer automated, policy-driven protection for email, files, calendars, and collaboration tools—all managed through a unified platform that supports flexible storage, centralized visibility, and simplified recovery workflows.

This guide explores how NinjaOne safeguards every part of your data environment: from endpoints and servers to Microsoft 365, Google Workspace, and long-term archiving.



Choosing where and how to back up your data

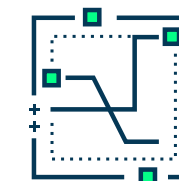
When it comes to backup, storage isn't just a technical decision—it's a strategic one. The right setup ensures you're protected and prepared. Whether you're optimizing for speed, security, scalability, or compliance, your storage strategy must match how your business runs.



Cloud storage gives you offsite, encrypted protection that grows as you do. It's a natural fit for cloud-first organizations and a lifeline in disaster recovery scenarios. With geo-redundant architecture and elastic scalability, cloud storage offers high resilience without hardware headaches. You get reliable protection with predictable, pay-as-you-go pricing and zero physical maintenance.



Local storage, on the other hand, is all about speed and control. For teams with strong on-prem infrastructure, keeping backups close to home means ultra-fast recovery, minimal latency, and no dependency on internet connectivity. It's a smart choice when you need tight control over data access, compliance zones, or recovery windows.

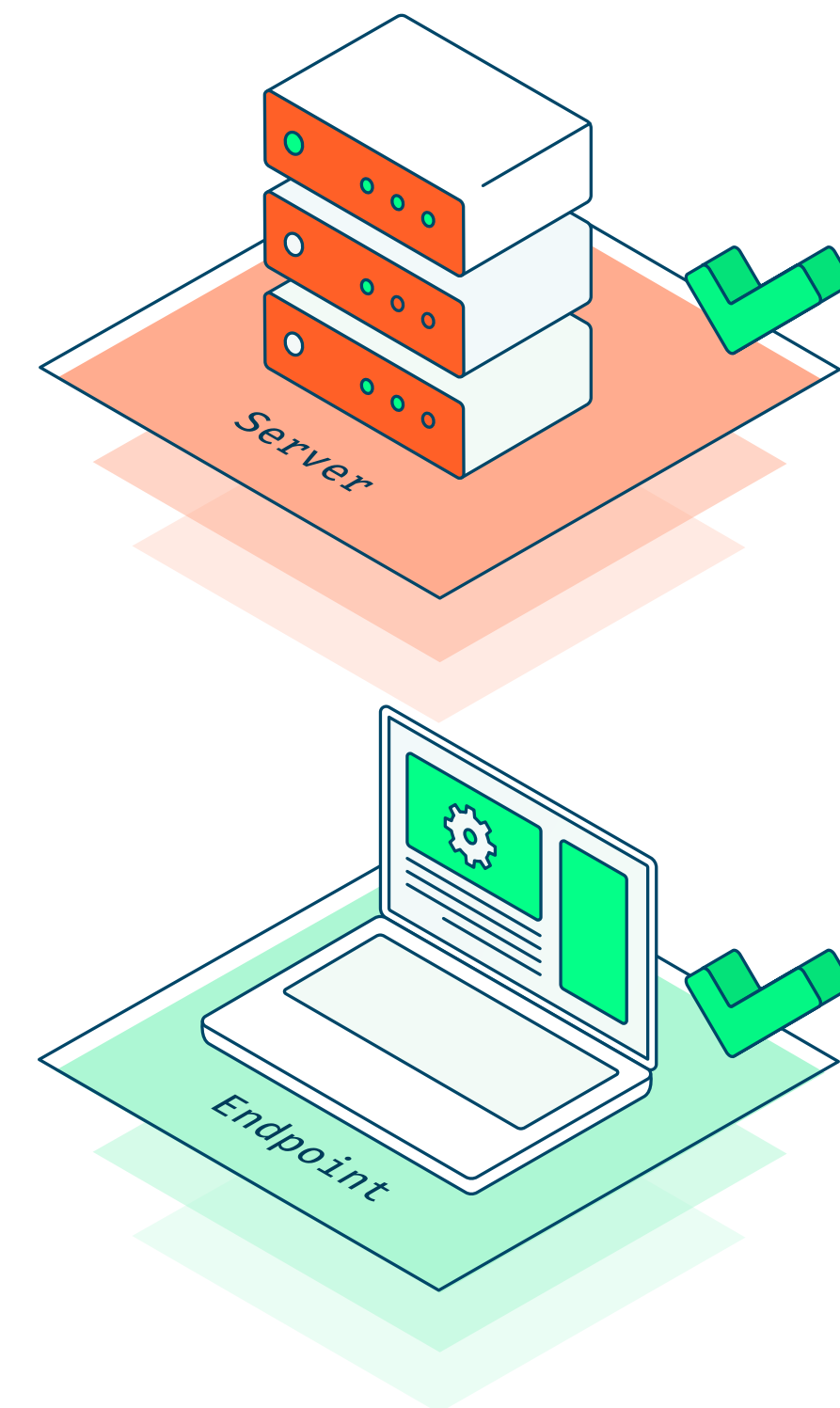


Then there's the hybrid approach, blending the cloud's resilience with local speed. It's the "best of both worlds" model that delivers fast, day-to-day restores while keeping a safety net in the cloud for larger-scale disruptions. Think local performance with cloud peace of mind. Beyond location, your infrastructure choice also comes down to how you operate.

Choosing where and how to back up your data *continued*

Cloud-based backup brings flexibility with minimal overhead. No hardware to buy or maintain, just automatic scaling to keep up with your data. Meanwhile, on-prem backup trades recurring fees for a one-time investment and full ownership of your storage environment.

Whatever your setup, make sure your solution supports a full range of recovery options: file-level restores, image-based backups, and complete system rebuilds with bare-metal recovery—clarity around deployment requirements—hardware, software, connectivity—matters too.



NinjaOne Endpoint Backup

NinjaOne Endpoint Backup protects laptops, desktops, and other end-user devices with secure, policy-driven backups. Built for hybrid workforces, it ensures that locally stored critical data remains protected and recoverable, no matter where the user works.

- + Perform file and folder-level backups with customizable schedules
- + Enable versioning for rapid restore of specific file iterations
- + Support remote recovery to mitigate risks from device loss, failure, or ransomware
- + Integrated seamlessly into NinjaOne's endpoint management platform for centralized visibility
- + File & folder-level backups with version control and fast recovery
- + Ideal for frequently accessed, user-generated content

NinjaOne Server Backup

NinjaOne Server Backup secures your on-premises and cloud-hosted servers with image-based and file-level backups engineered for business continuity. Whether protecting core infrastructure or specialized application servers, NinjaOne ensures rapid recovery, system rebuilds, and minimal downtime.

- + Create image-based backups for full system protection
- + Perform bare-metal recovery and disk-to-virtual restoration
- + Automate backup policies and retention schedules to suit business SLAs
- + Designed for critical workloads, including file servers, domain controllers, and application servers
- + Bare-metal recovery support for business continuity
- + Streamlined for disaster recovery scenarios

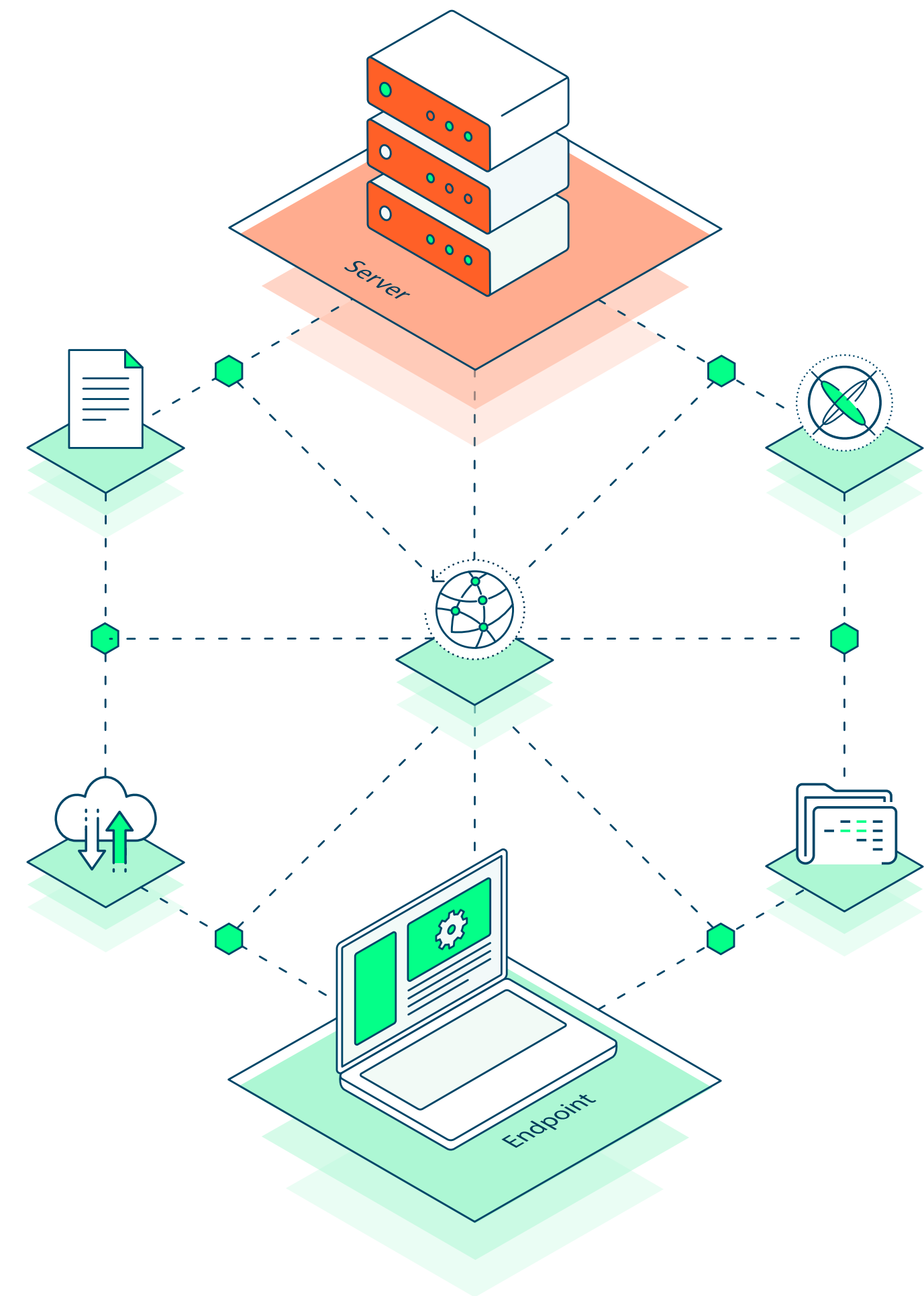
Why SaaS platforms Need Backup

While Microsoft 365 and Google Workspace are essential productivity platforms, neither is designed to provide true backup and recovery.

These services operate under a shared responsibility model, meaning that while the provider ensures platform uptime and availability, the responsibility for protecting user data—against accidental deletion, ransomware, or misconfiguration—falls on the organization.

In Microsoft 365, deleted emails are only retained for up to 30 days by default, and while tools like retention policies or litigation hold exist, they are complex to configure and not a substitute for comprehensive backup. Similarly, Google Workspace offers limited recovery windows and lacks built-in tools for point-in-time restores, immutable storage, or cross-user recovery.

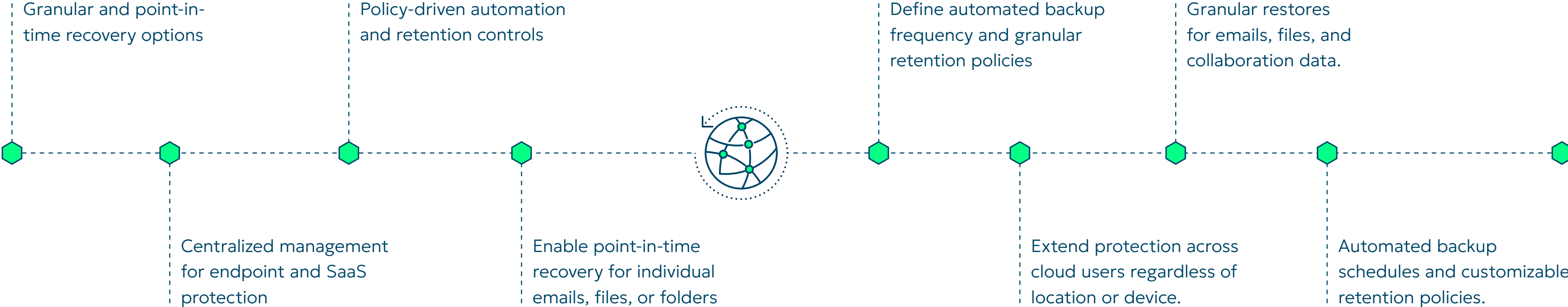
Choosing a third-party backup solution is essential to close these gaps, enabling automated backups, granular and point-in-time recovery, long-term retention, and support for compliance needs, all without relying solely on built-in platform limitations. Solutions like NinjaOne extend protection beyond what Microsoft and Google offer, ensuring that SaaS data remains secure, restorable, and under your control, no matter what happens.



How NinjaOne delivers SaaS backup *continued*

NinjaOne SaaS Backup delivers automated, cloud-native protection for Microsoft 365 and Google Workspace environments. It automatically backs up emails, documents, calendars, and more, guarding against accidental deletion, ransomware, and misconfiguration.

Built into the NinjaOne platform, SaaS Backup enables IT teams to manage cloud and endpoint backups from a single interface.



Microsoft 365 Applications protected by NinjaOne SaaS Backup



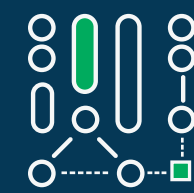
+ Exchange Online

Full mailbox backup, including inbox, sent items, folders, attachments, calendar entries, and contacts



+ OneDrive

Backup of files and folders stored in personal cloud storage



+ SharePoint

Protection for site collections, document libraries, and lists



+ Teams

Backup of team structure, channel messages, and associated files

Google Workspace SaaS backup



+ Gmail

Full backup of inbox, sent items, archived mail, and attachments.



+ Google Drive

Protection for files, folders, and shared drives (including Team Drives)



+ Google Calendar

Backup of event data and calendar metadata



+ Google Contacts

Backup of user contact information and directory entries

Note:

NinjaOne SaaS Backup does not directly back up Google Meet. However, if Google Meet recordings are saved to Google Drive, they are protected as part of Drive backups. Metadata such as chat, participants, and meeting history is not captured.

NinjaOne Archiver

NinjaOne Archiver is purpose-built for compliance, audit-readiness, and long-term retention of Microsoft 365 and Google Workspace email communications. It adds a layer of retention and legal protection on top of operational backup that's ideal for industries with strict regulatory requirements.

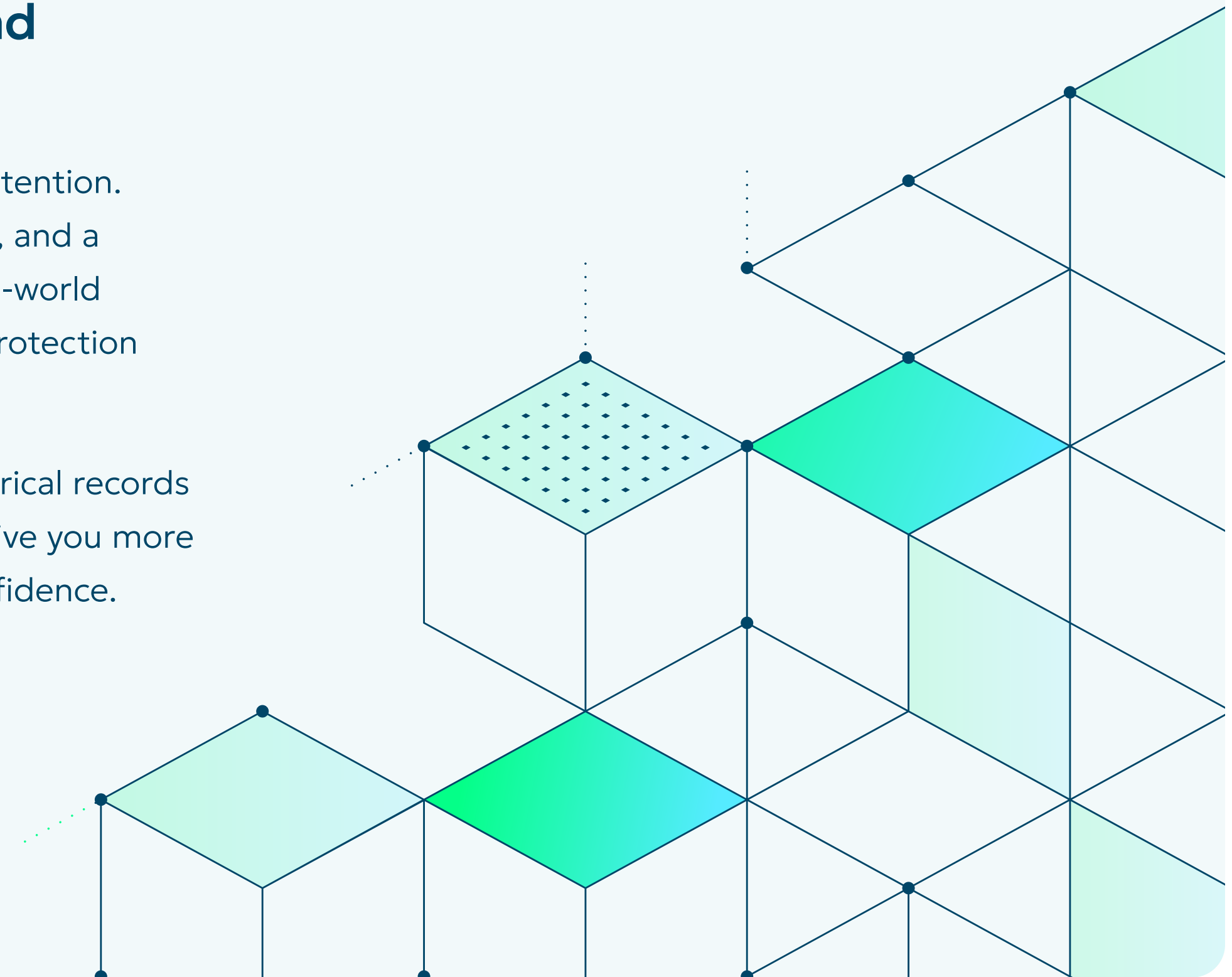
- + Capture and store email records in WORM-compliant, immutable storage
- + Support legal hold, e-discovery, and full-text search for litigation and audits
- + Enforce policy-based retention rules for HIPAA, GDPR, FINRA, SEC, and more
- + Enable compliance teams to preserve communications without burdening IT.
- + Ideal for meeting requirements like HIPAA, GDPR, FINRA, and SEC.

Why NinjaOne?

NinjaOne brings all your backup and archiving under one roof

Endpoints, servers, SaaS platforms, and long-term retention. You get centralized control, policy-based automation, and a ransomware-resilient architecture built to handle real-world threats: no juggling tools, no silos, just streamlined protection that scales with your needs.

Whether restoring live systems or locking down historical records for compliance, NinjaOne Backup and SaaS Backup give you more than recovery. It gives you continuity, clarity, and confidence.



About NinjaOne

NinjaOne, the automated endpoint management platform, delivers visibility, security, and control over all endpoints for more than 24,000 customers in 120+ countries.

The cloud-native NinjaOne platform automates endpoint management, patching, and visibility for environments at any scale. It is proven to increase productivity, reduce security risk, and lower costs.

NinjaOne is obsessed with customer success and provides free and unlimited onboarding, training, and support.

[Try NinjaOne for free](#)