Kaseya

# 365 USER

# SUBSCRIPTION COMPONENTS

# TABLE OF CONTENTS

Kaseya 365 USER

Kaseya

# 365 USER

## PREVENT

BULLPHISH ID

# Effortless Client Security Awareness Training for MSPs

The importance of conducting regular security awareness training that keeps up with the latest threats cannot be overstated. Having savvy, vigilant employees who recognize and avoid potential security threats and practice safe online behaviors drastically reduces the likelihood of a devastating cyber incident and fulfills compliance and cyber insurance requirements.

## CYBERATTACKS KEEP INTENSIFYING

Since employees form the core of any business, they will always be the main target of cyberattacks. The tactics used by cybercriminals are constantly evolving and so should your clients' approach to defense. Making sure your clients' end users pay careful attention and stay up to date with cybersecurity best practices is imperative.

**90%**
of security breaches are caused by human error

## LOWER CLIENTS' CYBER RISK LEVELS

Security awareness training and phishing simulations go hand in hand to reduce the likelihood of security breaches. Phishing simulations test employees on how they would respond to a real-life phishing attack. You can track which employees have clicked on links in the phishing email, opened an attachment or given away their password.

Once risky behaviors are identified, our platform delivers engaging educational videos to the users. Each video is accompanied by a quiz to test the training content retention.

Automated reporting lets you monitor ongoing progress and analyze and share metrics with clients to demonstrate the value of security training.

## MEET CLIENTS' CYBER INSURANCE AND COMPLIANCE NEEDS

**Security awareness training is now a requirement for obtaining cyber insurance coverage.** With the frequency and cost of cyberattacks escalating, it has become increasingly difficult to obtain a cyber insurance policy, leaving clients vulnerable to devastating recovery costs if and when an attack takes place. Help clients implement a user security awareness training program required to qualify for or to renew a policy.

**Ongoing security awareness training is required for compliance.** Help clients operating in healthcare, retail, government contracting and other sectors subject to regulatory oversight implement a security awareness training program to comply with industry regulations, like HIPAA, GDPR, CMMC, PCI-DSS, NIST 800-171 and others, and avoid incurring high fees for non-compliance.

**Reduce your clients' risk of experiencing a cyberattack by up to 70% with security awareness training.**

# PHISHING SIMULATION & SECURITY AWARENESS TRAINING

Ongoing, up-to-date employee cybersecurity training is a necessity in today's increasingly dangerous online threat environment. BullPhish ID educates and empowers your clients' employees, making them the best defense against cybercrime.

## YOUR TRUSTED PARTNER

Kaseya is trusted by MSPs around the world to deliver powerful IT security solutions. To ensure your success, we offer the best-in-industry channel partner program with done-for-you sales and marketing resources.

## EASY CAMPAIGN MANAGEMENT

Automated directory sync makes managing user groups for training and phishing campaigns easy and fast. Schedule campaigns for multiple clients at once and set up trainings weeks and months in advance to run automatically at designated times.

## CUSTOMIZABLE SIMULATIONS

Use our plug-and-play email templates to quickly launch phishing exercises or customize emails and sending domains to align with the needs of your clients and specific threats they may encounter.

## VIDEO-BASED TRAINING

Offer brief, engaging security and compliance training videos in eight languages. Test users' knowledge retention with online quizzes. **FREE BONUS FEATURE:** Upload your own training content.

## KEEP YOUR BRAND FRONT AND CENTER

Whitelabel the user training portal with your logo and/or your customer's logo and include your MSP's name in the portal URL.

## INSIGHTFUL REPORTING

Get automated reports showing your clients' phishing exercise and training campaign results. Assess your client' security posture and show the progress and value of training.

BULLPHISH ID

GRAPHUS

**Simple, Powerful, Automated!**

# Anti-phishing Defense for Microsoft 365 & Google Workspace

Graphus is a simple, powerful and cost-effective automated phishing defense solution that helps managed service providers (MSPs) quickly protect every inbox in a customer's organization from email-borne threats — whether they originate outside or inside a client's email platform.

Adding Graphus to your security stack enables you to improve clients' security posture by defending them from email-based cyberattacks, including phishing, spear phishing, business email compromise (BEC), account takeover (ATO), identity spoofing, malware and ransomware.

## How is Graphus unique?

To uncover these attacks, Graphus employs patented AI technology that monitors communication patterns between people, devices and networks to reveal untrustworthy emails. By focusing on the credibility of each interaction, Graphus identifies and blocks social engineering attacks targeting businesses and employees to keep your customers safe from today's biggest threats.

## Why add Graphus to your MSP security stack?

**Protect clients from costly security incidents and meet their security needs:**

- Help customers comply with industry regulations that require email security
- Help clients obtain or renew cyber insurance policies
- Keep customers informed with detailed email threat reports


**Increase revenue and become more profitable with:**

- Per-user pricing with aggressive margins
- Ability to target both Microsoft 365 and Google Workspace customers
- Powered Services, our partner portal that helps you market your services to drive new customer acquisition

**Enhance your productivity:**

- Deploy across customers' cloud email in minutes, with no email rerouting or agents to install
- Effortlessly manage multiple clients with our MSP-centric multi-tenant platform
- Seamless alerting and mitigation via integrations with other security tools and IT ticketing systems commonly used by MSPs

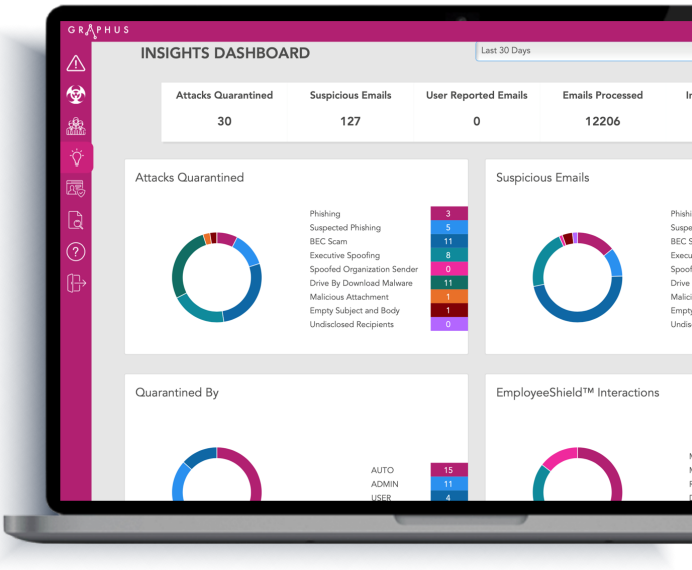
# 3 Layers of Defense for Microsoft 365 and Google Workspace Inboxes

**1. TrustGraph** automatically detects and quarantines suspected malicious emails that slip through clients' cloud email security or existing secure email gateway (SEG), preventing the end user from interacting with harmful messages.

**2. EmployeeShield** places an interactive warning banner at the top of suspicious messages to alert the end users and allow them to report an email as phishing, block it as junk or mark it as safe with one click.

**3. Phish911** empowers end users to bolster email security by proactively quarantining messages they deem suspicious for IT to investigate.

**Personal Graymail Filter** gives end users the ability to mark a message as junk with one click to stop receiving email from that sender – building a personal spam profile for each individual email recipient. The filter blocks the sender for that individual user only, so other end users within the organization who may want to continue receiving communications from that sender won't be affected.




**The intuitive and robust Graphus Insights Dashboard allows MSPs to monitor their customers'** real-time security posture, enabling them to quickly investigate and take action on detected threats. The reporting feature of the dashboard generates informative security metrics reports that MSPs can share with customers, demonstrating the value of their security services.

| GRAPHUS | VS | Secure Email Gateways |
|---|---|---|
| **ACTIVATION TAKES MINUTES**<br>Start protecting your customer's organizations instantly. No email configuration required. | | **ACTIVATION TAKES WEEKS**<br>An organization is left unprotected during the weeks or even months it takes to install an SEG. |
| **NO DELAY IN RECEIVING EMAILS**<br>Analyzes messages in real time with no delay in email delivery. Safe messages are never quarantined. | | **DELAYS EMAILS**<br>SEG filtering can cause delays in receiving messages or improperly quarantining safe messages. |
| **DETECTS ZERO-DAY ATTACKS**<br>Powered by patented AI technology, the TrustGraph® feature detects zero-day attacks in real time. | | **ZERO-DAY ATTACKS SLIP BY**<br>SEGs use traditional threat intelligence to detect attacks, allowing zero-day attacks to slip into inboxes. |
| **AUTOMATED PHISHING DEFENSE**<br>Integrates at the API level to detect sophisticated social engineering attacks. | | **LIMITED PHISHING DETECTION**<br>Built to stop spam and malicious emails, not sophisticated social engineering attacks. |
| **EMPLOYEESHIELD™ VISUAL NOTIFICATION**<br>Provides an interactive warning banner to notify your customers' employees of suspicious attacks and how to remediate threats. | | **EMPLOYEES AREN'T NOTIFIED**<br>Customers' employees are not warned of suspicious messages, leaving organizations extremely vulnerable to an attack. |

DARKWEB ID

## Actionable Threat Intel for Your Organization

With cyberthreats increasing every day, Dark Web ID helps ensure you are proactively protecting your company's brand, employees and executives.

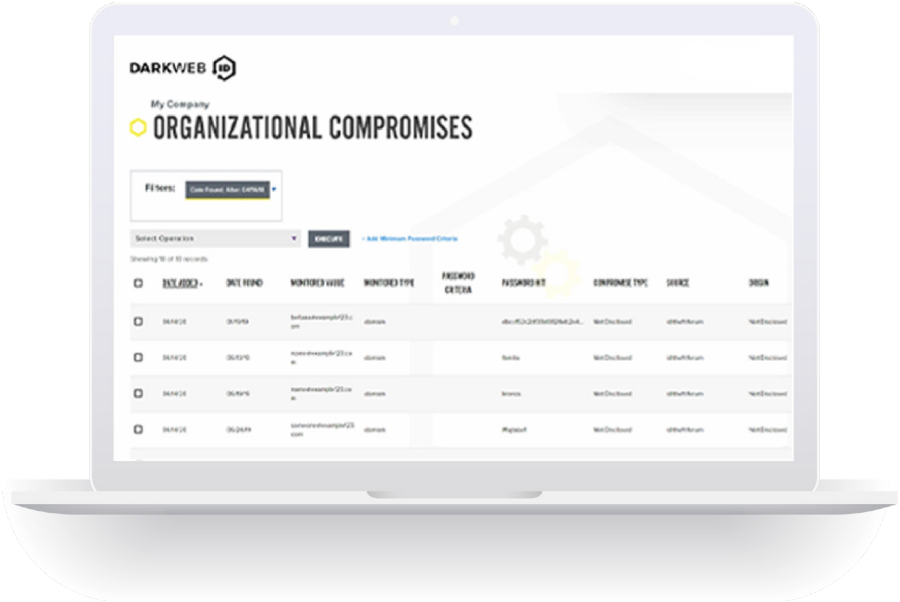
## Gain deeper awareness into your security gaps—before cybercriminals get the chance to exploit them and steal from you.

Stolen user credentials (email addresses and passwords) found on the dark web can indicate that your company or a third-party application or website used by your employees has been compromised—so you can take immediate action.

Cybercriminals traffic and buy stolen credentials so they can infiltrate your networks to steal your data. By monitoring the dark web for threat intelligence about stolen user data associated with your company's domains, you can be alerted when a compromise is detected and then respond to stop a potentially costly and devastating data breach.

**60%**

of the information available on the dark web could potentially harm enterprises




### MONITOR 24/7/365

- Hidden chat rooms
- Unindexed sites
- Private websites
- Peer-to-peer (P2P) networks
- IRC (internet relay chat) channels
- Social media platforms
- Black market sites
- 640,000+ botnets

# MONITOR, IDENTIFY AND MITIGATE THREATS

Your business security strategy extends far beyond your network, and Dark Web ID can help strengthen it. Easily monitor for exposure and leverage rich threat intelligence to take the appropriate actions that will protect your company's assets and reputation and lower the risk of breach.

### SAAS BUSINESS APPLICATIONS INCREASE RISK

Although web-based applications allow employees to do their jobs from most anywhere, they also open up your organization to risk. Payroll and HR platforms, CRM and marketing automation tools, travel sites, banking sites and social media accounts are accessed by your employees many times throughout a day. A recent survey shows that 65% of people reuse the same password for multiple or all accounts—potentially the same one they use to log in to your network.

### EMAIL MONITORING FOR HIGHLY TARGETED EXECS AND PRIVILEGED USERS

Your executives and administrative users often have greater access to systems, information and sensitive data. If their personal email credentials are compromised and they happen to reuse the same credentials at work, the attackers may use them to gain access to corporate systems. The attackers may also use social engineering to impersonate your executives to trick other employees to give up access, divert funds, or for other schemes. Therefore, it's important to monitor the personal mail addresses of your executive and administrative users along with their corporate email accounts.

### EXTEND SECURITY TO THE SUPPLY CHAIN

Some cyberattacks could happen due to exposure to third-party vendors from your supply chain. The interwoven systems of vendors and partners present security risks since data is shared across networks. The growing need for cyber supply chain risk management has prompted forward-thinking organizations to add dark web monitoring to vendor due diligence.

### QUICKLY PROVIDE YOUR IT SECURITY TEAM THREAT INTELLIGENCE

Are your security teams resource-constrained and focused on detecting and mitigating threats rather than installing new technology for monitoring? Dark Web ID takes just minutes to set up and will start showing compromise results right away. Reporting is flexible and can be integrated with your Security Operations Center (SOC) and other alerting and remediation platforms with available APIs.

### HOLISTIC VISIBILITY

By adding Dark Web ID monitoring to your security strategy, you will get a more complete picture of your company's security posture. Not only does it serve as an early warning mechanism that alerts you before breaches occur, it also provides invaluable data analytics to evaluate where employees need security awareness training or where multi-factor authentication and single sign-on are warranted.

DARKWEB ID

Kaseya

# 365 USER

## RESPOND

SaaS Alerts®

# Automatically Detect and Remediate Security Breaches in SaaS Applications

Imagine having a watchful protector that never sleeps, constantly guarding your clients' SaaS applications. Our platform does just that, detecting unauthorized access, and shutting it down without breaking a sweat.

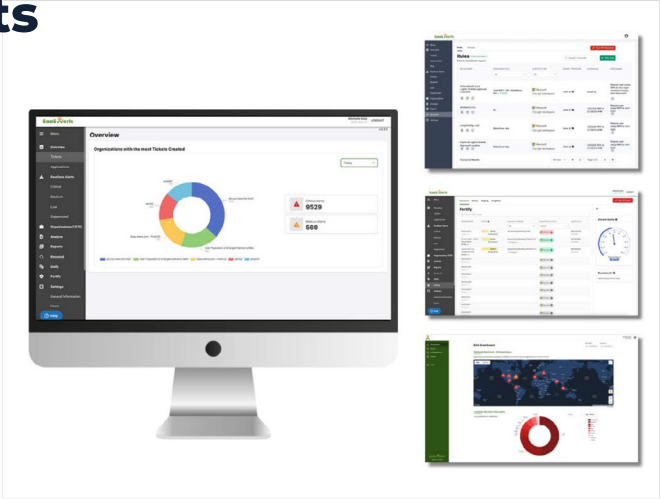

## The Most Comprehensive SaaS Security Platform Available

- MONITORING & ALERTING
- 24/7 DETECTION & RESPONSE
- SECURITY CONFIGURATIONS
- MONITOR MORE APPLICATIONS
- RMM & IT DOCUMENTATION TOOL MONITORING
- CUSTOMER & PROSPECT REPORTS

## How Does SaaS Alerts differ from MDR providers?

MDR providers rely on human "threat hunters" which are tasked with aggregating data from multiple sources and responding as quickly as possible, usually measuring response time in hours. SaaS Alerts provides alerting and remediation steps with actions taken within seconds of malicious activity **with no human interaction required.** This difference significantly minimizes the risk of data egress or malicious activity within your clients' most vulnerable environments

# A Deeper Look into SaaS Alerts



### MONITORING AND ALERTING
We use machine learning to aggregate and analyze user behavior in SaaS platforms. When unusual behavior is detected, you get an instant notification so you can take action fast.

### 24/7 DETECTION AND RESPONSE
SaaS Alerts automatically responds to detected threats and account compromises, temporarily disabling the account and blocking new login attempts. Automated threat mitigation occurs within minutes of detection and provides detailed forensic logs of compromised data and remediation steps.

### SECURITY CONFIGURATIONS
Microsoft security recommendations are complex and require a lot of time to implement. With SaaS Alerts, you can apply security recommendations across all your tenants in minutes and receive alerts if a security score regresses.

### BEYOND MICROSOFT 365
With our App Wizard, we can quickly integrate with any SaaS application with a viable API to pull mission-critical data into SaaS Alerts, so you can quickly detect and respond to SaaS security threats across almost all of your clients' SaaS applications.

### MSP TOOL MONITORING
MSPs have become prime targets for cyber attacks. SaaS Alerts offers complimentary protection for your own business, shielding you from impending threats by automatically alerting you when any unusual, high-risk behavior occurs within your MSP tool stack.

### USER IDENTITY VALIDATION
Reconcile device data with SaaS data to ensure only authorized users on authorized devices can gain access to critical company SaaS applications.

### INTUITIVE REPORTING
Powerful reporting of user behavior and SaaS application events provides a comprehensive and timely view of the current state of SaaS security for each of your clients — and allows you to both sell to and retain customers by demonstrating value.

## CORE APPLICATIONS WE PROTECT

Microsoft 365 · Google Workspace · slack · salesforce · Dropbox · okta · DUO · Microsoft Defender for Endpoint

SaaS Alerts®

Kaseya

# 365 USER

## RECOVER

datto | SAAS PROTECTION

# Comprehensive Backup for Microsoft 365 and Google Workspace

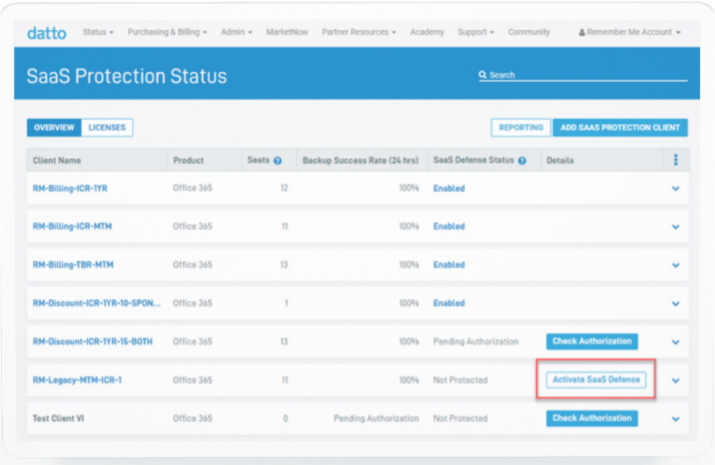
Your clients are making the move to the cloud to save time, simplify collaboration and free up valuable resources, but now it's up to you to protect that data. Under the shared responsibility model, Microsoft and Google guarantee application availability, but you're responsible for protecting data against ransomware, user errors, and other internal and external threats.

**But you can eliminate the fear and uncertainty of data loss with Datto SaaS Protection—a complete, reliable backup solution for Microsoft 365 and Google Workspace. SaaS Protection combines robust data protection, powerful backup automation, versatile recovery options and multi-layered data security for true peace of mind.**

**SIMPLIFY AND STREAMLINE BACKUP PROCEDURES**

**RECOVER WHAT YOU NEED, WHEN YOU NEED IT**

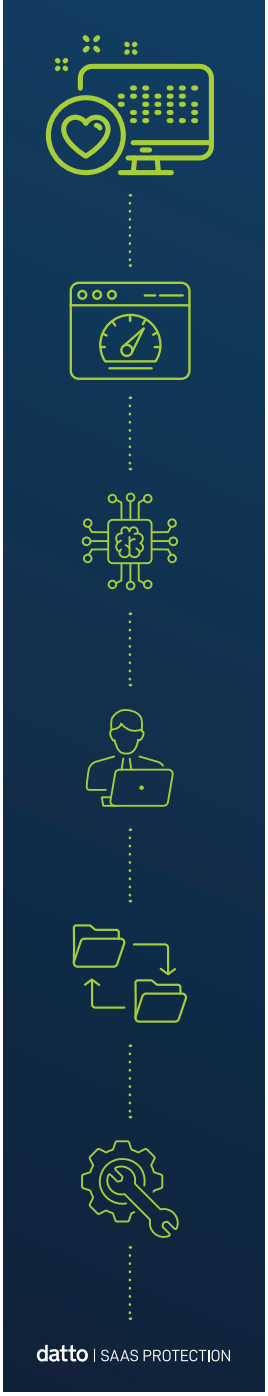
**KEEP YOUR SAAS DATA SECURE AND COMPLIANT**




SaaS Protection was designed to streamline the backup and recovery process for MSPs.

The platform provides powerful, yet easy-to-use capabilities. Accomplishing backup and restore of Microsoft 365 and Google Workspace data has never been so simple and intuitive.

# The SaaS Backup Solution MSPs Love




### AUTOMATED, CONTINUOUS SAAS BACKUPS

Protect Microsoft 365 and Google Workspace applications against accidental or malicious deletion, ransomware attacks, and other cloud data loss with 3x daily, automated backups.

### IMPROVED EFFICIENCY

Get new clients protected fast with streamlined onboarding and manage client backups from a single pane of glass. Whether you're protecting Microsoft 365 or Google Workspace data, our solution is fast, reliable and manageable at scale.

### COMPLETE CONTROL

Automated point-in-time SaaS backups capture relevant changes across both Microsoft 365 and Google Workspace in their entirety. Our solution also provides an independent backup copy of data outside of SaaS provider servers.

### RECOVER QUICKLY

Restore lost data quickly with flexible restore options such as point-in-time, granular, and non-destructive restore.

### BEYOND FILES AND FOLDERS

A true SaaS backup solution protects not just files and folders, but collaboration tools like Microsoft Teams, SharePoint, OneDrive, and Google Drive.

datto | SAAS PROTECTION

SPANNING

# Microsoft 365 and Google Workspace backup, purpose-built for SMBs

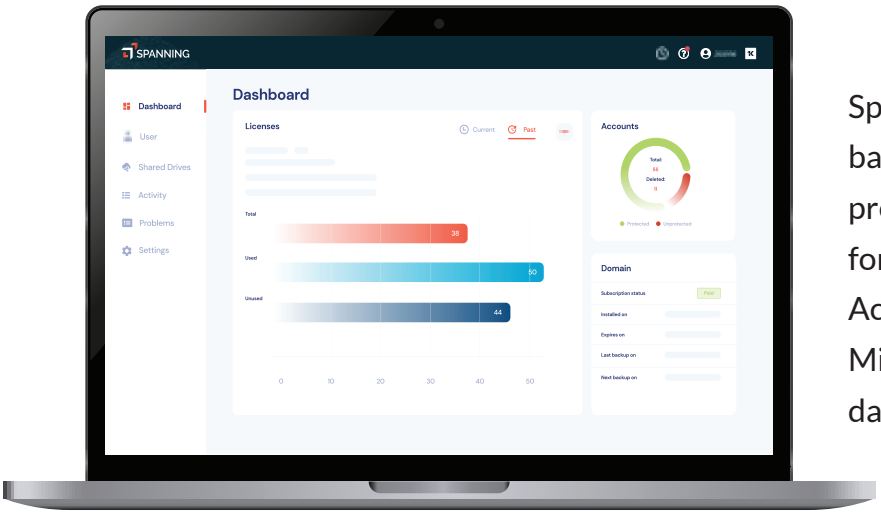
You've made the move to the cloud to save time, simplify collaboration, and free up valuable resources, but now it's up to you to protect that data. Under the shared responsibility model, Microsoft and Google guarantee application availability, but you're responsible for protecting data against ransomware, user errors and other internal and external threats.

**But you can eliminate the fear and uncertainty of data loss with Spanning—a complete, reliable backup solution for Microsoft 365 and Google Workspace. Spanning combines robust data protection, powerful backup automation, versatile recovery options, and multi-layered data security for true peace of mind.**

**24000+**
**BUSINESSES DEFENDED**

**2.5 MILLION USERS**
**USERS PROTECTED**

**3.9 BILLION**
**BACKUPS PER WEEK**




Spanning was designed to streamline the backup and recovery process. The platform provides powerful, yet easy-to-use capabilities for both administrators and end-users. Accomplishing backup and restore of Microsoft 365 and Google Workspace data has never been so simple and intuitive.

**SIMPLIFY AND STREAMLINE BACKUP PROCEDURES**
Say goodbye to backup headaches; daily, automated Saas backups and unlimited on-demand backups ease the burden and provide you with as many backup points as necessary.

**RECOVER WHAT YOU NEED, WHEN YOU NEED IT**
Powerful functionalities like granular search-based restore, point-in-time restore, and self-restore for end users allow you to recover effectively in a matter of minutes.

**KEEP YOUR SAAS DATA SECURE AND COMPLIANT**
Layered security, top-tier data protection practices, and extensive certifications with third-party regulations provide reassurance that your data is safe and up to code.

# SIMPLY SMARTER BACKUP & RECOVERY

### DAILY, AUTOMATED BACKUP

Spanning automatically completes daily backups as part of a recurring, incremental backup process. Each and every day, this auto-discovery and backup of new and/or altered content runs quietly in the background with zero additional effort from your admins or users. **Simply "set it and forget it."**

### CUSTOMIZABLE, ON-DEMAND BACKUP

If daily, automated backups don't provide you with enough backup points for comfort, you can supplement with on-demand backups as often as you like. These backups can be customized to your needs and are unlimited, allowing you to create as many backup points as necessary.

### GRANULAR, SEARCH-BASED RESTORE

Simply search, and once you've find the data you're looking for, you can choose to restore individual items, multiple items, or entire folders. Granular restore options afford you maximum control.

### END USER SELF-SERVICE RESTORE

Minimize the burden on admins by empowering your end users with Spanning's self-service restoration capabilities. Licensed users may be permitted to restore their own files, folders, and content. With zero IT intervention, restores can be accomplished quickly to ensure maximum productivity.

### ROBUST ADMIN FUNCTIONALITY

Manage backups effectively with admin capabilities such as cross-user restore. Admins are able to restore data back into original user accounts, or into a different user's account altogether. Admins can also customize backup settings and distribute licenses to align with organizational needs.

### ON-THE-GO, MOBILE ACCESS

Spanning was designed to accommodate the mobile-first, cloud-first mentality and on-the-go nature of today's workforce. The mobile-friendly user interface enables accurate restore of Microsoft 365 data anytime, anywhere. All you need is a Microsoft supported desktop, tablet, or mobile device.

## MULTI-LAYERED SECURITY

**HIGH AVAILABILITY**

99.9% uptime SLA
(service level agreement)

**DATA ENCRYPTION**

128-bit SSL in transit
and 256-bit AES at rest

**GLOBAL DATA CENTERS**

AWS data centers located in the U.S., Canada, EU, UK, and APAC regions

**ACCESS CONTROL**

Production server access is granted only to named Spanning employees who have specific operational requirements

**INTRUSION DETECTION**

Active guard with log analysis file integrity checking, policy monitoring rootkit detection, real-time altering and active response

**CREDENTIAL PROTECTION**

Optional dark web monitoring alerts of compromised accounts and credentials

**COMPLIANCE CERTIFICATIONS**

HIPAA, GDPR, ISO 27001, SOC 2 Type II ISSAE 16 & ISAE 3402), SAS-70 Type II, US-EU Privacy Shield, BBB EU Privacy Shield, and Swiss-US Privacy Shield

SPANNING

Kaseya

365

USER

# SUBSCRIPTION COMPONENTS

Go beyond the keyboard to protect the critical data and identity of all the users you manage in a single Kaseya 365 User subscription.

EXPLORE KASEYA 365 USER