eBook

datto
A Kaseya COMPANY

Future-Ready IT: Your 2025 Preparedness Playbook

Introduction: Preparing your IT strategy for success in 2025

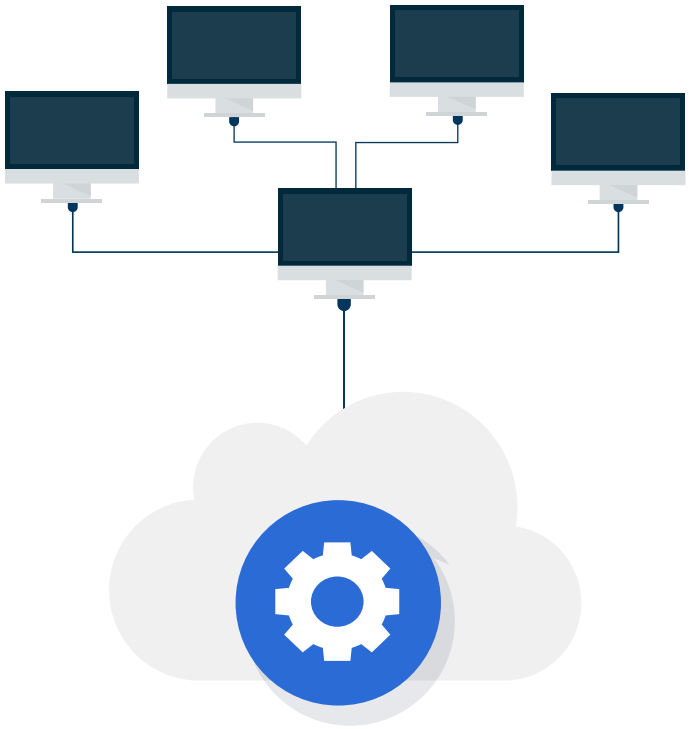
The role of IT professionals has never been more critical, especially as we look ahead to the evolving landscape of 2025. The rapid pace of technological change, combined with an increasingly complex threat environment, demands that IT teams remain more vigilant, adaptable and resilient than ever before. To provide IT professionals with a comprehensive overview of the key disciplines shaping IT preparedness in 2025, we've assembled this guide, grounded in insights from our extensive network of customers and leading industry research.

This eBook offers a structured look at what you need to know to stay one step ahead in 2025, with practical insights and actionable strategies for tackling the toughest issues across IT disciplines.

This guide explores:

- **Service management:** How AI-powered service desks are making IT teams stronger, smarter and faster than ever before.
- **Endpoint management:** Why an intuitive and seamlessly integrated unified endpoint management is crucial for saving IT teams time while also keeping endpoints secure.
- **Cybersecurity:** How IT teams can use proven security solutions to protect their organizations from advanced threats without adding headcount.
- **Backup and recovery:** How to fully protect data before an incident and recover it instantly if data loss occurs.

Each section highlights why these disciplines are indispensable for IT professionals, the key pain points in each area and practical solutions to help you stay focused on what matters most. Let's dive in.



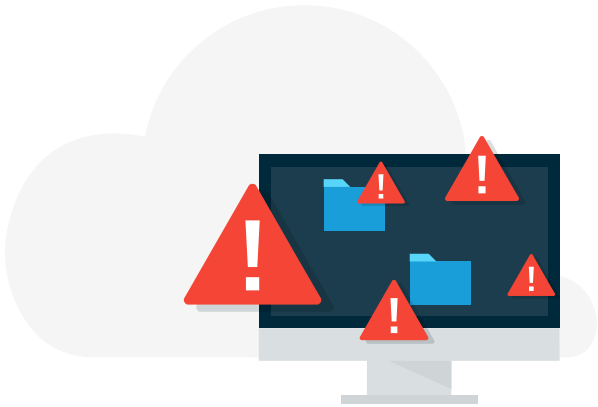
Service management: Building the foundation for operational success

Service management forms the backbone of IT operations, ensuring that systems run smoothly and issues are resolved quickly. An effective service management strategy enables IT teams to not only resolve incidents but also minimize them proactively. This allows IT to focus on strategic initiatives that advance the organization.

Key pain points in service management

Recent insights from IT Glue's 2024 State of IT Report offer a detailed view of the current IT landscape and future trends based on input from nearly 1,000 IT professionals worldwide. Similarly, Kaseya's 2024 Future of IT Survey Report gathers insights from IT team members across diverse industries and company sizes, providing a holistic understanding of the factors shaping IT decisions. Together, these reports reveal that IT professionals face complex challenges in managing ticket volumes, meeting end-user expectations and navigating tool integration. Below, we delve into the most pressing pain points and how strategic solutions, such as Autotask's service management capabilities, help alleviate these challenges.

- **Rising end-user expectations for faster service:** End-user expectations for faster service are increasing, driven by a demand for near-instant ticket resolution. According to the 2024 State of IT Report, **74% of respondents** reported that their end users expect faster ticket resolution times compared to five years ago, with 31% expecting near-instant resolution and 43% expecting much quicker responses.



- **Overwhelming ticket volumes:** IT teams are grappling with a heavy flow of support tickets, with workloads changing based on the complexity of each issue. Team sizes vary greatly, from a single technician to as many as 1,000, but the 2024 State of IT Report shows that the average team has around 22 technicians. These technicians handle a mix of ticket types each week, balancing their time across the following average ticket volumes:

Level 1 tickets: 160 per week

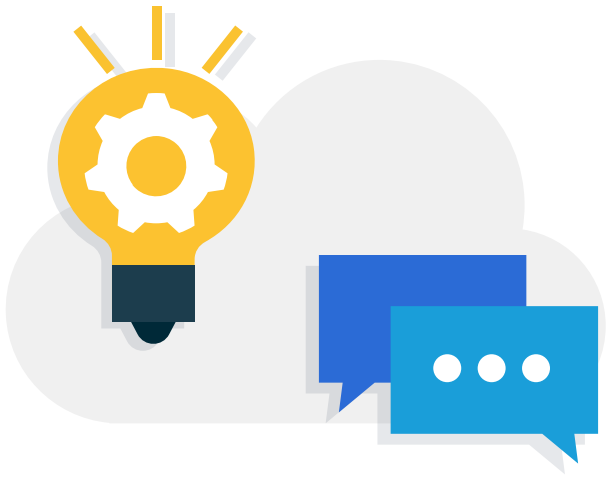
Level 2 tickets: 66 per week

Level 3 tickets: 39 per week

On-site visits: 33 per week

The time spent on tickets varies by type, with on-site visits taking the longest at an average of 100 minutes. Level 3 tickets take about 98 minutes, Level 2 tickets average 59 minutes and Level 1 tickets take around 35 minutes. These numbers highlight the need for efficient ticket management systems to help IT teams prioritize tasks and allocate resources effectively.

- **Staffing challenges:** Another challenge for IT teams is the lack of staff to handle the growing number of support tickets. The 2024 Future of IT Survey Report found that one in five IT teams is actively hiring to fill general IT roles. With too many tickets and not enough people, response times slow down, which can affect productivity across the organization.

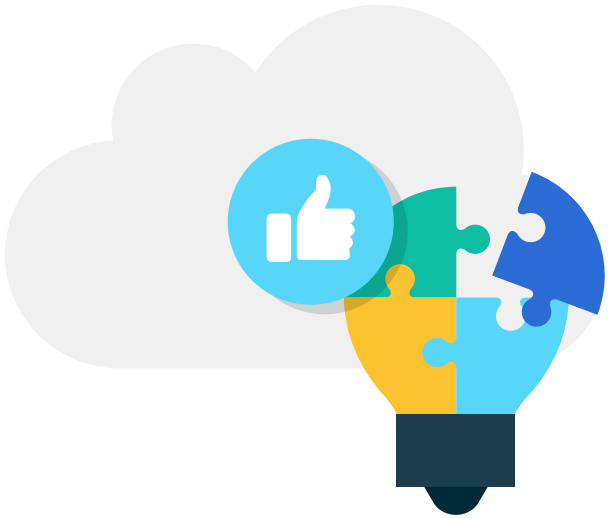


- **Lack of integration and automation between solutions:** Efficient IT management requires seamless integration across tools and processes. According to the Future of IT Survey Report, IT professionals point to three key integrations that significantly enhance efficiency: embedding IT documentation directly within endpoint management tools, enabling one-click access to remote endpoint management and setting up workflows for auto-remediation within service desks. Each of these integrations plays a pivotal role in optimizing IT workflows and reducing manual effort.

Solutions for service management challenges

To tackle these pain points, IT professionals are increasingly turning to comprehensive PSA solutions like Autotask, which offer automation, AI-driven enhancements and integration capabilities.

- **Automation for ticket triage:** By automating ticket prioritization and assignment, Autotask enables IT teams to distinguish critical tickets from less urgent ones, even in high-volume scenarios, ensuring that resources are used effectively.



- **AI-powered efficiency:** AI-powered tools allow for smoother and quicker processes, creating a more efficient IT environment. Autotask's AI assistant, Cooper Copilot, revolutionizes service desk efficiency by saving technicians time. Key features include:
  - **Smart Ticket Summaries:** Summarizes long ticket threads, highlighting the issue, actions taken and next steps, so technicians can quickly assess and act.
  - **Smart Writing Assistant:** Converts technical notes into polished responses, enhancing communication with end users and promoting satisfaction.
  - **Automatic documentation:** Automatically generates detailed resolution notes, aiding future troubleshooting and enabling junior technicians to handle complex tickets with confidence.
- **Integrated IT documentation:** When used alongside an IT documentation tool like IT Glue, Autotask enables a centralized and streamlined workflow that boosts productivity. According to the State of IT Report, technicians using both IT Glue and Autotask manage an average of 250 endpoints per technician, compared to 100 for Autotask alone and 40 for non-Autotask users. This integration eliminates the need to toggle between systems, helping technicians resolve tickets faster and with fewer errors.
- **Comprehensive tool integrations:** Built-in service desk integrations allow for one-click access to remote management tools and automated workflows for issue remediation. These integrations are vital in reducing friction between platforms, enhancing visibility and allowing IT teams to respond to issues more rapidly and efficiently.

Customer insights

Feedback from IT professionals reinforces the value of Autotask PSA in solving common service management challenges:

> Autotask is perfect for any help desk. From ease of use to the communication it provides, as well as the end user being able to see their current and old tickets. Autotask is great for seeing what is being done daily and what you have coming up.

★★★★★

Josh T., Tier 2 Engineer

> Best PSA on the market! We love all the integrations, especially with QuickBooks, and the app is fantastic. Our techs can open a ticket and 'start the clock' when they are on-site, then hit 'record' to track their time accurately.

★★★★★

Markus S., Director of Technology

Endpoint management: Securing every device in your organization

As IT professionals know, the efficiency of your service desk has a direct impact on your ability to manage and secure each endpoint. Ensuring every device is secure, compliant and up to date is essential — not only for maintaining a smooth workflow but also for protecting the organization from potential security threats.

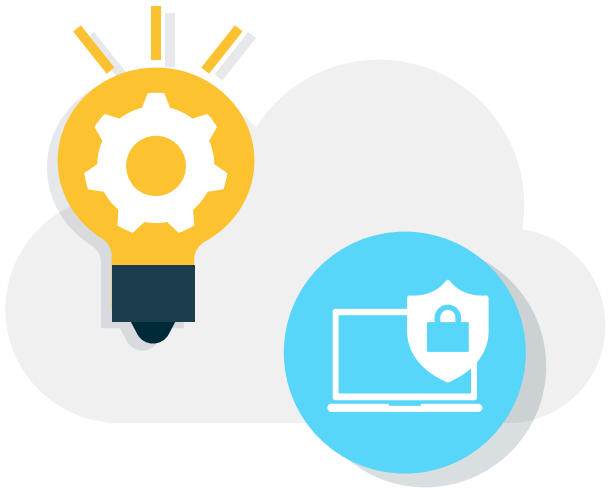
Key pain points in endpoint management

The increasing variety and complexity of devices, paired with the ever-present risk of human error, make managing endpoints a demanding task. Recent studies reveal that IT teams are dedicating more of their budgets to support a growing fleet of devices, all while grappling with vulnerabilities introduced by end-user behavior. Below, we explore the key pain points that underscore the need for a robust endpoint management strategy.

- **Growing quantity and complexity of devices:** According to Kaseya's Future of IT Survey Report, **39% of IT budgets** are now allocated to end-user hardware, such as desktops, laptops, tablets and mobile devices. However, the Kaseya Cybersecurity Survey Report 2024, which collects data on cybersecurity trends and forecasts from IT team members worldwide, highlights a major challenge: **29% of respondents** cite insufficient security support for different device types as a significant contributor to cybersecurity issues.

  From desktops to smartphones, each device presents unique challenges and security requirements. This growing complexity demands a comprehensive, flexible approach to endpoint management that can support multiple device types while ensuring they remain protected and compliant.

Human error is a top security concern for **36% of IT professionals.**



- **Human error**

  Human error is a major factor in endpoint management, often introducing vulnerabilities that can compromise network security, impact productivity and increase IT support costs. Concern over human error has risen significantly, with the Kaseya Cybersecurity Report 2024 noting that **36% of respondents** now identify it as a primary security concern , up from 16% last year. Additionally, two-thirds of respondents attribute security weaknesses to a lack of end-user or administrator training.

Solutions for endpoint management challenges

As the complexity of managing endpoints grows, unified endpoint management (UEM) solutions like Datto RMM have become invaluable. Here's how Datto RMM and similar tools address the key pain points in endpoint management:

- **Automated updates and patching:** Keeping operating systems and applications up to date is one of the most effective ways to secure endpoints. UEM solutions, like Datto RMM, help organizations ensure devices are running the latest security patches and fixes, making it easier to maintain security across the rising quantity and complexity of modern endpoints.
- **Remote access and device management:** Datto RMM allows IT teams to remotely access thousands of endpoints, enabling them to troubleshoot issues, deploy software and monitor device health without needing physical access.
- **Centralized information and quick deployment:** Datto RMM's device landing page offers a centralized view of key device information, allowing IT teams to assess the status of each endpoint quickly.

- **Intuitive interface and seamless integrations:** Datto RMM's user-friendly interface simplifies day-to-day management tasks, offering robust integrations that streamline workflows. This ease of use is complemented by powerful reporting capabilities, giving IT teams the insights they need to address issues proactively.

Customer insights

Feedback from IT professionals reinforces the value of Autotask PSA in solving common service management challenges:

> We appreciate the product's intuitive layout, which is relatively easy to understand. Despite its user-friendly design, it doesn't lack features, offering a wide range of functions and compatibility with other products. This enables instant reporting for faster technician assessments.

★★★★★

David W., Chief Technology Officer

> It's intuitive and makes things easy to integrate, and with all the components, it really helps in deployment. NOC services and personnel are top-notch, very knowledgeable, professional and responsive.

★★★★★

Lisa V., Help Desk Coordinator

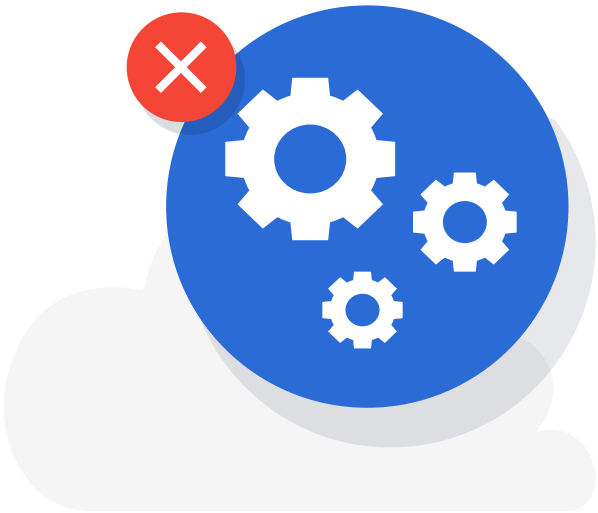
Cybersecurity: Fortifying your IT environment against emerging threats

By keeping endpoints well-maintained and compliant with security policies, endpoint management forms a strong foundation for cybersecurity. It ensures that other cybersecurity tools, like antivirus (AV), endpoint detection and response (EDR), and managed detection and response (MDR), can operate on secure, well-configured and consistently updated devices. As cyberthreats become increasingly sophisticated, robust cybersecurity strategies are essential for protecting sensitive data, maintaining compliance and ensuring operational continuity.

Key pain points in cybersecurity

IT teams face significant challenges in maintaining a strong security posture. From managing overwhelming alert volumes to addressing skills shortages and automating critical tasks, these pain points can hinder an organization's ability to respond swiftly to threats. Below, we examine the most pressing cybersecurity challenges and explore why advanced tools and strategies are essential for modern defense.

- **Alert fatigue:** In many organizations, security analysts are responsible for investigating a constant stream of alerts, which can lead to "alert fatigue." This phenomenon occurs when the sheer volume of alerts overwhelms analysts, making it challenging to distinguish critical threats from false positives or lower-risk issues. Without tools to filter and prioritize, alert fatigue can cause delays in responding to genuine threats and result in a weakened security posture.



- **Staffing and lack of security specialization**

  Demand for cybersecurity talent is on the rise. The Future of IT Survey Report shows that 71% of organizations plan to expand their IT teams, with IT security being the top hiring priority for 38% of them. However, finding skilled security professionals remains a challenge. IT security requires specialized skills to maintain defenses, navigate compliance regulations and respond to complex threats. Without sufficient security staff, organizations struggle to keep up with the fast-paced cybersecurity landscape.

- **Disparate solutions**

  Many organizations rely on a range of standalone security tools that don't always integrate seamlessly. Disconnected solutions can hinder visibility and create inefficiencies, as IT teams must switch between platforms to monitor and respond to threats. Integrated solutions, on the other hand, offer a unified approach that enhances operational efficiency and improves response times by centralizing data and alerts.

- **Lack of automation**

  Increasing productivity through automation is a top priority for many IT teams, following closely behind improving security itself. The Future of IT Survey Report indicates that **29% of organizations** are prioritizing automation to streamline workflows, reduce manual tasks and improve productivity. In cybersecurity, automation is essential for reducing repetitive tasks, such as alert triage and remediation, allowing security teams to focus on high-impact threats rather than getting bogged down with routine work.

Solutions for cybersecurity challenges

To overcome these challenges, IT teams need a multilayered security approach that includes AV, EDR and MDR.

- **Reducing alert fatigue:** Utilizing managed detection and response (MDR), like Datto Managed SOC, helps IT teams reduce alert fatigue by prioritizing and investigating high-risk threats. Datto's SOC team is comprised of expert cybersecurity professionals who will filter through noise to only alert you to credible threats.

  Additionally, Datto EDR's Smart Recommendations and correlation engine reduce unnecessary noise by filtering out low-priority alerts and highlighting critical threats. This capability allows IT teams to address real threats quickly and effectively without being overwhelmed by false positives.

- **Solving the cybersecurity staffing shortage:** By partnering with Datto MDR, you instantly augment your team with a trusted team of cybersecurity professionals. This enables you to gain the expertise of having a security team without the pain of recruiting, retaining and fully staffing professionals to protect your business 24/7.

- **Unified security tools:** Datto MDR unifies Datto AV and EDR with managed SOC capabilities into a centralized hub, allowing IT teams to monitor and respond to threats seamlessly across endpoints, cloud and network environments. This integration streamlines workflows and enhances visibility, making security operations more efficient.

- **Automation to improve productivity:** Automating repetitive security tasks is essential for maximizing productivity. Datto EDR's automated threat response takes immediate action, reducing manual workloads and ensuring faster threat mitigation. Meanwhile, Datto AV provides automated quarantine and remediation.

Customer insights

Datto EDR customers report significant improvements in endpoint protection and overall efficiency:

> Datto EDR really shines in its endpoint protection capabilities. Its real-time threat detection is impressive, catching potential issues before they become problems. The interface is quite intuitive, making it easy to monitor and manage all our endpoints efficiently. It's a versatile solution that seems well-suited for organizations of various sizes.

★★★★★

Fausto C., Senior Engineer

> The web dashboard gives a quick comprehensive overview of the protected endpoints. It can be rolled out using Datto RMM (Unified Endpoint Management) and immediately begins scanning, protecting, and resolving issues. Raising alerts and resolution is simple and efficient.

★★★★★

Verified G2 Reviewer

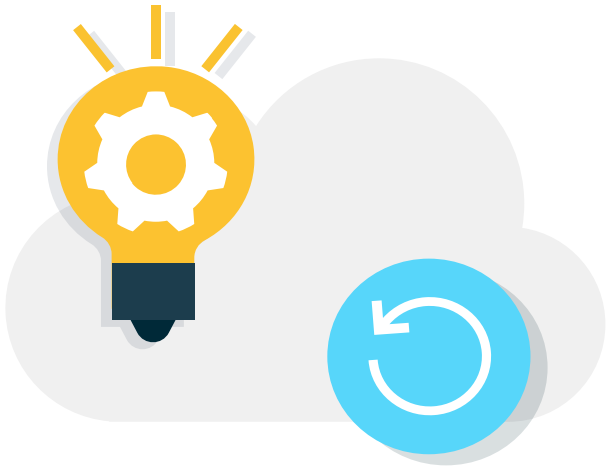
Backup: Ensuring data resilience and business continuity

While a robust security strategy with AV, EDR and SOC capabilities is essential for protecting endpoints and networks from active threats, true resilience requires a comprehensive backup plan as well. Even the strongest defenses can't prevent every incident, and sophisticated attacks, accidental deletions and unforeseen disasters can still occur. That's where backup solutions as the first and last line of defense play a critical role, regardless of whether they are appliance-based, virtual or SaaS. Together, security and backup create a fail-safe ecosystem that protects data integrity and business continuity.

Key pain points in backup management

As data volumes grow and threats evolve, IT teams face increasing pressure to keep backups secure, compliant and readily accessible. Below, we explore the most pressing pain points in backup management and why addressing them is important for resilience and continuity.

- **Managing recovery points:** As data volumes grow, so does the challenge of managing recovery points. Ensuring that backups are recent, uncorrupted and readily accessible is essential for a successful restoration. IT teams must monitor and verify recovery points consistently to ensure they're usable when needed.
- **Changing compliance standards:** Regulatory requirements around data backup and disaster recovery are evolving, and IT teams must adapt to stay compliant. According to the 2024 Future of IT Survey Report, **14% of respondents** cited changing backup and disaster recovery standards as a top challenge . This requires IT professionals to regularly update their backup policies and conduct thorough testing to verify compliance.

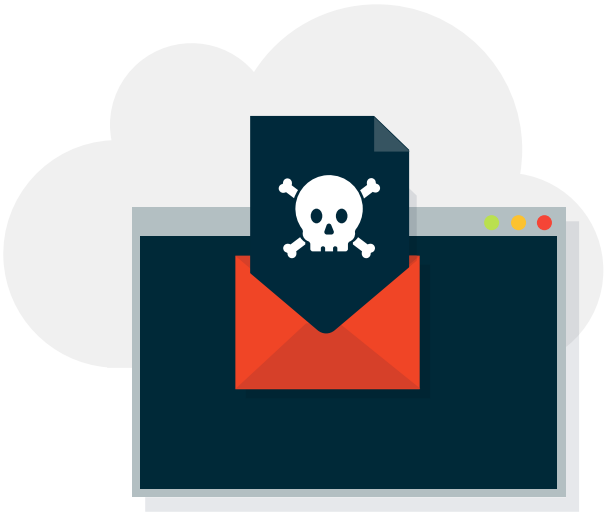


- **Cloud services' shared responsibility model:** As more organizations adopt cloud services, they must consider the shared responsibility model of cloud providers. This model stipulates that while providers secure the cloud infrastructure, customers are responsible for protecting their own data within it. IT professionals need cloud backup solutions capable of safeguarding cloud-resident data, such as Office 365 and IaaS environments like AWS and Azure.
- **Ransomware targeting backups:** Ransomware attacks are becoming increasingly sophisticated, and backups are a primary target. According to The State of Ransomware 2024 report by Sophos, a staggering **94% of organizations** hit by ransomware reported that attackers attempted to compromise their backups. This means backup strategies must include strong defenses to protect backup files from malicious tampering.

Strategies for backup resilience

To address these challenges, IT teams should adopt a resilient backup strategy that goes beyond technology, integrating people and processes into a robust plan. Here are some key tips for ensuring effective backup resilience:

- **Adapt backup policies for compliance and cyber insurance:** Update backup policies regularly to meet any new compliance requirements in your industry. Testing is crucial to ensure recovery points are clean, determine when a compromise occurred and verify that backups remain unaffected. Being able to prove that you have a clean recovery point is key for maintaining compliance and restoring operations quickly.



- **Implement a multifaceted backup strategy:** Given the diverse locations of data — on-premises, in the cloud and across SaaS applications — backup strategies must be comprehensive. Datto's backup solutions, for example, support appliance-based, virtual and SaaS backups, allowing IT teams to select the appropriate level of backup for each data type. For mission-critical data, premium BCDR appliances and cloud disaster recovery solutions offer rapid recovery options. For endpoint backups that require off-site protection without instant recovery needs, other solutions provide efficient and cost-effective safeguards.
- **Prepare for cloud data backup:** With the shared responsibility model in mind, IT teams must ensure they have tools to back up cloud-based data. This includes applications like Office 365 and IaaS environments, like AWS EC2 and Azure VMs. Backing up cloud data is especially essential for comprehensive protection since more organizational data resides outside traditional on-premises environments.
- **Defend against ransomware with backup security:** Given the increasing focus of ransomware attacks on backups, it's essential to secure backup solutions themselves. Solutions like Datto's backup products are designed with ransomware protection in mind, helping to prevent backups from being compromised during an attack and ensuring quick data recovery when needed.

Customer insights

Customer feedback on Datto's backup solutions highlights the value of resilience and ease of use:

> This is the best option to set up your backups with 'set it and forget it' functionality. I love the protection against ransomware!

★★★★★

Darryl F., Systems Administrator

> All I can say is that it's a fantastic product that meets all of your needs.

★★★★★

Lokesh S., Senior System Engineer

Conclusion: Building a resilient IT strategy in 2025

As the IT landscape continues to evolve, the need for a comprehensive, proactive approach to IT management is more critical than ever. In 2025, successful IT teams will be those that not only secure their environments but also create resilient infrastructures that support long-term growth and adaptability. This journey begins with mastering each core discipline: service management, endpoint management, cybersecurity and backup.

Together, these interconnected strategies create a robust IT framework that helps organizations stay competitive, secure and prepared for the future.

To learn more about how you can make 2025 your best year yet, hear from other IT professionals about how they saved time and reduced stress with Datto.

Download the eBook

datto
A Kaseya COMPANY