Backup and Recovery

Through the Small and Medium Business Lens

Contents

Introduction

Your small/mid-sized business always weighs cost, risk, and reward when looking at every purchase. But this approach becomes more complex when faced with choosing a backup and recovery solution. Limited budgets and fluctuating backup expertise only serve to further complicate things. All the while, you're struggling to deal with balancing the challenges of data growth/silos and the need to store, manage, and protect data across diverse environments. As bad actors and cyberthreats like ransomware become more sophisticated and prevalent the costs, risks, and rewards around cybersecurity take on a whole new meaning for your small and/or mid-sized org.

According to Veeam's 2023 Ransomware Trends report, small businesses were the target of 85% of ransomware attacks. This is one of the reasons 92% of companies intend to spend more on data protection, according to Veeam's 2024 Data Protection Trends Report.

As bad actors and cyberthreats like ransomware become more sophisticated and prevalent the costs, risks, and rewards around cybersecurity take on a whole new meaning for your small and/or mid-sized org.

Whether dealing with on-premises servers, hybrid-cloud setups, or fully cloud-based infrastructures, the need to balance time, cost, and expertise is crucial. As the threat landscape and your business changes, your organization must be capable of adapting to varying data and a host of market and regulatory needs. This means you need the ability to leverage:

- Backup scalability
- Movement between hypervisors (moving image-based backups to Proxmox, VMware, or Hyper-V virtualization platforms)
- Amazon, Azure, and Google Cloud
- Transitioning to the cloud
- New technology integration

All of the above require a highly versatile backup solution that meets your organization's expertise, time, and budget requirements. The best place to start is determining which backup platform elements your business should prioritize when assessing different vendor solutions.

Determining Priority Elements in Assessing Backup Solutions

The only way for you to assess and choose the right backup solution is by developing a list of requirements based on your business, data, and technology needs.

Business Considerations

If you're an IT leader working with an organization, either internally or externally, you may have a business stakeholder involved in the final choice of a backup solution. These stakeholders will require clear proof that the platform meets business considerations including cost, future compatibility without incurring major expense, and the reputation of the vendor among other business and sector peers.

To navigate a sea of choices, everyone involved in your decision-making process must have a sufficient understanding of the solution's costs and features, as well as your business/budget requirements.

Cost and Budget Management

Balancing cost and budget constraints with solution features and functions is challenging, but not impossible. Your budget can be part of the problem when it doesn't factor in all potential costs beyond the purchase price, such as:

- Licensing structure
- Personnel expertise and hours
- Maintenance and management based on the desired level of internal control
- Potential upgrades and scalability costs
- Fees for extra features or storage capacity needed both today and tomorrow

The goal is to balance affordability and functionality while making sure the solution delivers long-term value and scalability without unexpected costs.

Scalability for Future Growth

Your organization and its data are continually growing, which requires a backup solution with inherent scalability and flexibility. A scalable solution should seamlessly accommodate growth in data volume, user base, and application complexity.

Vendor Support and Reputation

Identifying your company's list of feature and function priorities, along with vendor support and reputation, is pivotal to all backup vendor decisions. Whether your organization has extensive in-house IT support or not, a platform should include pre-sales to continuous expert support via:

- An extensive content and media knowledge base
- Ongoing, fast, and helpful support and access to actual personnel
- Real-world demos based on each small or mid-sized organization's particular scenario

A vendor's support tools help ensure trust, transparency, and alignment, demonstrating that their comprehensive solution can cater to varied small or mid-sized business needs. Additionally, it is crucial that they have an easily identifiable and verifiable reputation among these businesses and decision-makers (business stakeholders, C-suites, engineers, sysadmins, and other backup process owners).

As part of this reputation, it should be simple to find countless real-world stories, conversations, and interactions from the user community beyond the vendor's own collateral. Vendors should be able to show a proven track record of reliability, consistent customer support, and resources for questions and challenges. They should also be able to demonstrate fast response and resolution without downtime, along with a continuous track record of meeting SLAs.

Technical Considerations

While business considerations inform many technical considerations, the latter takes a broader view of the security world where backup plays a key role, including the impact of:

- Technical aspects of the backup solution for data security
- How backup operators interface with the solution
- Hybrid environment compatibility

Data Security

Cyberthreats are increasing in volume and sophistication with smaller and mid-sized orgs as the target. This requires a backup solution with end-to-end encryption, secure access controls to protect all data from unauthorized access and breaches, and comprehensive ransomware protection, detection, and recovery features.

Ransomware continues to be an ever-growing threat, and an effective backup solution should detect and prevent such attacks while providing the tools for quick recovery after an incident occurs.

Intuitive Operation

Your small or mid-sized business will benefit most from a single backup solution that is comprehensive in terms of its abilities but also intuitive for simple operation, management, and monitoring. This requires the platform to have a single-user interface that is transparent and intuitive for operation by a generalist IT professional, automated backups and a straightforward restore process, and finally, extensive alerts and reporting.

Hybrid Cloud Integration and Compatibility

More organizations are moving data/workloads to the cloud. How they use cloud environments can vary, but they all need some level of backup integration and compatibility across on-premises and cloud environments.

Just a few of the reasons teams like yours are seeking backup solutions that can integrate with a hybrid-cloud environment include:

- Diverse and siloed data stores, operating regionally or even globally
- Existing/legacy on-premises infrastructure
- On-premises data stores for increased security and regulatory compliance
- Drive to lower total cost of ownership (TCO)/capital and operational expenditures (CapEx, OpEx)
- Ability to scale as business needs change
- Data resiliency to ensure data integrity, availability, and continuous operations

Integrating legacy on-premises infrastructure with cloud-based backup solutions is the bigger challenge for smaller teams. Having multiple backup products without integration leaves visibility and functionality gaps, which bring even more complications, including higher costs, time, risks, and errors. Many organizations like this also combine remote monitoring and management (RMM), security, and backup solutions that lack critical features and thus require IT workarounds.

When first assessing a solution's compatibility with your company's specific present and future needs, you will need to focus on these key business and technical considerations.

Critical Data Security Factors for SMB Backup Solutions

For businesses like yours, data security challenges may be on a different scale than large enterprises, but the dangers and growing complexity are equal.

Are Cyberattacks Inevitable for SMBs?

Small and mid-sized businesses are particularly vulnerable to cyberattacks, with ransomware being one of the most significant threats. These companies often struggle to recover from such incidents, leading to prolonged downtime, loss of customer trust, and sometimes even permanent closure.

Vital Concerns for Proactive and Reactive Cybersecurity

While reactive and proactive data security has always included backups and disaster recovery, they've become a priority in the current threat landscape. Small and medium organizations must understand what concerns a data backup tool addresses to know if it will be a good fit for their needs.

Reliability and Uptime

These two factors are crucial to ensuring data is always protected and accessible, even if hit by a system failure or cyberattack. The right solution builds on proactive threat detection to deliver the security needed for workloads and data located anywhere and everywhere in real time.

Comprehensive and Granular Workload Recovery

Having a comprehensive approach to backup and recovery starts with meeting recovery time objectives (RTOs) and recovery point objectives (RPOs). This requires a backup solution that supports comprehensive and granular workload recovery objectives. The goal is delivering instant recovery across virtual machines (VMs), physical servers, workstations, and cloud instances — regardless of the platform in use:

- vSphere, Hyper-V, Oracle Linux Virtualization Manager, or any other hypervisor
- AWS, Azure, Google, or hybrid-cloud environments
- Any platform or database management system

Even small businesses must have the ability to create backups and recover data from storage snapshots. This should include comprehensive and automated verification testing, scheduling, and recovery isolation. Small and mid-sized businesses often have diverse data storage needs where the broad protection and recovery of data from network-attached storage (NAS) devices is crucial. While hybrid enables the 3-2-1 backup rule of data backup, the increasing ransomware risk has many businesses opting for an additional offline copy.

This air-gap copy has no link to the network or internet, allowing for greater ransomware protection, unauthorized access prevention, preservation of data integrity, and immutable backups.

Of the 1,200 organizations previously reporting cyberattacks, 85% leverage immutable cloud technologies, according to the Veeam 2024 Ransomware Trends Report. Immutable copies differ from air-gap copies in that the form is still accessible via the network or cloud, but it has highly restricted role-based access.

Meeting Compliance Standards

Small and medium businesses must ensure data backup and recovery while meeting a changing roster of regulatory compliance measures. Non-adherence to the necessary regulations can damage your business, brand, and bottom line, involving both fines and legal trouble. As regulations continually develop, businesses must constantly know which ones cover different types of data and where multiple regulations intersect across the same data stores.

These organizations also require real-time monitoring and reporting capabilities to identify and address compliance issues proactively, which means the ability to:

- View the entire hybrid virtualization and backup infrastructure from a central UI
- Monitor cloud environment snapshots, backups, replicas, and storage consumption
- Identify protected and unprotected data
- Meet specific data retention policies
- Ensure verification of correct backup and storage at prescribed times
- Continuously monitor on-premises, hybrid, and multi-cloud environments, as well as the associated data protection activities

This level of visibility, management, monitoring, and reporting allows personnel with a minimal level of time and backup/recovery expertise to use the platform easily.

Data Sovereignty and Avoiding Vendor Lock-In

Data sovereignty is particularly important for businesses like yours that are operating in multiple jurisdictions. Instantly knowing where data is stored in a hybrid-cloud environment (on-premises and across cloud environments) is critical to meeting all local and international regulatory requirements. Issues can arise when backup solution providers don't offer clear data sovereignty policies and reporting mechanisms.

Avoiding vendor lock-in is also crucial for smaller teams who are looking to maintain flexibility and freedom in their IT operations, particularly around storage. Choosing a storage-agnostic backup solution allows for the movement of data between different storage platforms, meaning businesses can quickly adapt to changing needs or implement new technologies.

Evaluating SMB Backup Solutions

Cost, security, and regulatory compliance considerations form the basis for the practical aspects of evaluating whether backup solutions meet your business requirements.

Assessment of Business Requirements

When evaluating a backup solution, you must first assess your company's specific needs. Businesses like yours often have diverse data protection requirements including safeguarding critical applications such as Microsoft 365 or ensuring regular backups of CRM databases and other sensitive information. This is one of many reasons why closing gaps in backup, recovery, and visibility can be challenging without centralized management.

Scalability Planning

The growth of your business always includes data and workload growth, making scalability an ongoing consideration when selecting a backup and recovery solution. Scalability must avoid complexity and significant costs related to upgrades or replacements.

Ideal backup solutions should offer flexible licensing models so organizations like yours can add cost-effective capacity as needed. Consequently, they must choose a solution that meets current needs while also offering a clear and cost-effective path for future expansion.

Security and Compliance Features

It's difficult for IT teams to plan and implement proactive, reactive, and fully integrated backup and security systems that have a single management/monitoring user interface. Things get harder with most smaller teams lacking a security specialist and even more relying on third-party IT support. That's why a comprehensive backup solution must include robust security features such as:

- End-to-end encryption with industry-standard encryption algorithms, including Advanced Encryption Standard (AES)-256
- Multiple public key encryption methods to encrypt data blocks, metadata, and session keys
- Advanced threat detection capabilities
- Defined and flexible access controls

However, these features can only ensure data remains protected from unauthorized access and cyberattacks when a solution is fully integrated into your environment, eliminating visibility and control gaps.

This enables a business to manage and have control over data encryption in transit (while being uploaded), data encryption at rest when stored across all storage environments, and encryption user access and permissions. Advanced threat detection capabilities are also essential, as they help identify and mitigate potential security breaches before they can cause damage.

Ease of Deployment and Use

Solutions that are difficult to deploy or require extensive training create challenges by increasing management time and costs. IT teams must spend significant time troubleshooting and overseeing the system instead of focusing on other important tasks.

The best solution emphasizes user-friendliness and simplicity, with easily configurable features for those with limited technical expertise.

Long-Term Data Management

Long-term data management is a critical aspect of any backup solution, particularly for that need to comply with regulatory requirements or maintain historical data for business purposes. A flexible data retention policy allows you to archive data according to your specific needs, ensuring that you meet both business and compliance requirements. Each business will have different regulatory and security needs for their data.

Not all backup solutions offer adequate data retention options. Some have rigid policies that don't align with business needs, while others lack the ability to manage data over the long term, resulting in, data loss, compliance issues (fines, penalties, audits, or legal actions), and the need for costly additional solutions to fill the gaps.

When evaluating backup solutions, prioritize those that offer customizable data retention policies, regulatory analysis, and robust archiving capabilities supporting long-term data management.

Trial Periods and Testing

Real-world testing during a trial period is an effective way to evaluate a backup solution. It enables your small/medium business to understand if the solution performs in the actual environment, meets business needs, and integrates with existing infrastructure.

A solution without comprehensive testing and validation processes introduces issues with performance, compatibility, and usability. The dynamic nature of data and workloads requires backup environments and systems to match those dynamic changes in real time. Testing and validation allow for the maintenance, adjustment, and visibility required to know whether your backup environment is:

- Performing at peak efficiency, adjusting to changes, and minimizing risks/points of data access failure
- Ensuring compatibility across all environments while showing all backup rules are operating as defined (how and when they are expected)
- Understood by its operators in terms of management, visibility, and defined outcomes in the event of data recovery needs

Vendor Reputation and Support

A backup solution vendor's reputation and support are crucial factors in the decision-making process. Every business, regardless of size, wants more granular validity about the platform and its reputation, along with vendor responses and support for fast issue resolution. Thorough vendor research gives your organization deeper knowledge about the backup solution itself and the vendor—as well as the vendor's credibility, the quality of customer support, and customers' satisfaction with the solution.

Compatibility and Integration

Businesses like yours need comprehensive, resilient, responsive, and scalable backup and recovery as much as enterprises. The chosen solution must also save time, reduce costs, and minimize disruptions during deployment or updates.

Compatibility with existing IT infrastructure is essential for a backup solution to deliver seamless integration with current systems, transparent setup methods, and unified monitoring and management across all environments, platforms, clouds, technologies, and infrastructure. The solution must do all of this without leaving gaps, workarounds, or blind spots.

The SMB Hybrid Backup World

More small and mid-sized businesses are operating in a hybrid-cloud environment where they must safeguard data while balancing cost, flexibility, and control. The demarcation line between cloud-based and on-premises data and workloads is constantly shifting in ways that require a highly versatile backup and recovery solution.

The debate between cloud-based and on-premises backups has been a central theme in data protection strategies over the past decade. Understanding the benefits and challenges of each approach is essential for selecting the option that best aligns with your small or medium-sized business's unique requirements.

Cloud-Based Backup Benefits

Cloud-based backups have become an increasingly popular choice for many reasons. One key advantage is their scalability. Unlike on-premises solutions, where adding storage capacity often requires purchasing additional hardware, cloud-based solutions allow easy storage scalability as the business evolves:

- Low entry costs, which can be a major plus for smaller teams with limited budgets and resources
- Broad accessibility from any internet-connected device when a primary site is down
- Comprehensive security features
- Easy management and scalability via a few clicks to increase backup capacity in contrast to a complex on-premises physical hardware setup

Cloud-Based Backup Challenges

Despite the pros associated with cloud-based backups, they do have perceived data security challenges for small/medium organizations surrounding cloud providers' shared responsibility models. It's still the org's responsibility to ensure data backup across clouds, meet changing data sovereignty or compliance regulations, and proactively handle any regulatory concerns based on industries like BFSI or healthcare.

Other potential challenges include escalating storage costs reflecting data growth, which requires close monitoring and management. This also avoids potential latency due to bandwidth issues when migrating large data stores, which can delay recovery time.

The SMB Hybrid Backup World

Benefits and Challenges of On-Premises Backups

On-premises backups offer businesses like yours a high degree of control over their data and backup processes, which extends to data security and regulatory compliance. A significant drawback, however, is cost due to the substantial upfront investment required for hardware, as well as ongoing maintenance and management.

On-premises backups are also difficult, time-consuming, and costly to scale, not to mention the needed spend — and maintenance — for additional hardware as your storage needs grow. Other significant challenges to on-premises backups include business operation disruptions due to hardware upgrades and replacements as well as increased vulnerability to physical disasters that can cause primary data loss and ongoing business downtime.

Given this mix of pros and cons associated with cloud-based and on-premises backups, many of these organizations opt for a hybrid approach that leverages the strengths of both.

The SMB Hybrid Backup World

Hybrid Data Backups: The Best of Both Worlds

Advancing technologies and changes in the business landscape have many organizations of all sizes turning to hybrid backup solutions, which leverage the cloud as well as on-premises infrastructure.

Hybrid goes beyond the on-premises backup of critical data for quick access and control while storing less sensitive or archival data in the cloud. It's about having deployment control over each environment via a purpose-built backup and recovery platform that is flexible, comprehensive, and centrally managed.

These three attributes work together to meet your business-specific backup needs today and tomorrow in ways that save time, avoid changing risks, and maximize RTO while limiting costs. This includes giving your team transparency in terms of controlling/managing all functions across virtual desktop infrastructure/desktop as a service (VDI/DaaS) platforms, Windows Server, Oracle DB, and more.

The ability to send backups between clouds and on-premises environments seamlessly is what drives small and medium organizations' robust data protection strategy. However, hybrid backup solutions demand careful planning, implementation, and management.

The ideal SMB hybrid-cloud backup solution should provide:

- End-to-end layered security that builds on the 3-2-1-1-0 golden backup rule with air gaps
- Logical air gap of backups from production
- Least-privilege access controls
- Immutable backups for cyber resiliency
- Fast, reliable recovery through a broad scope of support for granular and full-instance recoveries, in and out of the cloud
- Hybrid and multi-cloud readiness via standardized data protection across platforms with built-in centralized management, observability, and portability.
- Enhanced disaster recovery capabilities via data copies on-site and in the cloud to ensure faster recovery

Your company must also be certain the solution delivers seamless integration while providing coordinated backup processes to avoid redundancy or data inconsistency. Balancing the costs, benefits, and management of a hybrid environment can be more complex without the right backup provider and support partner.

What the Ideal SMB Backup Partner Should Deliver

It's difficult for your organization's IT and business leadership to grapple with the dual importance of business operations and backups when it comes to data security. The challenge is finding a vendor that can bring a deep understanding of the needs of small and/or medium businesses. This could include taking steps like having a comprehensive approach that is both proactive and reactive where backup technologies, systems, and methods are capable of keeping all your data safe, no matter where it's located.

The ideal backup platform should give your business seamless and integrated data/workload protection no matter where your data or workload lives. That means a platform that provides your organization with a backup solution capable of integrating with virtual machines (Proxmox, Hyper-V, Nutanix AHV, and Red Hat Virtualization) and physical servers (Windows, Linux, IBM AIX, Oracle Solaris, Mac, and NAS).

Your small or mid-sized org may not use multiple infrastructures, database management systems, or cloud providers. You still, however, need a single backup platform that can work with all of them, including:

- Cloud: AWS, Azure, Google
- Applications: Microsoft, Databases, Kubernetes, Oracle, SAP HANA, PostgreSQL, MySQL

This must include cloud-based software as a service (SaaS) such as MS365, Salesforce, Azure, and more, which can be easily added if the solution offers some type of universal license.

Reliable Data Protection/End-to-End Security

The ideal backup provider offers a single vendor solution that takes a holistic approach to ransomware protection, enabling your organization to detect, protect, and recover with confidence, which means restoring clean data instantly, minimizing downtime, and keeping your business running smoothly.

These and other features should be fully integrated to provide secure access controls and multi-layered protection, including proactive threat hunting and immutability everywhere to prevent unauthorized data manipulation. Some of the key approaches to doing this include:

- Early threat detection during backup processes to deliver inline entropy and file extension analysis
- The inclusion of an incident API that can expand proactive support by directly feeding infections into cyber threat tools to mark existing restore points as infected or to trigger a backup
- Having a centralized threat dashboard that highlights threats, identifies risks, and measures the security score of your entire environment
- Continuous data protection (CDP) to enable rollbacks to the moment before an infection hits, with minimal data loss to maintain your business continuity
- Enabling a dedicated generative AI assistant and a security and compliance analyzer to support your small IT team by easily putting real-time data in their hands

Instant Recovery Capabilities

Your IT team, and the organization's entire workforce, can't operate effectively if they're worried about a system failure, ransomware attack, or natural disaster. The right solution means having unparalleled instant recovery capabilities to ensure your entire company can recover all data quickly and efficiently if such an incident does arise.

Your business will be dealing with virtual machines, physical servers, workstations, or cloud instances in different combinations today and down the road. You can't afford to settle for anything less than a backup solution that offers seamless recovery across platforms like VMware, AWS, Azure, and Hyper-V directly from the backup. This form of instant recovery limits downtime and disruptions to maintain business operations despite disaster striking.

Storage Versatility

Every organization like yours has unique storage needs that the ideal data platform must be designed to address. This will involve steps like migrating and managing backup data across different storage types, maintaining data reduction, and being easy to manage. This includes the ability to create immutable backup copies using advanced object storage functionality on Amazon S3 and supported S3-compatible on-premises object storage.

Your small/mid-sized business may currently or will soon be leveraging hybrid and multi-cloud infrastructure. The right solution is ready to fill those needs by enhancing AWS, Azure, and Google Cloud backups to further guarantee resilience, security, and cost-effectiveness.

Disaster Recovery Capabilities

As a small business, you know disaster recovery cannot be an afterthought. Nor can it be a mere add-on or solution from an additional vendor. That means the best choice is a single vendor solution capable of keeping data and workloads safe and instantly available to meet RPOs/RTOs by:

- Integrating VM replication for on-site or off-site disaster recovery to enable rapid recovery and minimal disruption during incidents
- Supporting replication from backups or production environments to different platforms and cloud environments
- Providing extensive compatibility for NAS protection, supporting small and medium organizations, NFS, Microsoft Windows, and Linux file shares

Flexibility and ongoing RPO improvements serve as a baseline, so the ideal solution should deliver advanced NAS protection and restore capabilities. Such wide coverage is essential to ensuring small and medium businesses can recover from any disaster rapidly.

Effortless Management

Highly advanced security expertise can be difficult to source for smaller teams. The tool you choose needs to simplify backup management with automated testing and monitoring systems. The best backup and replication system tests your backups and monitors their integrity by running VMs directly from backup files or replicas in an isolated environment to verify recoverability.

This is where proactive monitoring features provide early threat detection through AI-powered malware detection and automated scans using a security and compliance analyzer. Everything begins and ends with a user-friendly interface designed for businesses like yours to reduce the need for constant supervision and extensive training. Features like automated backup validation and comprehensive dashboards for proactive threat monitoring and analytics make the management of backup and recovery processes easy and efficient, giving users real-time insights into data protection status.

Flexible Licensing and Scalability

Every small and medium-sized business needs data protection that can scale as their business and data volumes grow. However, licensing can be expensive and complex, with situations where smaller teams may need multiple vendor solutions to provide data everywhere-and-anywhere coverage without gaps.

The most versatile and affordable solution solves those challenges with a single comprehensive data platform and a universal license. This type of flexible, portable licensing gives your organization the flexibility and power to easily reallocate resources across virtual, physical, and cloud-based environments as your business needs change.

BaaS and DRaaS Considerations

If your business lacks internal IT personnel, you still need comprehensive backup and recovery with various options and a certain level of control. Backup-as-a-service (BaaS) and disaster-recovery-as-a-service (DRaaS) solutions should be part of a vendor's offering, including managed BaaS and off-site backup in addition to BaaS for Microsoft 365 and public cloud environments. These provide your business with additional layers of protection and recovery options.

Robust Support Ecosystem

Small and mid-sized orgs need a partner that can provide flexible, comprehensive data protection through solutions that are secure, reliable, and scalable. This means very little without the proper support, expertise, and personnel to make the solution work for your specific environment, business, people, and data.

The ideal vendor shows its commitment to supporting organizations like yours via a robust support ecosystem that would have 24/7 global support from hundreds of support engineers, an extensive knowledge base, and active user communities for peer assistance. Such comprehensive support means your business always has reliable and efficient issue resolution, no matter what challenges you face.

Meeting Your Organization's Changing Backup and Recovery Needs

This e-book has covered the critical data security factors that businesses like yours must consider when choosing a backup solution, including high availability, robust security, regulatory compliance/data sovereignty requirements, vendor lock-in, and business/technical needs.

Additionally, smaller teams should pay special attention to integrating with hybrid-cloud platforms and environments, ensuring ease of deployment, management, monitoring, automation, integration, and much more.

Taking these factors into account gives small teams the tools to make informed decisions that protect business data, support growth, and ensure long-term operational continuity.

Veeam continues to listen to the current and future needs of these organizations to deliver a backup and recovery solution platform that excels in terms of your protection, usability, versatility, and budget requirements.

Our goal as the ideal backup partner is to always be available to provide a clearer understanding of small/medium organizations' security backup and recovery landscape while providing solutions that protect your company's most valuable asset — its data.

About Veeam Software

Veeam, the #1 global market leader in data resilience, believes every business should control all their data whenever and wherever they need it. We're obsessed with creating innovative ways to help our customers achieve data resilience. We do that by offering purpose-built solutions that provide data backup, data recovery, data portability, data security, and data intelligence.

Headquartered in Seattle, with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, who trust Veeam to keeptheir businesses running.

Learn more at www.veeam.com or follow Veeam on Linkedin @veeam-software and X @veeam.

→ To learn more about Veeam solutions to support your small business

veeam.com