

How MSPs Can Deliver Data Resilience That Is Secure by Design

Contents

Introductions	**3**
Core Data Security Challenges for MSPs in an Evolving Threat Landscape	**4**
Ransomware and Extortion Attacks	4
Ai-Enhanced Threats	4
Phising and Social Engineering	5
DDoS Attacks and Service Disruptions	5
Shadow IT (Shadow SaaS, AI, and Data)	5
Supply Chain and Third-Party Risks	5
MSP Data Protection Complexity in Diverse Environments	6
Ensuring Regulatory Compliance and Data Sovereignty	6
Building a Secure-by-Design Data Protection Strategy for Data Resilience	**7**
Immutable Backups	8
Air-Gapped Storage	8
Continuous Monitoring and Alerts	8
Endpoint Security and Automated Recovery Testing	10
Integrating Secure-by Design Principles into End-to-End Data Security	10
The Role of Automation in Data Security	10
Further Requirements for a Secure-by-Design Data Protection Strategy	11
Improving MSP Visibility and Control	12
Choosing The Right Data Protection Partner for Total Security	**13**
Focusing on Proactive and Reactive Data Proteciton	14
Ensuring Seamless Integration with Security Partnerships	14
Ensuring Future Scalability and Growth	14
Flexibility to meet Client Needs	15
Centralized Management for Multi-Tenant Environments	15
Why Veeam is the Future of MSP Data Security and Resilience	**16**

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Introduction: The Strategic Business Importance of Data Security for MSPs

Any MSP that can solve the complex challenge of data security can build a trusted and profitable business. This has never been truer in an era of relentless and innovative cyber threats, where resilience is the means to giving clients true data security by design.

What does this mean?
The landscape of hybrid, multi-cloud, and virtual worlds is here to stay, and how organizations use them to drive and create data for business outcomes will always be in flux. In this permanently changing landscape, Zero Trust and National Institute of Standards and Technology (NIST) 2.0 frameworks are critical for showing how to navigate the terrain. What they cannot do is give MSPs the specific tools to construct a data security vehicle that will work for every organization in a multi-tenant environment.

Threats, along with data and the technology ecosystem it travels through, are always changing. NIST 2.0 and Zero Trust reflect MSP Cybersecurity best practices for MSPs to find practical ways to improve data resilience and meet security challenges.

Data resilience, in its most straightforward form, is about ensuring organizations have access to core business functions and data accessibility after an eventual cyberattack or outage. Zero Trust means that you "never trust, always verify" users and devices inside and outside your network. This least-privilege approach to data access is dynamically applied based on each user.

Zero Trust aligns with NIST and its core functions in vital ways for MSPs aiming to deliver secure-by-design data resilience by:

- Identifying a continuous inventory of assets, users, and their behaviors, ensuring all interactions are verified and monitored
- Protecting data and systems through a focus on identity access management
- Aligning continuous monitoring and constant verification
- Establishing strong governance policies for people, processes technology, and the data they use and produce
- Delivering resilient and secure backup and recovery of all core data and systems

This alignment provides a clear blueprint for MSPs to implement a secure-by-design approach to data resilience across multi-tenant environments. This demands that MSPs integrate security into every operational layer for a multi-faceted strategy that prevents breaches and data loss while ensuring quick recovery when such incidents occur.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Core Data Security Challenges for MSPs in an Evolving Threat Landscape

The primary task of an MSP is to protect critical client data from attacks that cripple each business's ability to operate and innovate by navigating a complex and dangerous landscape. Every overlooked vulnerability or unpatched system could open the door to infiltration and data exfiltration. MSPs must focus on prevention and recovery by seeing how sophisticated threats work together to achieve those goals.

Ransomware and Extortion Attacks

Many reputable surveys show over half of responding companies have suffered a ransomware attack in the last year, which was corroborated by Statista. Regardless of whether the overall percentage of businesses affected is much lower, MSPs can't afford to gamble with client data security and resilience.

It ultimately doesn't matter whether the data is encrypted, outright stolen, or the organization paid the ransom; productivity, resilience, and data are always lost in some form. According to a 2023 survey of 1,200 CISOs in the Veeam 2024 Ransomware Trends Report, 43% of ransomware-compromised data is irrecoverable.

The ways attackers gain access to data and how they control it can vary, which leads to the other top data security challenges for MSPs:

- Unpatched vulnerabilities and security gaps, which are often a root cause
- Preying on human errors via phishing and social engineering
- Business email compromise (BEC) attacks, which are far more targeted at executives and trusted business contacts

These are only some of the many means of infiltration leading to ransomware and data exfiltration, as well as posing significant risk to MSPs and their clients.

AI-Enhanced Threats

Cybercriminals are using generative AI to scale their attacks, generate malicious scripts, and develop more targeted phishing campaigns. These AI-based cyber threats are among the top emerging risks, according to a recent Gartner survey.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Phishing and Social Engineering

Threat actors use sophisticated tools like generative AI to craft convincing emails, impersonate trusted individuals, and create deepfake identities. MSP clients are especially vulnerable, as they often operate in hybrid environments where communication spans multiple channels and platforms, increasing the likelihood of a breach.

Ready-made phishing kits on the dark web eliminate the need for bad actors to understand sophisticated technologies and coding. This only makes recovery a more crucial part of data resilience.

DDoS Attacks and Service Disruptions

Distributed denial-of-service (DDoS) attacks are becoming harder to detect and mitigate, especially application-layer attacks that directly target critical business functions. With DDoS-as-a-service platforms now readily available, even inexperienced attackers can launch large-scale disruptions. These attacks threaten the availability of client services and the trust placed in the MSP's ability to maintain business continuity.

Shadow IT (Shadow SaaS, AI, and Data)

Shadow IT has become more of a core data security problem for MSPs where every client operates in a hybrid/multicloud and SaaS world. This is bigger than the unauthorized use of applications like Slack, Trello, Zoom, ChatGPT, Dropbox, and many others. It now includes the data stored and moved across cloud environments.

A recent IBM article citing their "Cost of a Data Breach Report" revealed that data stored across an organization in multiple environments was compromised in 40% of incidents, while unmanaged data sources (shadow data) were affected in 35% of breaches.

MSPs should follow NIST 2.0 and Zero Tolerance frameworks as part of their monitoring and detection tool/technology implementations. The challenge comes when disparate tools lead to increased work to track results across a multi-tenant environment.

Supply Chain and Third-Party Risks

For MSPs, managing the security of not just their clients but the associated supply chain as well adds another layer of complexity to an already demanding role.

Cybercriminals are increasingly leveraging supply chain zero-day vulnerabilities as an efficient way to infiltrate networks. These cyber attackers exploit supply chain partner infrastructure or software to gain access to sensitive systems or use social engineering attacks on third-party vendors.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

MSP Data Protection Complexity in Diverse Environments

MSPs face unique challenges in safeguarding diverse, multi-tenant environments where they must provide end-to-end, proactive, and reactive data protection. Each client's needs are different, and workloads often span on-premises, cloud, and SaaS environments.

The mix of hybrid, virtual, and physical environments, platforms, and endpoint devices alone makes data protection across diverse environments a complex challenge for MSPs. The widespread use of platforms like Microsoft 365 further complicates data protection efforts, as clients demand seamless integration with their existing systems. Many phishing campaigns look to rob credentials by compromising cloud-based services, e.g., Microsoft 365 or Google Workspace.

Limited resources, including limited budgets for advanced tools and expert personnel, can create data security gaps. Data silos and a lack of vendor integration also hinder the ability to implement effective proactive and reactive data protection measures.

Ensuring Regulatory Compliance and Data Sovereignty

Data security across multi-tenant environments becomes more challenging when factoring in data movement and storage across different hybrid and virtual environments. This adds to the complexity and pressure of meeting diverse regulatory requirements across multiple industries where a host of regulations and auditing practices are in place. By addressing these core data security challenges, MSPs can enhance their ability to deliver secure-by-design data resilience, safeguarding their clients' critical assets in an increasingly hostile cyber environment.

The stakes of providing data resiliency are high since a single breach can ripple across the entire client base, jeopardizing the provider's reputation and business. Ensuring this never happens requires every MSP to establish a thorough data protection strategy.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Building a Secure-by-Design Data Protection Strategy for Data Resilience

The fast pace of technology shifts and cyber threats requires every MSP to develop a comprehensive data protection strategy to meet evolving client needs.

Rather than developing the granular expertise of a managed security services provider (MSSP) focusing on experts keeping pace with every security adjustment, MSPs need an agile and adaptable strategy. On a foundational level, this starts with frameworks and guidelines like NIST and Zero Trust that keep pace with changing security needs and threats.

MSPs can then build on this framework and foundation to craft a strategy driven by backup best practices, features, and solutions that drive data resilience. This gives MSPs and their clients the ability to recover fast and maintain business continuity when incidents occur. To achieve this, companies need a comprehensive and agile platform approach that enables the following attributes.



© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Immutable Backups

Data stored in immutable backups remains unchangeable, providing an unassailable layer of protection against ransomware and other threats. With data, workflows, and platforms in the cloud, the major cloud storage providers have object lock technology. This means critical data will remain uncompromised even if production systems are breached.

MSPs working in a multi-tenant framework often need additional control over immutability. This may include retention policy management to support changing clients/SLAs and immutability duration and changes.

Air-Gapped Storage

Physically or logically isolating backups creates a barrier against attacks. Air-gapped storage, whether through secure tape solutions or isolated cloud instances, makes critical data inaccessible to cybercriminals.

Continuous Monitoring and Alerts

Alarms and visibility are critical to resilience and a secure-by-design approach. AI-driven monitoring tools detect ransomware activity early, enabling swift containment. These systems analyze user behavior, flagging unusual patterns such as sudden data encryption.

MSPs often deal with a mix of legacy and new data and technology stack infrastructure. These environments are continuously in flux, so monitoring and alerts give MSPs a way to deliver both proactive and reactive data security across complex environments. The right solution should offer:

- Threat detection and protection to identify and neutralize malware, phishing attempts, and other attacks before they escalate
- Data resiliency via backup and recovery alerts and monitoring
- Increased network visibility (VMs, objects, groupings, and their physical elements) across internal/external flows, and connections to determine normal behavior

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Endpoint Security and Automated Recovery Testing

True endpoint security and protection requires advanced endpoint monitoring tools to protect client devices, while real-time threat detection systems identify and neutralize malware, phishing attempts, and other attacks before they escalate.

Regularly testing backups is also critical, as this guarantees they work properly and can be recovered. Automated recovery tools, meanwhile, enable near-instant restoration of systems, reducing downtime from days to hours.

All the above measures align with NIST 2.0 guidelines and the Zero Trust framework as part of a secure-by-design recovery strategy.

Integrating Secure-by-Design Principles into End-to-End Data Security

A secure-by-design approach demands that MSPs integrate security into every layer of their operations to stop sophisticated ransomware and other attacks. MSPs can use NIST alignment to make sure a multi-tenant client environment is built on secure-by-design principles that encompass present and future data and technology infrastructure. The provider can integrate this framework into each client's environment regardless of their differing architectures, needs, and level of sophistication or sector.

Key components of these frameworks for end-to-end data security include:

- **Zero Trust identity management** Identity access management (IAM) solutions provide granular control, preventing unauthorized access to sensitive systems via multi-factor authentication (MFA) and a least-privilege access model, meaning no user or device is trusted by default.
- **End-to-end encryption** This is non-negotiable for both data at rest and in transit to ensure confidentiality and meet compliance standards; secure-by-design solutions use advanced encryption protocols to safeguard all data flows.
- **Firewalls and network segmentation** Next-generation firewalls and segmented networks isolate potential breaches, preventing lateral movement by attackers.

These and many other aspects of a secure-by-design approach enlist automation to increase the effectiveness of data security.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

The Role of Automation in Data Security

Automation and AI in data security are critical enablers of secure-by-design data protection strategies. By reducing human error and increasing efficiency, MSPs can deliver data resiliency to their clients through the following mechanisms.



AI-Powered Threat Detection

AI tools can record and analyze patterns in real time to detect anomalies and immediately alert on possible threats.

For example, they can flag login or data access attempts that are out of the ordinary.



Automated Backup Scheduling and Replication

Automation ensures that backups occur regularly, minimizing gaps in data protection. Critical workloads are prioritized, and backups are stored across diverse locations for redundancy.



Immutable Storage Snapshots

A backup and recovery platform capable of this level of automation creates immutable snapshots immediately upon backup. These real-time snapshots safeguard backup data from ransomware encryption and other threats.



Disaster Recovery (DR) Orchestration

Automation streamlines recovery processes, ensuring clients can recover entire systems quickly without manual intervention. Features of DR orchestration, like automated failover and granular recovery, support rapid restoration of critical systems.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Further Requirements for a Secure-by-Design Data Protection Strategy

Secure-by-design data resilience mandates:

- Proactive security tools for detecting and preventing threats before they cause damage
- Backup and disaster recovery solutions, which serve as the last line of data security defense via both proactive and reactive measures

The right backup and recovery solution should bring comprehensive automation and integration that supports:

- IAM management and monitoring that provides integration and visibility into existing IAM architectures such as cloud-based IAM services like Entra ID
- Threat detection and response for complex threat detection and analysis, existing SIEM/SOAR platform integration, and automated recovery
- Robust encryption that includes KMS integration
- Endpoint security compliance monitoring
- Incident investigation and forensics
- Threat isolation and cleanup
- Security task automation, e.g., for data protection software updates
- RESTful APIs that use automation and standardization for deployment, job configuration, third-party integration, and access
- Proactive compliance audits where automated audit tools verify compliance with regulations like GDPR and HIPAA, providing MSPs with actionable insights to close gaps

By embedding automation into backup, recovery, and threat detection processes, MSPs can enhance both the efficiency and reliability of their data protection strategies.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Improving MSP Visibility and Control

To implement secure-by-design principles effectively, MSPs need centralized tools that provide full visibility and control over client environments via:

- **Integrated dashboards:** Unified dashboards give MSPs a comprehensive view of backup status, security incidents, and recovery readiness across all clients.
- **Real-time alerts and reporting:** Continuous monitoring and automated alerts ensure teams identify and address threats before they escalate.
- **Assured compliance and data sovereignty**

All the solutions and approaches in this chapter position MSPs to fully support their clients in meeting compliance requirements for industry-specific regulations through:

- **Localized storage:** Offering regional storage options ensures compliance with data sovereignty laws, preventing sensitive information from crossing unauthorized borders.
- **Immutable storage and audit trails:** Immutable backups and detailed logs satisfy legal requirements for data integrity and traceability, protecting clients against fines and reputational damage.
- **End-to-end encryption and access control:** Encrypted data, coupled with robust access controls, ensures compliance with industry regulations while maintaining client trust.

By adopting a secure-by-design approach, MSPs can be certain that they are accounting for data protection in every aspect of each client's operations. Immutable backups, layered defenses, AI-driven automation, and centralized control provide the foundation for true data resilience.

When combined with strict adherence to regulatory frameworks and Zero Trust principles, these strategies enable MSPs to deliver the secure and reliable services their clients expect.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Choosing The Right Data Protection Partner for Total Security

It's difficult under the best of circumstances to choose the ideal data protection partner for MSPs. Different needs, legacy and hybrid architectures, existing cybersecurity solutions, and a host of other variables only add to the challenge.



Costs in terms of what MSPs and their clients can afford and the immovable high threshold for complete data resiliency can often be at odds. This means the right partner should first provide:

- Easy integration, security, reliability, and scalability
- Robust data resilience across complex and varied hybrid environments
- Fast, flexible, and secure recovery
- Visibility for MSP clients via reporting and/or dashboards for status of data protection, such as job config/retention policy changes and RTO/RPO status
- Deep automation and integration with third-party solutions to meet diverse client environment protection scenarios
- Flexible licensing options and predictable pricing models that scale with the MSP's client base

However, an MSP must have a data protection partner that goes beyond these elements in the following ways.

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Focusing on Proactive and Reactive Data Protection

The best solutions enable both proactive and reactive threat detection, monitoring, alerts, and remediation (including response where possible and backup and disaster recovery as the last line of defense). This provides a holistic approach to data security that covers all potential vulnerabilities and attack vectors for business continuity and data resilience. MSP clients expect nothing less.

Ensuring Seamless Integration with Security Partnerships

Your backup solution should offer seamless integration with third-party detection, investigation, and response platforms for broad resilience. Automation systems, as well as AI-driven platforms for unified security and observability, work in partnership to meet Zero Trust frameworks and NIST guidelines, delivering maximum data resilience and protection.

Ensuring Future Scalability and Growth

MSPs need data protection solutions to be scalable to meet the growth of individual clients and their client base, which means:

- Prioritizing solutions that offer multi-tenant management, flexible and scalable backup and disaster recovery options, and seamless integration with cloud and hybrid infrastructures
- Delivering regular updates, vigorous support, and continuous monitoring across changing environments, with analysis that learns what is normal and data on emerging threats

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Flexibility to Meet Client Needs

One size will never fit everyone in the world of data protection, so the chosen partner must provide MSPs with:

Data protection services that cater to businesses of various sizes, from smaller and mid-sized organizations to large enterprises

Tiered solutions that address diverse needs, including backup frequency, retention, and disaster recovery capabilities

Centralized Management for Multi-Tenant Environments

MSPs that use multitenancy have different clients, approaches, and needs for delivering data security and resilience. However, they all require:

- Managing multiple client environments with centralized control for backup, security, and disaster recovery
- Real-time monitoring and alerting systems to ensure continuous protection and quick identification of potential issues

Of course, none of the above will mean much to MSPs that need to satisfy and grow a diverse client base without comprehensive support geared to their needs, both today and tomorrow.



© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Why Veeam Is the Future of MSP Data Security and Resilience

One thing MSPs know is that everything will change tomorrow. This means that they need to offer total data protection—from proactive threat prevention to backup and rapid recovery.

Veeam solutions are purpose-built for powering data resilience via data backup, data recovery, data portability, data security, and data intelligence. With Veeam, IT and security leaders rest easy knowing that their client apps and data are protected and always available across cloud, virtual, physical, SaaS, and Kubernetes environments.

Veeam is your ideal data protection solution partner. You'll not only be able to leverage innovative solutions but also gain a true partner that's dedicated to helping you deliver reliable BaaS and DRaaS offerings. MSPs can unlock exclusive products, pricing, and perks that are designed to fuel your recurring revenue business by joining the Veeam Cloud & Service Provider (VCSP) Program.

No matter what may change tomorrow, MSPs have a partner capable of meeting the challenge of delivering secure-by-design data resilience.

About Veeam Software

Veeam, the #1 global market leader in data resilience, believes every business should be able to bounce forward after a disruption with the confidence and control of all their data whenever and wherever they need it. Veeam calls this radical resilience, and we're obsessed with creating innovative ways to help our customers achieve it.

Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 68% of the Global 2000, who trust Veeam to keep their businesses running. Radical resilience starts with Veeam.

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

→ To learn more about how Veeam supports comprehensive data protection for MSPs

© 2025 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.


veeam
veeam.com