Veeam Cloud & Service Provider Program

Achieving Ransomware Resiliency with BaaS and DRaaS

Table of Contents

Ransomware is evolving

As the development, distribution and stealth of ransomware increases, and human error makes the job of bad actors easier, comprehensive data defense is the only answer. This becomes even more clear when there is no guarantee of regaining access to your data by paying the ransom.

In 2021, 47% of the data attacked was encrypted, and of that data, only 64% was recoverable. That's according to the industry's largest independent worldwide study and global report, Veeam's® "Data Protection Trends Report."

Penetrating a network and encrypting data via ransomware is becoming a more effective strategy for cybercriminals as time goes on. Ransomware as a Service (RaaS) makes it easier for those with limited knowledge to launch an attack with minimal investment. Criminal groups act as the operators, attracting affiliates (hackers) with everything they need to target organizations — for a fee.

Organizations of all sizes are failing to address security gaps or strengthen the weak link of people in the security chain. According to the Data Protection Trends Report, 76% said they suffered from some type of ransomware attack in 2021.

Managed Service Providers (MSPs) seeking to supply a comprehensive level of defense to their SMB customers must start with business continuity and disaster recovery (BCDR). Supplying that type of data resiliency requires MSPs to understand and have solutions to the challenges they face. This starts with defining how Backup as a Service (BaaS) and Disaster Recovery as a Service (DRaaS) can break the cycle of ransomware effectiveness.

76%

suffered from some type of ransomware attack

47%

of the data attacked was encrypted

64%

was recoverable

MSP challenges in protecting customer data

MSPs vary in their approach to fulfilling the security needs of their customers, as these can range from issues related to protecting multi-cloud environments or complex on-premises infrastructure to endpoint vulnerabilities. MSPs also face the unique dual challenge of having to defend their own environments to prevent supply chain attacks while also fortifying the environments of their customers against bad actors.

This has led to a plethora of security solutions that include or rely on BCDR. Most of these solutions, however, leave gaps in security coverage, which MSPs can find difficult to monitor and manage. The alternative - managing multiple solutions can also be difficult and costly. Service providers are therefore often unable to present a compelling service model to prospective customers.

An increasing number of experts, organizations and MSPs understand that a secure backup is the last line of defense in combating ransomware. But there are still countless service providers that have yet to embrace this reality. Their ability to make that determination requires gaining a true understanding of how BaaS and DRaaS work and how it's effective in protecting MSPs and their customers.

Combating ransomware with BaaS & DRaaS

Companies are increasingly looking to cloud-based services like BaaS and DRaaS to help solve their data protection challenges, including ransomware. It helps to understand the difference between these services and how they support combating ransomware.

BaaS

Backup as a Service (BaaS) is an approach to data protection where companies purchase backup and recovery services from a provider. Instead of performing backups and restores plus maintaining hardware, software and licensing independently (whether data is on-premises and/or a public or private cloud), BaaS enables a company to essentially outsource backup responsibilities to an expert in various ways. This model takes the CapEx and internal admin needs out of the equation since the service provider will handle maintenance, management and monitoring to deliver the following benefits:

- Monitoring and reporting of data protection status
- Comprehensive data encryption
- Redundancy and failover for fast recovery (RTO and RPO)

BaaS use cases

There are many different solutions a service provider may offer that fit under the BaaS category.

Off-site backup

Off-site backups are the foundation of a BCDR strategy focused on mitigating any kind of downtime risk. The ideal best practice is the 3-2-1-1-0 rule where three backup copies are created, with two copies on different types of media, one copy stored off-site and one copy stored offline so it always remains untouched and unchanged. The zero stands for ensuring all copies are stored without errors. This requires daily monitoring for errors that are corrected via regular restore testing.

Different backups that are commonly used include:

- Tape backups for long-term storage of massive amounts of media-rich data on external drives, discs or other external media
- Cloud backups that mirror on-site data
- Hybrid cloud backups that combine local (on-site) and cloud backups to optimize security and minimize risk

Service providers can offer this service with a multi-tenant infrastructure and flexible BCDR solution. This is an effective customer acquisition strategy that gives the MSP an opportunity to sell more value-added services like DRaaS.

Managed backup

Managed BaaS is often available in two varieties: partially or fully managed. Some companies engage in partially managed agreements where there is shared responsibility for backup and recovery duties. This may mean the customer has access to a self-service portal to maintain backup jobs and recover files as needed and the service provider is responsible for overall software maintenance and patching. The customer submits service desk tickets for any issues and expects a response within a predefined amount of time.

In fully managed scenarios, the company outsources all backup responsibilities. The customer may still access self-service portals for reporting and dashboards or even restore capabilities. What is in the scope of the BaaS offering is defined upfront with agreed-upon SLAs.

To offer managed backup services, MSPs must focus on balancing costs and accessibility, not to mention nearly infinite scalability and recovery speeds that meet SLAs. These factors are all integral to attracting customers and ensuring customer loyalty and satisfaction. To offer such backup services, MSPs will require advanced features that include:

- End-to-end data encryption for full security
- Single-pane-of-glass remote management and monitoring
- Automatic data verification
- Ability to control backup schedules and data retention
- True multi-tier, multi-tenant cloud architecture

Public cloud

It can be difficult for organizations to understand who is responsible for what when it comes to cloud security. This affects the way organizations set up their cloud architectures and how MSPs can manage and monitor those architectures for security vulnerabilities. Making matters more challenging is the difference in how the major cloud providers like Amazon Web Services (AWS), Google Cloud and Azure apply the shared responsibility model.

Cloud providers, organizations and encryption tools all have their shortcomings in how they handle (or don't handle) encryption. Encryption keys and encrypted data control can create challenges for an MSP without some form of unified encryption support that enables more flexible and consistent management and monitoring.

This is where service providers can help customers protect their data that is hosted in public cloud providers like AWS or Microsoft. The data and applications in these environments are not immune to ransomware threats and need to be considered part of a comprehensive strategy.

DRaaS

DRaaS uses data protection software for disaster recovery efforts. During an outage, the data protection software powers on or recovers data at an appropriate location, usually a secondary site or the cloud. The DRaaS provider returns IT infrastructure control and functionality to an organization after a disaster. This is one reason estimates call for the global DRaaS market to hit $26.73 billion in 2026.[2]

DRaaS uses virtual servers to mirror a complete existing infrastructure (compute, storage and networking functions) in fail-safe mode. Businesses can thus continue running their applications from a cloud environment managed by the service provider to avoid using the compromised on-site servers. The result is fast or nearly instant post-disaster recovery for a business, which can then migrate data and processing back to the new or recovered on-site servers when ready.

While BaaS only moves an organization's data, DRaaS moves data, computing and networking to the cloud for access and recovery.

Every organization needs to protect data in the digital age. BaaS and DRaaS are complementary solutions that work best in tandem when the unexpected happens — cyberattacks, insider threats, hardware failures or natural disasters.

The challenge for many SMBs is that the process and costs of monitoring and managing these environments can be burdensome. That is why SMBs are increasingly turning to MSPs for this service, either as a single tenant or part of a multi-tenant environment run by the service provider.

Mapping a Cybersecurity defense strategy

Every business today essentially runs on data. The ability to protect data and avoid business downtime will continue being a challenge going forward as ransomware attacks grow in number and sophistication. It's estimated that downtime costs $1,467.00 per minute or $88,000 per hour, according to Veeam's 2022 Data Protection Trends Report.

MSPs must develop and map a cybersecurity defense strategy to avoid customer environment downtime and close the gap between data recovery SLAs and speed. This is vital for the protection of customer and MSP data. A sound defense strategy requires a singular, holistic and highly integrated end-to-end BCDR solution that can:

- Identify potential ransomware activity
- Verify data protection
- Detect data and backup procedure and system anomalies proactively
- Respond to detected threats or system anomalies
- Enable scalable recovery without introducing threats
- Provide speed of service via automation and orchestration

The five crucial points for an effective defense strategy

Earning customer loyalty means constant scrutiny of the MSP for delivery of value, service and ROI. With ransomware resiliency, an MSP's backup defense strategy is the foundation for ensuring the safety and availability of customer data. There are five crucial points that the strategy must provide: immutability, proactive monitoring and alerting, protecting tenant backups, backup verification, and quick recovery.

1 Immutability

Protecting data through immutable backup storage is paramount so that data remains fixed to ensure it cannot be deleted, encrypted or changed. That requires MSPs to provide immutability for a wide variety of storage options to meet the needs of customers. This is true whether it's short- or long-term storage of structured or unstructured data across on-premises and multi-cloud environments.

The foundation of the Veeam Platform, Veeam Backup & Replication™, enables on-site, immutable, short-term backup storage for fast recovery. This includes options like a Hardened Linux repository to enable immutable primary backups using generic compute and storage with a supported Linux x64 distribution (this negates the need for a packaged storage appliance). It also enables tiering of backups into an off-site immutable object storage offering, providing additional protection against malicious activity or accidental deletion.

These immutability options can be applied for every MSP customer use case and requirement across sectors, including the protection of an MSP's own infrastructure. This is where having object storage immutability options for cloud and on-premises can come into play. Service providers can also offer their own immutable object storage by partnering with a Veeam Ready – Object partner like Backblaze or Wasabi.

To see a complete list of Veeam-verified partners, visit our directory>>

2 Ensuring 24/7 proactive monitoring & alerting

Monitoring and alerting can only be effective if they are proactive, not reactive. MSPs rely on backup alerts to let them know when disk space is running low, there's been a VM backup failure, or that certain data has been collected and backed up properly, to name just a few.

The ability to automate alerts is vital when there may be hundreds of alerts enacted across different tenant environments by an MSP. These alerts must be highly accurate, with the ability to fine-tune them so false alarms don't waste time and money or increase risks.

It's also important to have timely, regular, intuitive and actionable reports on whether the MSP consistently configures the backup system and environment in the most optimal way. These can include backup infrastructure, job history and capacity planning reports, among others.

Veeam partners and customers alike can gain actionable insights to detect ransomware. Veeam ONE™ provides proactive monitoring, reporting and alerts via 340+ preset alarms and 150+ pre-built reports, including infrastructure performance and configuration assessments. All of this helps MSPs maximize monitoring and alerting benefits to:

- Detect anomalous activity for CPU/memory/network/IO utilization and more, along with incremental backup size anomaly detection
- Tune predefined alerts
- Create custom alerts from metrics exposed from bare metal to applications

Veeam ONE can monitor the Veeam Backup & Replication environment as well as virtual infrastructure. To enable monitoring in a multi-tenant environment, add VMware Cloud Director or vSphere as a monitored instance in Veeam ONE. From there, partners can set up the web-based application to allow clients with access to self-serve with dashboards and reporting.

3 Protecting tenant backups from intentional or accidental deletion

Any backup solution implemented by an MSP can fall prey to insider attacks or accidental deletion. This requires an MSP to have a mechanism to protect backup data of physical or virtual machines, Microsoft, Linux and more. This is where the Insider Protection feature within Veeam Cloud Connect supports a modern data protection strategy.

Veeam Cloud Connect enables easy off-site backups and replicas to a Veeam-powered BaaS or DRaaS service provider without second infrastructure management complexity. Essentially, Veeam Cloud Connect makes Veeam-powered BaaS and DRaaS possible.

When enabled, Insider Protection provides retrieval of specific restore points in the backup chain from a file in the recycle bin to help prevent intentional or accidental deletion. Veeam Cloud Connect also gives MSPs the control to protect and recover Tier-1 applications via vSphere APIs for I/O Filtering (VAIO) for continuous replication to private or managed clouds.

4 Verifying backups automatically to ensure recovery

Service providers need an efficient way to ensure backups are successful that doesn't involve building their own scripts or using backup logs that don't show the recoverability of data. Creating a process is time-consuming, so MSPs must be able to verify backups automatically for successful recovery.

Another important and useful feature in Veeam Backup & Replication is SureBackup®. SureBackup allows you to test VM backups and confirm if you can recover data successfully. Veeam Backup & Replication scans the backed-up data for malware, boots the VM in an isolated environment, performs the test and reports back the results.

5 Validating backups are clean before restoring them

It's imperative that service providers have an efficient and assured way to validate backups before restoration, that is, using antivirus software to scan machine data before restoring it to your production environment. If the antivirus software detects malware during the scan, the backup solution should be capable of stopping the restore process or completing the restore with restrictions based on predefined settings.

The Veeam Platform enables partners to successfully restore data, with native features like Secure Restore and Instant Recovery.

Secure Restore enables you to restore data to the production environment after it is reviewed with antivirus software. If the antivirus software detects malware, Veeam Backup & Replication will halt the restore process or restore with restrictions. With Secure Restore, service providers can run multiple automated (scheduled) or manual configurable tests on backups to confirm data is malware-free and recoverable.

With Instant Recovery, service providers can immediately recover workloads to a production environment by running them from compressed, deduplicated backup files. This enables MSPs to meet and improve customer recovery objectives.

Veeam solutions are purpose-built for standalone organizations and MSPs to deliver easy accessibility, manageability and monitoring via a centralized console. This allows you to administer backup, restore and replication operations in all supported platforms (virtual, physical, cloud) to achieve ultimate data protection resiliency.

In summary, utilize these five crucial points for an effective defense strategy and ransomware resiliency:

1 Immutability

2 Ensuring 24/7 proactive monitoring & alerting

3 Protecting tenant backups from intentional or accidental deletion

4 Verifying backups automatically to ensure recovery

5 Validating backups are clean before restoring them

Achieving data protection and resiliency with Veeam

Veeam supports partners with the technology and programs to deliver Veeam-powered solutions to meet their customer's data protection needs. With a simple, flexible, reliable and powerful platform, Veeam enables partners to deliver BaaS & DRaaS solutions that ensure customer confidence and loyalty.

Veeam delivers end-user security and architecture control so MSPs can create single and multi-tenant environments. With an API-driven architecture that uses native snapshots, storage options and security bolstered by universal immutability, Veeam meets every customer data backup and recovery requirement whether on-premises or in the cloud.

MSPs supporting the backup and recovery needs of large enterprises face the same challenges as an SMB client but on a larger scale. This level of scalability and flexibility must also meet MSPs serving multiple tenants.

Do you support large enterprise clients?

Veeam Disaster Recovery Orchestrator helps large companies automate and orchestrate their disaster recovery response. Designed for companies with their own secondary data center, Veeam Disaster Recovery Orchestrator:

- Automates DR testing
- Dynamically generates documentation
- Helps avoid RPO and RTO violations
- Enables resiliency with one-click recovery

By supporting rather than competing with partners, Veeam delivers the technology and support that grow your business, bottom line and customer trust. MSPs and their customers demand affordable, flexible and agile protection against ransomware, which Veeam has delivered to countless service providers and customers across the globe.

Visit our site to learn more about **Veeam-powered BaaS and DRaaS to combat ransomware.**

You can also join our **Veeam Cloud & Service Provider partner program** or **request a consultation.**

[1] "ransomware as a service," Sean Michael Kerner, 2021. (TechTarget's Tech Accelerator: "The complete guide to ransomware")

[2] "Disaster Recovery as a service (DRaaS) Global Market Report," March 2022. The Business Research Company