



Veeam vs. SMB vendors

Quick Feature Comparison

The following document highlights Veeam®’s unique capabilities for data protection across major workloads vs. the general competition of vendors which specialize in the backup for small and midsize business (SMB). These include Acronis, Altaro, Arcserve, Druva, Nakivo, Unitrends and Veritas Backup Exec.

SMB-specialized backup vendors may provide benefits like very low prices and upfront simplicity, but they do not offer the functionality and customization necessary to tailor data protection to your business needs. Nor do they offer the scalability or workload support that your business will need as your IT infrastructure grows.

The following document highlights Veeam’s capabilities for data protection across major workloads vs SMB-specialized backup vendors.

Feature	Veeam	Competition	Details
Virtual machine data protection			
Protect data on any major hypervisors			Veeam: Natively backup and recover data for all major hypervisors (VMware, Microsoft Hyper-V, Nutanix AHV, and Red Hat). Competition: Vendors typically backup VMware and Hyper-V only.
Properly protect and recover applications			Veeam: Protect all major applications, including Microsoft, Oracle, SAP, MySQL. Easily protect applications with advanced integrations like agentless application-aware backup and logs processing. Minimize downtime thanks to intuitive wizards for granular application item recovery. Competition: Vendors support Microsoft applications only (sometimes not all Microsoft applications). Vendors regularly need agents to backup applications and do not fully protect applications (i.e. no or limited logs support). Vendors typically do not offer application item recovery for all applications and offer basic granular recovery options.
Minimize data loss and downtime			Veeam: Achieve any RPOs, down to seconds, thanks to a single platform that offers CDP, VM replication, storage snapshot, backup, and backup archiving. Minimize RTOs by restoring data in the best way for your organization, no matter the issue, thanks to the broadest set of recovery options. Cross-platform instant recovery lets you restore virtual, physical, and application data in minutes. Competition: Vendors lack the capabilities needed to achieve the RPOs that critical workloads need, as they do not provide CDP and typically lack storage snapshot integrations, offering only backup and basic VM replication. Most vendors cannot minimize downtime due to their limited set of recovery capabilities and manual steps in some recovery scenarios (i.e. ransomware recovery).
Reuse backups for more than recovery		to	Veeam: Verify backups and replicas recoverability by running advanced tests on them in isolated sandboxes. Reuse backups for business purposes by running them in on-demand sandboxes (i.e. for test & dev, security tests). Competition: The few vendors that offer recoverability verification typically offer few and basic tests as well as no or poor sandboxes isolation. Vendors do not offer on-demand sandboxes to use for business purposes.



Feature	Veeam	Competition	Details
---------	-------	-------------	---------

Public cloud data protection

Protect data on any major clouds			<p>Veeam: Natively backup and recover data for all major clouds: AWS, Azure, and Google Cloud.</p> <p>Competition: Vendors natively support 1 cloud at best and regularly use backup agents to protect cloud data.</p>
Protect all major cloud instance types			<p>Veeam: Natively protect cloud instances beyond computing instances, including cloud databases (i.e. RDS, Azure SQL) and private network settings (i.e. VPC).</p> <p>Competition: Most vendors offer basic cloud integration and support computing instances only (cloud databases and private network settings not supported).</p>
Move data anywhere			<p>Veeam: Move data to, from, across, and within any clouds and on-premises. Store backups of a cloud workloads on other clouds or on-premises. Restore backups of a cloud workloads to another cloud or on-premises.</p> <p>Competition: Vendors do not offer data mobility (i.e. no AWS to VMware mobility). They can rarely store backups of a cloud workloads out of that cloud. They cannot restore backups of a cloud workloads to another cloud or hypervisor.</p>

Physical server data protection

Protect data on any major physical systems			<p>Veeam: Natively backup and recover data for all major physical systems: Windows, Linux, MacOS, IBM AIX, and Oracle Solaris.</p> <p>Competition: Most vendors natively protect Windows and Linux systems only.</p>
Protect all major applications			<p>Veeam: Protect all major Enterprise applications and databases, including Microsoft, Oracle, SAP, MySQL, and more. Easily protect and restore applications with native integrations for application consistency, logs processing, and granular application item recovery.</p> <p>Competition: Vendors support Microsoft applications only (sometimes not all Microsoft applications). Vendors typically offer no or limited logs support, do not offer application item recovery for all applications, and offer basic granular recovery options.</p>
Minimize downtime			<p>Veeam: Minimize RTOs by restoring data in the best way for your organization, no matter the issue, thanks to the broadest set of recovery options (full machine, disk, file). Cross-platform instant recovery lets you restore physical servers to hypervisors or clouds in minutes.</p> <p>Competition: Most vendors cannot minimize downtime due to their limited set of recovery capabilities and manual steps in some recovery scenarios (i.e. no Bare Metal Recovery). Vendors rarely offer instant physical server recovery or physical to virtual/cloud conversion capabilities.</p>

Workstation data protection

Protect data on any major workstation systems			<p>Veeam: Backup and recover data for all major workstation systems: Windows, Linux, and MacOS.</p> <p>Competition: Most vendors typically protect Windows systems only, sometimes Linux systems too.</p>
---	--	--	---



Feature	Veeam	Competition	Details
Properly protect and recover workstations			<p>Veeam: Protect workstations wherever they are without hindering users' activity, thanks to workstation-specific capabilities (i.e. local backup cache in case workstations cannot connect to corporate network during backup, settings to control backup in case of low battery or metered network).</p> <p>Competition: Many vendors protect workstations like they protect physical servers, making it difficult to properly protect workstation off the corporate network. Vendors rarely offer a local backup cache or settings to control backup in case of low battery or metered network.</p>
Minimize downtime			<p>Veeam: Minimize RTOs by restoring data in the best way for your organization, no matter the issue, thanks to the broadest set of recovery options (Bare Metal Recovery, full machine, disk, file). Cross-platform instant recovery lets you restore workstations to hypervisors or clouds in minutes.</p> <p>Competition: Most vendors cannot minimize downtime due to their limited set of recovery capabilities and manual steps in some recovery scenarios (i.e. no Bare Metal Recovery, no full machine or disk restore). Few vendors offer instant workstation recovery or workstation to virtual/cloud conversion capabilities.</p>

NAS data protection

Protect data on any major NAS systems		to	<p>Veeam: Backup and recover data for all major types of NAS shares: SMB, NFS, Windows, Linux, and specific NAS filers (i.e. Dell EMC PowerScale, Lenovo ThinkSystem DM, NetApp ONTAP).</p> <p>Competition: Several vendors cannot protect NAS data yet. Vendors that protect NAS data typically do not support all NAS configurations (i.e. no NAS filer integration, lacking support for SMB, NFS, Windows, or Linux).</p>
Minimize downtime			<p>Veeam: Minimize RTOs by restoring NAS data in minutes with instant file share restore.</p> <p>Competition: Vendors cannot minimize downtime due to their limited set of recovery capabilities and lack of instant file share recovery.</p>

Monitoring and reporting

Simplify data protection administration			<p>Veeam: Centrally monitor all your data protection activities and data, thanks to a single intuitive dashboard across all sites and workloads. Get detailed information about each task.</p> <p>Competition: Vendors offer basic dashboard information and sometimes lack monitoring across sites or workloads. Dashboards provide scarce details about each task.</p>
Make informed decisions thanks to insightful reports			<p>Veeam: Gain complete visibility of, and insight into, your data protection activities thanks to the broadest set of pre-built and customizable reports. Reports cover all activities (i.e. backup, restore, administrative), production workloads status, backup infrastructure components status, and more.</p> <p>Competition: Gain marginal visibility of, and insight into, your data protection activities, as vendors offer few and basic reports focused on backup and restore jobs results only (failure, caution, success).</p>
Automate issues troubleshooting and fixing			<p>Veeam: Solve issues before they become a problem and eliminate manual issues troubleshooting and fixing, thanks to Intelligent Diagnostics and Automated Remediation, which find potential issues before they cause trouble and recommends solutions that Veeam can automatically implement if desired.</p> <p>Competition: Administrators must manually troubleshoot and fix issues after they impact production or backup data, as vendors lack automated issues analysis, solution recommendations, and automated issues fixing.</p>



Feature	Veeam	Competition	Details
---------	-------	-------------	---------

Ransomware protection

Mitigate issues before they become threats to your environment			<p>Veeam: Mitigate the risk of threats before they jeopardize your business, thanks to potential ransomware alarms triggered by suspicious activities on VMs and backup files (i.e. abnormal CPU usage or datastore write rate). Additionally, you also get automated regular antivirus scanning of backups.</p> <p>Competition: Most vendors have limited threat detection or none at all. They rarely have alarms triggered by potential ransomware activities, nor the ability to scan backups for ransomware threats.</p>
Protect backups from malicious tampering			<p>Veeam: Protect backup data from attacks thanks to multiple security layers, like immutable storage in the cloud and on-premises, end-to-end encryption, and access security (i.e. role-based access, MFA).</p> <p>Competition: Most vendors have limited ransomware protection and, typically, they offer one air-gap option (tape, rotated drives or few MSPs), either one immutability option (typically AWS Object Lock) or none; or a single point of failure (i.e., backup files dependent on a server/db).</p>
Quickly recover from a ransomware attack			<p>Veeam: Do not pay a ransom but quickly recover ransomware-free data, thanks to Veeam Secure Restore, which verifies your data is malware free and ready to recover anywhere and in way; or on-demand isolated sandbox for further investigations.</p> <p>Competition: Vendors do not provide ransomware-free recovery as they lack the ability to scan backups for ransomware threats during restore, have limited recovery options (standard VM and OS file restores, basic app-item restores) and don't offer on-demand isolated sandbox for forensics.</p>

Legend

	Complete capability		Limited capability		Non-practical capability		No capability
--	---------------------	--	--------------------	--	--------------------------	--	---------------