Why Druva?

Druva's fully managed, 100% SaaS approach effectively removes the challenges that plague DIY backup solutions like Veeam. Everything customers need to protect and secure their data is included on day 1: Storage, compute, software, and security. With just one platform, organizations protect all workloads, and rest easy knowing the solution is fully maintained, security-hardened, up-to-date, and ready with the latest features and capabilities. Best of all, the efficiency of cloud-native SaaS delivers the lowest possible Total Cost of Ownership. Finally, a data protection solution that works for you, and not the other way around.

AI

Druva Proactive AI (Agentic)	**Veeam** Reactive AI (Tool-based)
Built-In: Prompt DruAI with queries like "show me stale data from orphaned accounts" to identify risk vectors before an attack.	**Bolted-On:** Threat Hunter and IOC scanning work retroactively, forcing you to choose where it runs, interpret results, or integrate with a SIEM.
Actionable: Ask in plain English and let DruAI fix issues automatically—for example, "Show which EC2 backup jobs failed and explain why."	**Nonexistent:** Veeam is only developing the proposed Copilot integration for Veeam Data Cloud.
Automatic: DruAI spots anomalies, connects the dots, recommends clean recovery points, and handles the recovery for you.	**Manual:** Veeam Threat Hunter and Recon Blast Radius don't have built-in AI or natural-language cyber investigations.
Self-Diagnose & Repair: DruAI spots trends and risks in your environment, suggests fixes, and can take action.	**Chatbot:** Veeam Intelligence is a Veeam documentation-trained chatbot without any context about your environment.

TCO

See your savings now

Druva	Veeam
100% SaaS solution: Druva includes everything needed for data protection at no extra cost — storage, compute, software, and security.	**Do-it-yourself challenges:** You source, build, secure, manage, and refresh 7+ Veeam products — each with its own license and infrastructure requirements.
More value for money: Key features such as backup and recovery for Entra ID and Managed Data Detection and Response services come at no extra costs for all Druva customers.	**Spend more. Get less:** With Veeam, costs are coming from everywhere. Need to protect your Microsoft Entra ID? That costs extra. Need to protect data center and cloud data? Better get ready to buy a few extra products. Want security for your cloud data? That's not even available.
Hands-off: Fully managed, maintained, and monitored by Druva. Solution is always security hardened and up-to-date with latest features.	**All hands on deck!** It is your headache to keep Veeam and all its server components secure and up-to-date in every location. With 20 critical CVEs in 2024 alone, that's a lot of overtime to keep Veeam patched and up to date.
Unified: One cloud-native solution for on-premises, cloud, edge, and SaaS. No additional deployments needed.	**Fragmented:** Separate products and deployments for backing up on-premises, cloud and SaaS workloads.
Efficient: Built-in global deduplication and storage tiering smartly reduce spend and bandwidth.	**Costly:** Extra costs for backup infrastructure like storage, compute, and even egress fees for restores!
Transparent: Predictable, pay-as-you-go pricing flexibility based on actual consumption.	**Inconsistent:** Traditional licensing, with complexities of balancing sockets, capacity, workloads, storage, and/or users.

Druva is

100% SaaS

which means

up to 40%

lower TCO

Security

Explore Druva's security capabilities

Druva	Veeam
Modern architecture: Cloud-native, segregated and fortified microservices layered on robust AWS infrastructure.	**Legacy architecture:** Outdated 3-tier architecture sits in the "line of fire" and is a popular target for hackers and malware due to the many known vulnerabilities in the Veeam software.
Secure by design: Fully secured and constantly hardened by Druva, monitored 24x7 by security experts, FedRAMP-certified.	**Secure by implementation:** It is your responsibility to know, implement, configure, and maintain security best practices. Hardening, patching, and fixing CVEs are all up to the customer.
Protected: Entire backup infrastructure — not just storage — is fully air-gapped and immutable with dual-envelope encryption. All built-in. Proactively use backup data for threat hunting across Amazon EC2 and VMware.	**Exposed:** Air-gapping the backup infrastructure is your responsibility. Providing immutability is also up to you to configure or procure separately through third-party storage.
Proactive: Managed data detection and response (MDDR) of backups with immediate, human alerting - at no extra cost!	**Manual:** Traditional event notification requires you to correlate and diagnose. Additional vendors required for monitoring services.
Resilient: Backup application is always available, with guaranteed SLAs. Three copies of data. Separated control and data planes.	**Vulnerable:** Availability is your responsibility. Veeam Backup Server is a single point of failure and needs HA/DR planning.

The Most Mature and Most Secure SaaS Platform for Data Protection

Simplicity

Switch to Druva in 4 Easy Steps

Druva	Veeam
Single UI: Across all workloads, locations, and data. Secure and consistent user access from anywhere in the world.	**Multiple UIs:** Data center, cloud, and SaaS have their own consoles, policies, development cycles, and learning curves.
Global: Unified view for endpoint, datacenter, hybrid, cloud and SaaS r data. Federated search, compliance, and legal hold.	**Limited:** With separate products needed for many different workloads and limited support for SaaS apps, it becomes increasingly complex to quickly find what data is where. . No federated search, legal hold, or eDiscovery across edge and SaaS.
Elastic: Storage and performance scale transparently as you grow — no hidden costs, no surprises.	**Static:** With Veeam, planning for future growth is your responsibility. Overprovisioning leads to wasted costs. Underprovisioning leads to negative performance and service level impacts.
Conversational AI: Dru is a true intelligent copilot to automate and accelerate support operations, as well as aid cyber investigations and incident response.	**Rudimentary AI:** Veeam's chatbox experience is limited to only 30 queries a day before it risks being overloaded.
Cloud First: Druva was built in the cloud since day 1 and provides SaaS backup capabilities for all of our supported workloads including Google Workspace, M365, Salesforce, Dynamics 365, on-premises, endpoint, and of course cloud-native workloads.	**Cloud last:** Veeam was the last vendor to introduce any native SaaS-based offering, and it is limited to only Azure and M365. For all other workloads you need to build it yourself.
Rapid time-to-value: With no servers or infrastructure to ship/deploy, customers can immediately start protecting their data. Easy onboarding, and easy to scale.	**Prolonged process:** Traditional deployment , with all the complications of do-it-yourself software and associated costs — Delaying when you can actually start your first Veeam backup.

Zero Patches.

Guaranteed Recovery.

Ransomware Protection

Learn more: On-Demand Webinar

Druva	Veeam
Advanced threat monitoring: Wide set of anomalies across workloads on-premises, in the cloud, and within your SaaS data sources such as M365. Intuitive visualization. Global SaaS telemetry continuously improves anomaly detection algorithms.	**Basic anomaly detection:** No support for ransomware detection/recovery of key workloads like M365 and cloud data. Needs additional compute resources. Limited to Veeam's core product only.
Rapid response: Security teams can immediately start incident analysis and response using backup data in the Druva cloud, even when your primary infected environment is unavailable. Guaranteed access to tamperproof files and granular, changed data logs.	**Delayed response:** The Veeam backup environment itself needs to be recovered first before any incident analysis or recovery efforts can start. Proactive planning is needed to ensure all logs are available and the Veeam backup servers themselves are resilient.
Secure rollback: Druva manages a secure cache of deleted files for up to 7 days. Recover deleted backup data with self-service rollback actions.	**No insider protection:** If a bad actor gains access to Veeam and deletes the backup data, there is no recourse.
Accelerated recovery: Built-in recovery scans automatically detect and remediate malware during recovery - all on Druva compute and with no added effort for you.	**Limited recovery:** Building the recovery workflows is your responsibility. You configure and run the malware scans and manage the remediation yourself.
Curated Recovery: Minimize data loss and accelerate recovery with a curated snapshot containing the most recent, clean files across a given timeline.	**Risk of data loss:**Veeam marks the entire backup set as clean or infected — tossing the good out with the bad. This prolongs the recovery process.

Druva Ransomware Recovery Workflow

Learn more at www.druva.com/platform