



Ransomware / Incident Response Review

Druva Team:

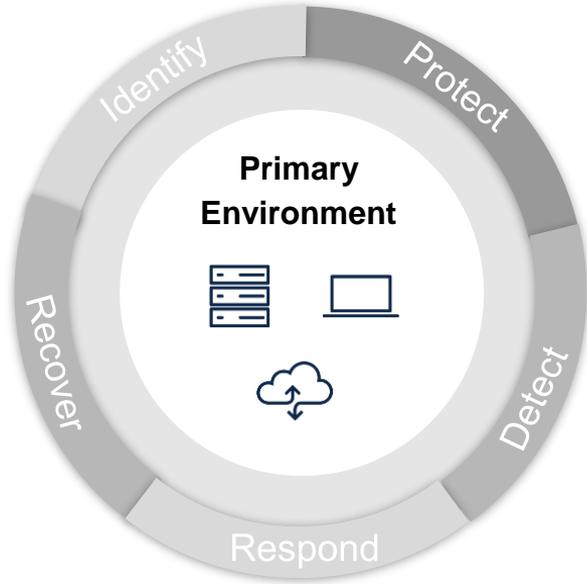
Cody Morphis – Account Executive

Jesus Fernandez – Solutions Architect

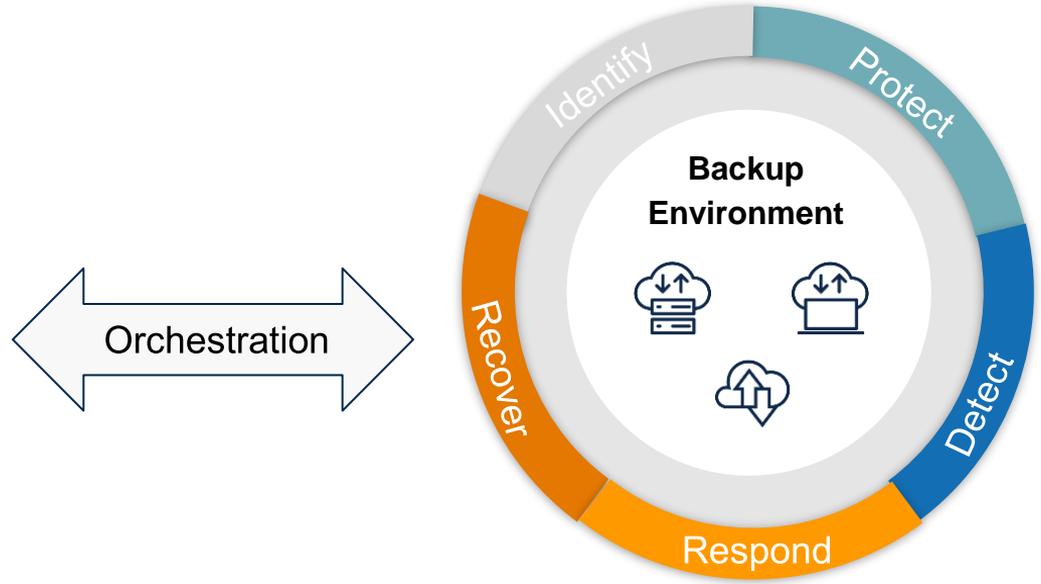
JP Bachmann – Manager, Growth

Cyber resilience for prevention and response

Primary Environment - Prevention



Backup Environment - Response



Cybersecurity vendors for Firewalls, Email Gateways, Endpoint Security (e.g. EDR)



Druva solutions including our platform security and add-on services

The background of the slide is a dark grey chain-link fence pattern. A solid blue vertical bar is on the right side, containing the main text.

Foundational ransomware protection

All workloads

Data integrity

Risk: Some backups are vulnerable to ransomware

Reason: Ransomware needs two things to execute:

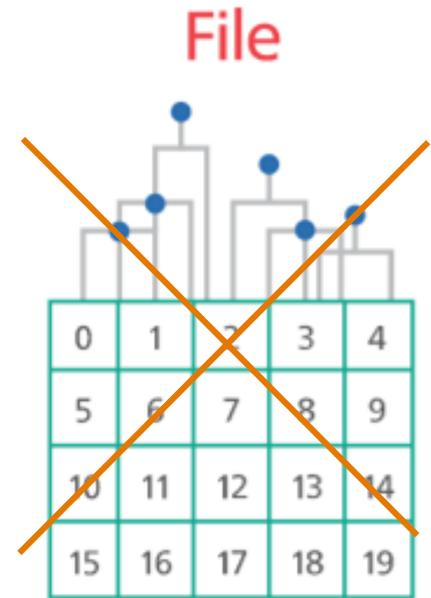
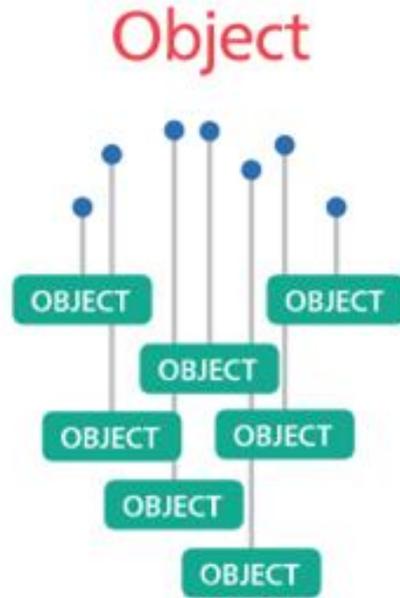
1. Persistent environment
2. File system

Many backup solutions provide both

Solution:

Druva is only connected to the network very briefly during backup, so there is no persistent environment.

We use **object-based** storage, so there is no file system.



<https://forums.veeam.com> > veeam-backup-replication-f2

Yes, Ransomware can delete your Veeam backups. - Veeam ...

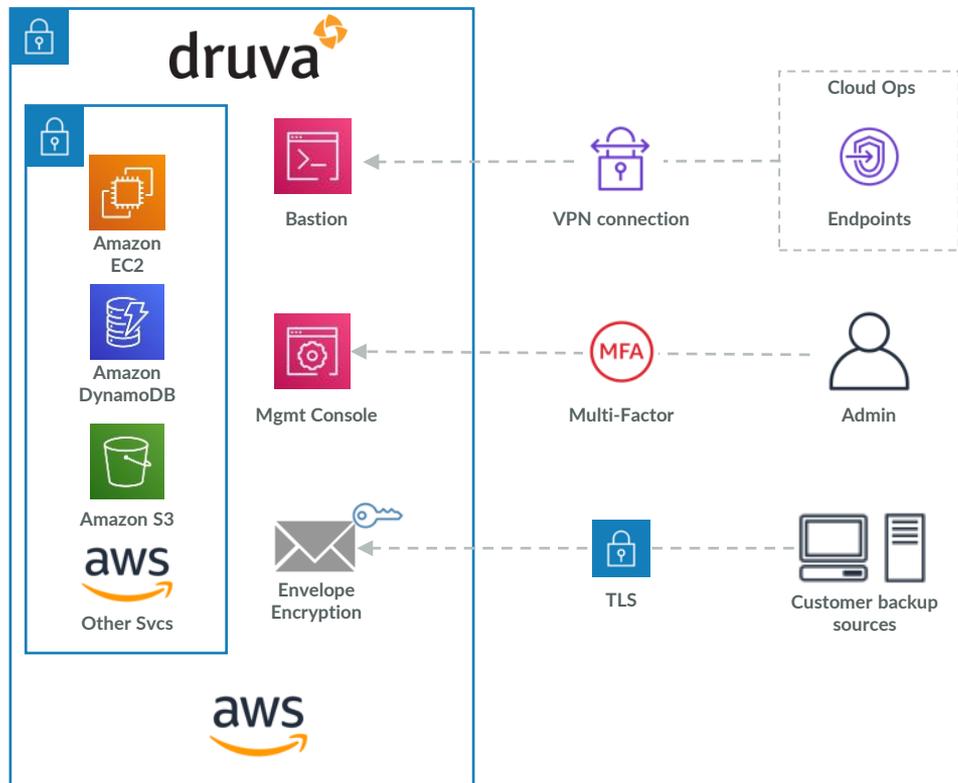
Zero trust architecture

Risk: Ransomware can use compromised credentials to access and delete backups

Reason: Same credentials used for both primary and backup environments

Solution:

Druva requires separate account access and multi-factor authentication to access the backup environment



Industry standards and certifications

(SaaS) Application Services

druva

(PaaS) Distributed Database Services
(IaaS) Infrastructure: Compute + Storage

powered by **aws**

Continuous PEN-Test(s) by 3rd Parties & customers
Coalfire, Bishop Fox, Cobalt.io
Open Vulnerability Disclosure Policy
<https://www.druva.com/disclosure-policy/>

Accelerated Ransomware Recovery

IDENTIFY



Unusual Data Activity:
Identify anomalous data sets

CONTAIN



Quarantine
Prevent Malware Spread

RECOVER



Curated Recovery
Recover Clean & Uninfected Data

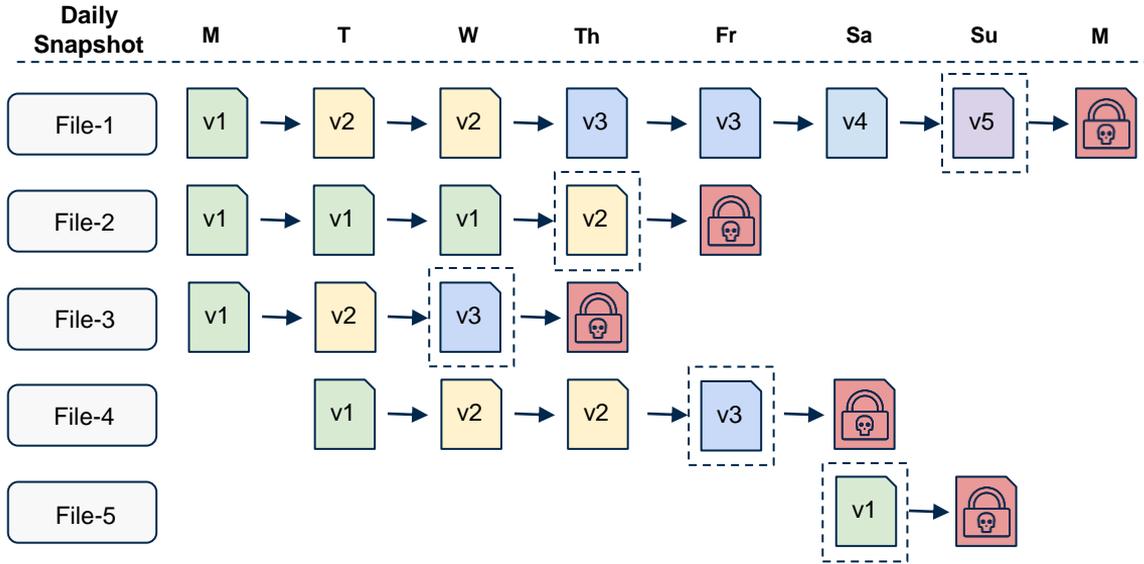
Security Posture and Observability

- Unusual Data Activity Monitoring
- Access Insights
- Deletion Rollbacks
- SIEM Integration
- Risk Dashboard (Roadmap)

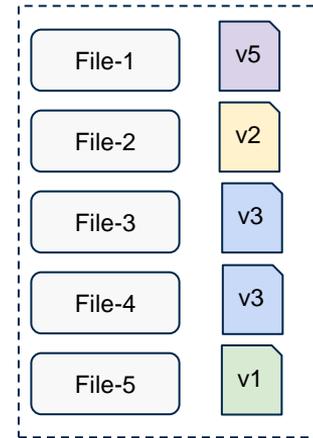
Accelerated Ransomware Recovery

- Malicious File Scan
- Quarantine
- Curated Snapshots

Curated Recovery



Curated Snapshot:
Saves time and data



Automatically finds the most recent clean version of each file and adds it to a single “golden snapshot”



Druva Receives Cyber Catalyst
Designation for Outstanding Product
Security and Ability to Combat
Ransomware

Cyber Resiliency and Ransomware Protection



Protect



Data Integrity & Availability



Operational Security

It's simple to keep your backup data safe. No hardware, software, manual updates, or complex configurations.

Prepare



Posture & Observability



Continuous Monitoring

Get a centralized view of all your security posture and data risks so you can be ready for cyber attacks.

Recover



Accelerated Recovery



Forensics

Automate the process of recovering clean and complete data sets so you can get back to normal.

API integrations with security solutions



Trust Certifications



Druva Cyber Resiliency Vs. Legacy

		druva 	Legacy
Foundational Protection	100% Cloud SaaS / DPaaS		
	Air-gapped, immutable backups		 \$\$
	Ransomware resistant architecture (data sharding)		
	Multi-Factor Authentication		
	Delayed Deletion		
Operational Security	24x7 managed SecOps		
	managed patching and upgrades (to address CVEs and other risks)		
	Vulnerability Scanning		
	Security Remediation		
	Penetration testing		
	24x7 threat monitoring and response		
	Data Sovereignty		
Posture and Observability	Access Insights		
	Anomaly Detection		
	Deletion Rollback (Up to 7 Days)		
Accelerated Ransomware Recovery	ARR for endpoints		
	Built-in AV scanning		
	Scans using customer forensic info (hashes)		
	Quarantine Workflow		
	Pre-built SOAR integrations		
	Curated Snapshot		



The Druva Data Resiliency Guarantee

Total Coverage. Zero Compromises.

- RISKS**
- ✓ **Cyber risk** (ransomware and beyond)
 - ✓ **Human risk**
 - ✓ **Application risk**
 - ✓ **Operational risk**
 - ✓ **Environmental risk**

- SLAs**
- ✓ **100% Confidentiality.** Guarantee that Customer Data will not be compromised as a result of a Security Incident.
 - ✓ **100% Immutability.** Guarantee that the last successful backup of Customer Data will be recoverable (not changed) in the event of a Ransomware Incident.
 - ✓ **99% Reliability.** Guarantee that backups will complete successfully in accordance with Customer Policies.
 - ✓ **99.999% Durability.** Guarantee that Customer Data backed up is recoverable (not corrupted).
 - ✓ **99.5% Availability.** Guaranteed uptime up to 99.5%



Thank you