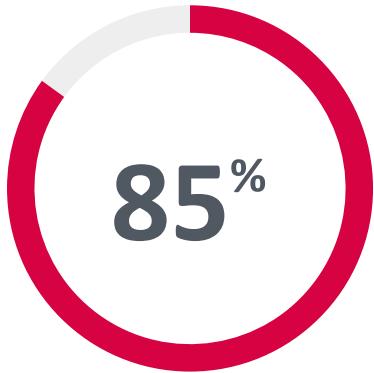


# МАКСИМАЛЬНАЯ УСТОЙЧВОСТЬ для поддержания работы вашего бизнеса

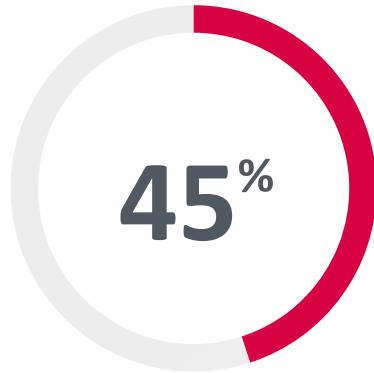


Лебедев Алексей  
Старший Системный Инженер

# Потеря данных - это, к сожалению, реальность



организаций, пострадавших от  
вирусов-шифровальщиков в  
2023\*



продуктивных данных,  
пострадавших от кибератак\*



Вирусов-шифровальщиков,  
атаковавших бэкапы\*

# ЛИДЕР РЫНКА

#1

по доле рынка Data  
Replication & Protection,  
согласно IDC

81%

списка Fortune 500

#1

в способности к  
**ИСПОЛНЕНИЮ** и **ЛИДЕР**  
согласно **Магическому  
Квадранту Гартнера**

+75

лидер рынка по  
**Net Promoter Score**

# Veeam Data Platform

Recovery Orchestration

Monitoring & Analytics

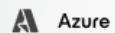
Backup & Recovery

Native APIs

Platform  
Extensions



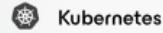
AWS



Azure



Google Cloud



Kubernetes



Cloud



Virtual



Physical



Apps



SaaS



Microsoft 365



Salesforce

On-Premises • In the Cloud • XaaS

# Veeam Data Platform

## ЧТО НОВОГО В 23H2

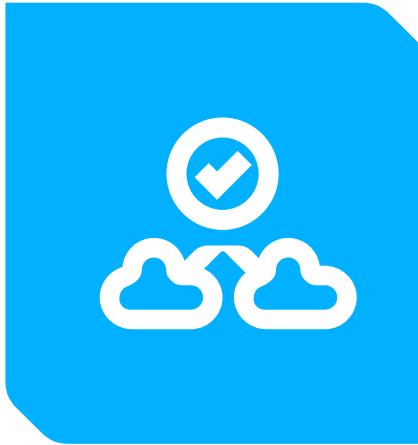
# Мы обеспечиваем непрерывную работу вашего бизнеса



Безопасность  
данных



Восстановление  
данных



Свобода  
данных



## Поиск + определение киберугроз

Минимизируйте ущерб  
от кибератаки

## Безопасность данных

Обеспечьте безопасность своих данных с помощью многоуровневой системы безопасности, которая дает вам уверенность, что ваши данные всегда защищены.

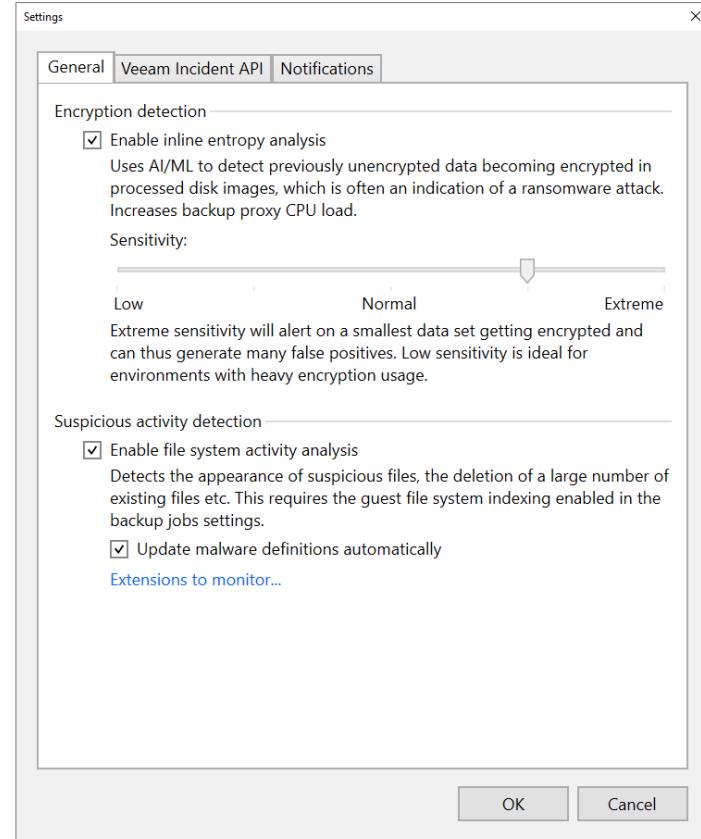
- Malware Detection
- Отправка событий на Syslog сервер
- Синхронная коммуникаций с ServiceNow
- Veeam Incident API

# Malware Detection

## AI-оперативное сканирование и анализ файловой системы

Определите заражение как можно раньше:

- Измерение и анализ изменений
- Обнаружение известных следов инфекций
- *Маркировка бэкапов как "чистый", "подозрительный" или "инфицированный"*

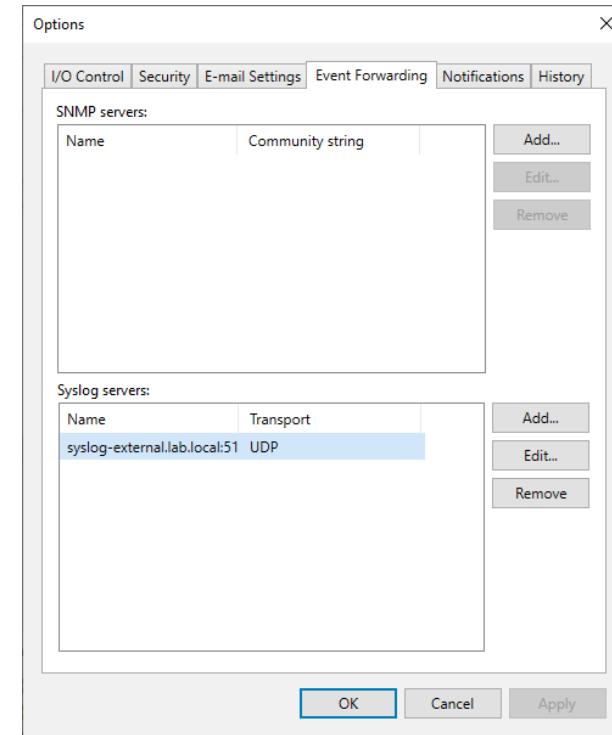


# Syslog Event Forwarding

Используйте все инструменты

Сделайте вашу защиту более заметной

- Предоставление данных инструментам SIEM для сбора и анализа.
- Упрощение конфигурации и управления
- Оптимизация и централизация мониторинга



# Интеграция с ServiceNow

## Обеспечение контроля за платформой

- Интеграция с Veeam ONE™
- Использование существующих рабочих процессов и повышение прозрачности между командами.
- Двусторонняя интеграция гарантирует актуальность обеих платформ.

The screenshot shows a list of incidents in ServiceNow. The columns are Number, Opened, and Short description. The incidents listed are:

Number	Opened	Short description
INC0010036	2023-10-31 15:04:42	Potential infrastructure malware activity
INC0010035	2023-10-31 14:04:30	Potential infrastructure malware activity
INC0010033	2023-10-31 06:49:33	Test ticket
INC0010032	2023-10-31 06:49:33	Latest snapshot age
INC0010031	2023-10-31 07:17:07	Latest snapshot age
INC0010030	2023-10-31 07:16:44	Latest snapshot age
INC0010029	2023-10-30 06:02:03	Latest snapshot age
INC0010028	2023-10-30 07:17:06	Latest snapshot age
INC0010027	2023-10-30 07:17:06	Latest snapshot age
INC0010026	2023-10-30 07:16:33	Latest snapshot age
INC0010025	2023-10-30 06:00:14	Latest snapshot age
INC0010023	2023-10-30 07:17:09	Latest snapshot age
INC0010022	2023-10-30 07:17:02	Host NIC link status
INC0010021	2023-10-30 07:17:02	Latest snapshot age
INC0010020	2023-10-30 07:17:02	Latest snapshot age
INC0010019	2023-10-30 07:17:02	Host NIC link status
INC0010018	2023-10-30 07:17:02	Latest snapshot age
INC0010017	2023-10-30 07:17:02	Latest snapshot age
INC0010016	2023-10-30 07:16:54	Host NIC link status
INC0010015	2023-10-30 07:17:09	Latest snapshot age
INC0010014	2023-10-30 07:16:54	Host NIC link status
INC0010013	2023-10-30 07:17:02	Latest snapshot age
INC0010012	2023-10-30 07:17:02	Latest snapshot age
INC0010011	2023-10-30 07:17:02	Host NIC link status
INC0010010	2023-10-30 07:16:51	Latest snapshot age
INC0010009	2023-10-30 07:16:51	Host NIC link status
INC0010008	2023-10-30 07:17:09	Guest disk space
INC0010007	2023-10-30 07:17:09	Guest disk space

The screenshot shows the details of a specific incident in ServiceNow. The incident number is INC0010036, opened on 2023-10-31 15:04:42, closed on 2023-10-31 15:34:42, with a medium urgency and new state. The short description is "Potential infrastructure malware activity".

Activities section:

- System Administrator: Summary: Veeam Backup & Replication strengthens the security of the backup system using advanced tools like inline real-time scans. It also provides an API that other services can use to check and mark VMs for quarantine.
- System Administrator: Summary: Veeam Backup & Replication strengthens the security of the backup system using advanced tools like inline real-time scans. It also provides an API that other services can use to check and mark VMs for quarantine.
- System Administrator: Summary: Veeam Backup & Replication strengthens the security of the backup system using advanced tools like inline real-time scans. It also provides an API that other services can use to check and mark VMs for quarantine.
- System Administrator: Summary: Veeam Backup & Replication strengthens the security of the backup system using advanced tools like inline real-time scans. It also provides an API that other services can use to check and mark VMs for quarantine.
- System Administrator: Summary: Veeam Backup & Replication strengthens the security of the backup system using advanced tools like inline real-time scans. It also provides an API that other services can use to check and mark VMs for quarantine.
- System Administrator: Summary: Veeam Backup & Replication strengthens the security of the backup system using advanced tools like inline real-time scans. It also provides an API that other services can use to check and mark VMs for quarantine.

Additional comments (Customer visible): Additional comments (Customer visible):

Related Links:

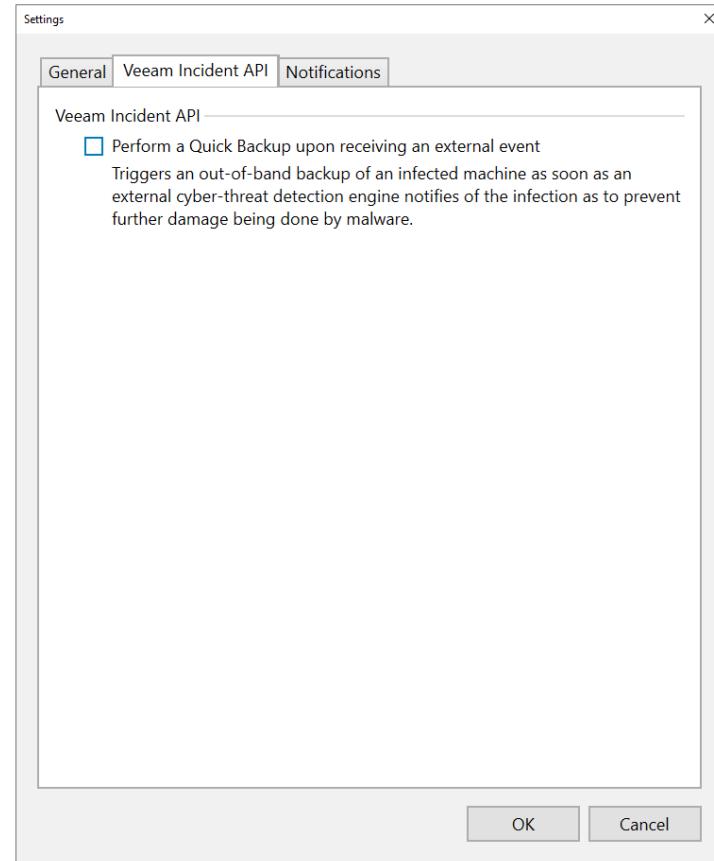
- Update
- Resolve
- Delete

# Veeam Incident API

## Получите второе мнение

Получайте отчеты о заражениях в режиме реального времени от сторонних инструментов.

- Интеграция с инструментами EDR/XDR
- Исключение барьеров между командами бэкапа и безопасности
- Минимизируйте ущерб, выполнив немедленный бэкап при оповещении





Ответ +  
восстановление  
после программы-  
вымогателя

Предоставьте своей  
команде возможность  
сократить время  
реагирования на  
инциденты

## Надежное восстановление данных

- Избегите повторного инфицирования
- Сканируйте контент с помощью YARA
- Восстановитесь на «чистую» точку с первого раза

# Избегите повторного инфицирования

Вскройте угрозу ещё до восстановления

## Автоматическое обнаружение вредоносных программ в оффлайн режиме

- Автоматическое сканирование по расписанию в новом режиме SureBackup®
- Произвольный выбор объектов
- Использование возможностей как Антивирусного ПО, так и YARA

New SureBackup Job

Settings  
Choose recovery verification job settings.

Name

Linked Jobs

Content analysis

Scan backup content with an antivirus software

Scan backup content with the following YARA rule:  
MALW\_Mirai.yar  
YARA rules location: C:\Program Files\Veeam\Backup and Replication\Backup\YaraRules\

Scan options:

Continue scanning remaining files after the first occurrence

Backup integrity

Perform backup integrity check (read and verify each block against a checksum)

New SureBackup Job

Name  
Type in a name and description for this SureBackup job.

Name

Linked Jobs

Description:  
Scan for threats  
Automated threat scanning

Backup verification mode:

Full recoverability testing (recommended)  
Runs machines in an isolated environment directly from backup and performs tests against live applications. This ensures recoverability of your production workloads in a DR event.

Backup verification and content scan only  
Performs backup integrity check and its content analysis to detect traces of malware or any other unwanted or sensitive data. These tests do not require setting up a virtual lab.

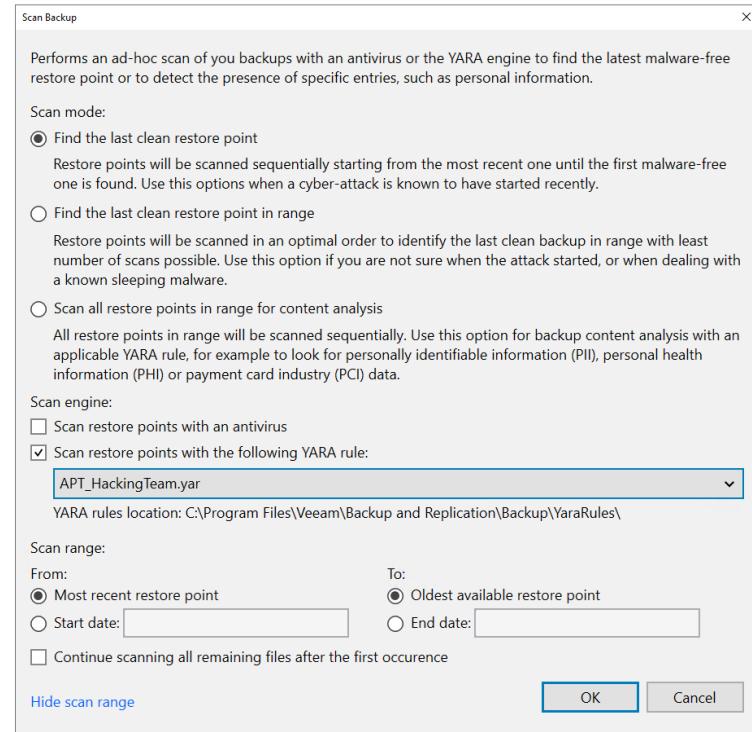
< Previous Next > Finish Cancel

# YARA анализ

Какие потенциальные риски скрываются в ваших бэкапах?

Выявите штаммы программ –  
вымогателей в вашей среде

- Комплексное обнаружение на основе сигнатур
- Определение нарушений политик

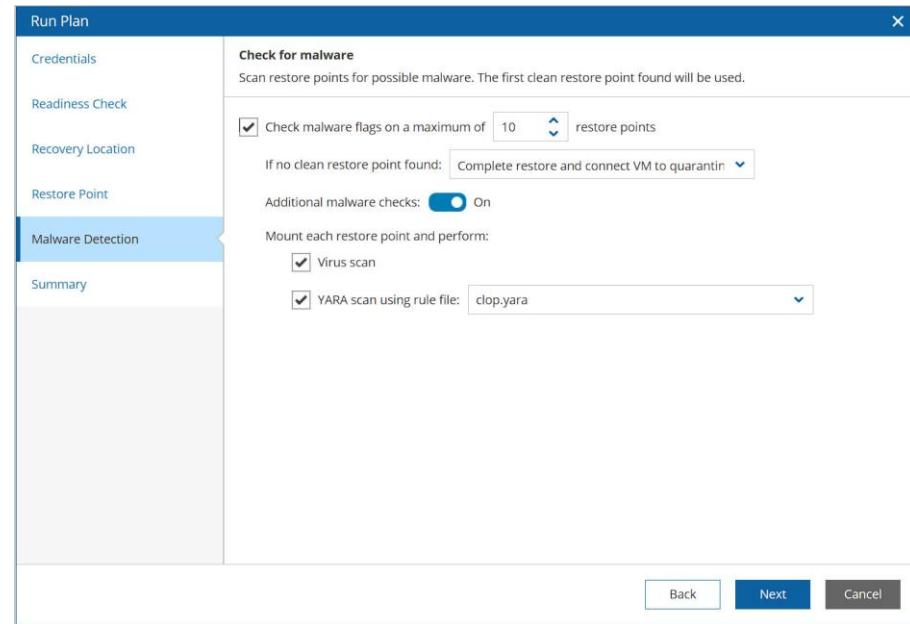


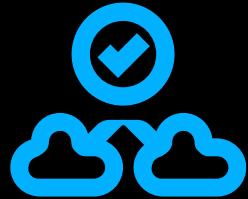
# Восстановление на «чистую» точку

## Автоматический поиск неинфицированного бэкапа

### Уверенность в случае аварии

- Ускорьте восстановление за счёт обхода зараженных точек восстановления
- Гибкое восстановление на землю или в облако с последующей кастомизацией
- Автоматизированное тестирование и отчётность для аудита





## Надёжная + соответствующая требованиям защита

Укрепите вашу  
позицию в области  
безопасности и  
соответствия  
стандартам

## Свобода данных

Поддержка гибридных и мультиоблачных инфраструктур, которые помогают защитить все ваши данные без запирания данных у вендора. Ваши данные должны быть защищены там, где они вам нужны — в облаке, локально или на периферии.

- Анализ соответствия стандартам
- “Four-eyes” авторизация
- Veeam Threat Center

# Security and compliance analyzer

## Следуйте лучшим практикам

- Выявите риски инфраструктуры резервного копирования
- Выполнайте проверки по расписанию
- Следуйте лучшим практикам по защите вашей инфраструктуры

Security & Compliance Analyzer	
The following best practices are guidelines from data protection and cyber-security experts. Not following them exposes your backup infrastructure to significant risks and reduces chances of successful recovery following a cyber attack, a natural disaster or a hardware malfunction.	
Best Practice	Status
Backup infrastructure security	
Remote Desktop Service (TermService) should be disabled	Passed
Remote Registry service (RemoteRegistry) should be disabled	Passed
Windows Remote Management (WinRM) service should be disabled	Passed
Windows Firewall should be enabled	Passed
WDigest credentials caching should be disabled	Passed
Web Proxy Auto-Discovery service (WinHttpAutoProxySvc) should be disabled	Passed
Windows Script Host should be disabled	Passed
SMBv1 protocol should be disabled	Passed
Link-Local Multicast Name Resolution (LLMNR) should be disabled	Passed
Product configuration	
MFA for the backup console should be enabled	Passed
Immutable or offline (air gapped) media should be used	Passed
Password loss protection should be enabled	Passed
Backup server should not be a part of the production domain	⚠️ Unable to detect
Email notifications should be enabled	Passed
All backups should have at least one copy (the 3-2-1 backup rule)	Passed
Reverse incremental backup mode is deprecated and should be avoided	Passed
Unknown Linux servers should not be trusted automatically	Passed
The configuration backup must not be stored on the backup server	Passed
Host to proxy traffic encryption should be enabled for the Network transport mode	Passed
Hardened repositories should not be hosted in virtual machines	Passed
Network traffic encryption should be enabled in the backup network	Passed
Linux servers should have password-based authentication disabled	Passed
Backup services should be running under the LocalSystem account	Passed
Configuration backup should be enabled and use encryption	Passed
Credentials and encryption passwords should be rotated at least annually	Passed
Hardened repositories should have the SSH Server disabled	Passed
S3 Object Lock in the Governance mode doesn't provide true immutability	Passed
Backup jobs to cloud repositories should use encryption	Passed

# “Four-eyes” авторизация

## Избегите случайных удалений

- Активируйте подтверждение второго администратора
- Установите запрет на удаление резервных копий и их хранилищ
- Действия логируются в истории, журнале Windows и по email

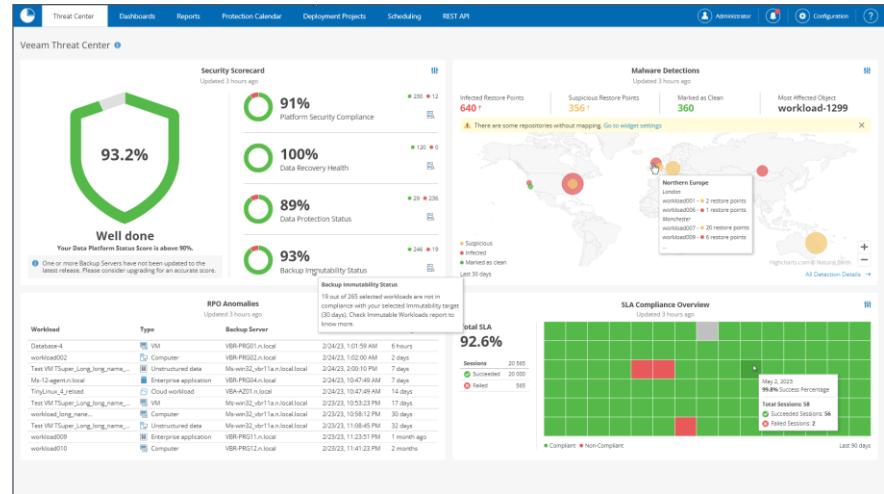
The screenshot shows the Veeam Backup and Replication interface. At the top, there's a configuration dialog titled "Users & Roles" with tabs for "Security" and "Authorization". Under "Four-eyes authorization", a checkbox is checked for "Require additional approval for sensitive operations", with a detailed description below it. A setting for "Automatically reject pending approvals after: 7 days" is also shown. Below this, a confirmation dialog from "Veeam Backup and Replication" asks if the user wants to proceed with a pending backup deletion request, providing "Yes" and "No" buttons. At the bottom, the main interface shows a table of "Pending approvals" with two entries:

Event ↑	Initiated by	Initiated at	Expires at
Delete backup NAS...	LAB\hannes	9/20/2023 10:31:59 AM	9/27/2023 10:31:59 AM
Delete repository S...	LAB\hannes	9/20/2023 10:33:50 AM	9/27/2023 10:33:50 AM

# Veeam Threat Center

## Направьте внимание на защиту

- Комплексная оценка степени защиты
- Глобальная карта обнаруженных угроз
- Определение RPO аномалий



# Veeam Data Platform Packages

Platform Editions	Backup and Recovery	Monitoring and Analytics	Recovery Orchestration	Ransomware Warranty (add-on)
Premium	●	●	●	●
Advanced	●	●		
Foundation	●			
Supporting product components	Veeam Backup & Replication*		Veeam ONE	Veeam Recovery Orchestrator

## Also Available:

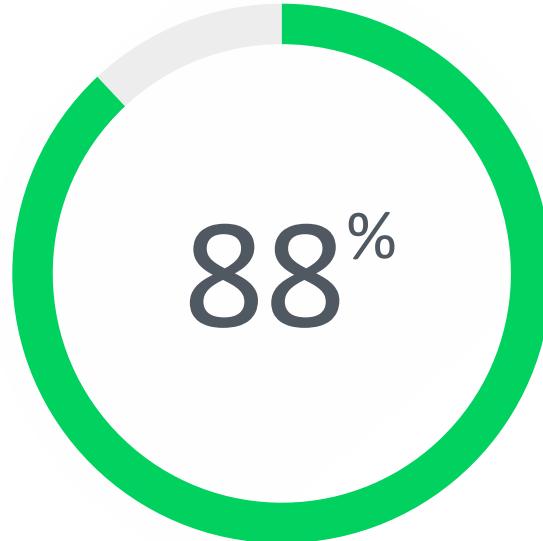
- Veeam Data Platform Essentials for Small Business

\* Certain advanced features are only available in Advanced or Premium editions

● Full Featured

● Some capabilities may be limited

# Курс на BaaS – Backup as a Service



организаций с большой  
вероятностью будут  
использовать BaaS/DRaaS в  
течение следующих двух лет

Представляем

# Veeam Data Cloud



Представляем

# Veeam Data Cloud

## Veeam Data Platform

Самостоятельно управляемая  
защита данных для гибридных  
и мультиоблачных данных.

- Cloud      ■ Apps
- Virtual     ■ SaaS
- Physical

## Veeam Data Cloud

Полностью управляемые  
облачные сервисы резервного  
копирования для XaaS и данных в  
мультиоблачной среде.



Microsoft 365



Azure

Максимальная  
устойчивость

Фундаментальный AI

# Ключевые особенности

Представляем

## Veeam Data Cloud

- Безлимитное хранилище на Veeam-аккаунте для Microsoft 365
- Гибкий RPO
- Прозрачная exit-policy. Ваши резервные копии останутся у вас

# Посмотрите

## на Veeam Data Cloud в действии!



**Dashboard**

**Backup Status**

- Last Backup
- Status
- Restore Points

Storage Use (GB)

**Users**

- Protected Accounts
- Total Accounts
- Unprotected Accounts

Proportion of protected accounts

**Retention**

- Target
- Current
- Oldest Retention Point

Progress towards target retention

**M365 Licence Activity**

200 Active 10 Inactive

**Licences**

- Active Licences
- Inactive Licences
- Unprotected Users

Manage Licences

**Storage Use**

3213.21GB

Highest Storage Users

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

**Dashboard**

**Session Status**

Status	Count
Failed	1
Warning	0
Success	11
Running now	0

**Protected Workloads**

Workload Type	Count	Status
Virtual Machines	4 of 9	44%
Azure SQL Server Instances	2 of 2	✓
Azure Files	2 of 2	✓

**Session Logs**

Type	Status	Start Time	End Time	Source	Created By	Actions
File Level Restore	Success	20/03/2023 8:17:45 PM	20/03/2023 10:57:45 PM	Azure		<a href="#">Edit</a>
File Level Restore	Success	20/03/2023 8:17:45 PM	20/03/2023 10:57:45 PM	Azure		<a href="#">Edit</a>
File Share File Restore	Success	20/03/2023 8:17:45 PM	20/03/2023 10:57:45 PM	Azure		<a href="#">Edit</a>
File Level Restore	Success	20/03/2023 8:17:45 PM	20/03/2023 10:57:45 PM	Azure		<a href="#">Edit</a>
File Level Restore	Success	20/03/2023 8:17:45 PM	20/03/2023 10:57:45 PM	Azure		<a href="#">Edit</a>

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

# Veeam Data Cloud for Microsoft 365 : NEW Backup Service Deep Dive

 Thursday, March 21 | EMEA - 12 p.m. CET

Don't miss this webinar if you want to optimize or start executing on your Microsoft 365 backup strategy and experience the simplicity of a SaaS solution, enabling you to create your first backup in less than five minutes. In this webinar:

- See a demo of Veeam Data Cloud's modern and intuitive UI in action
- Understand how you can reap the benefits of an all-in-one backup service
- Learn more details on how you can get started right away!



REGISTER NOW



Follow us!



Join the community hub:

