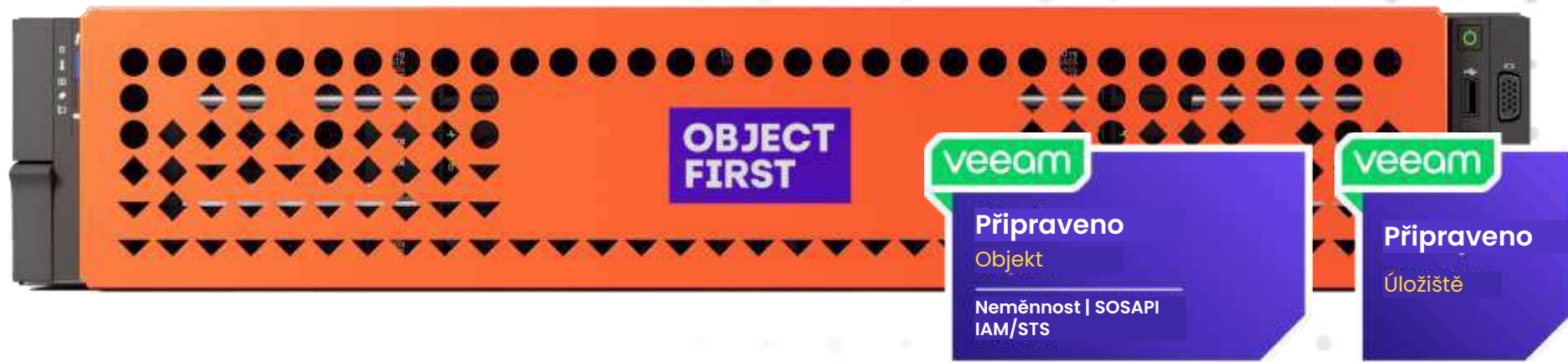


Odolnost vůči ransomwaru



Miroslav Hlúbik

Object First, Territory Sales Manager
miroslav.hlubik@objectfirst.com



Martin Beran

Veeam Software, System Engineer Advisory
martin.beran@veeam.com

NIS2

veeam

ARE YOU READY? OVERVIEW WHO'S AFFECTED? SOLUTIONS WHITEPAPER

NIS2 is Coming: Everything You Need to Know and More!

Understand what the cybersecurity directive means to your business, and how Veeam can help with NIS2 compliance... time is ticking

OVERVIEW WHO IS AFFECTED?

Are You Ready for NIS2?

Veeam NIS2 dotazník – jste připraveni?

NIS2 Compliance Checklist



Discovered that you need to comply with the NIS2 directive? Knowing what steps to take to be compliant is not an overnight fix. We've created this handy checklist, so you can work out a plan of action. The penalties for non-compliance can be severe, make sure you know what is at stake that you, as an individual and your organization could face. Here, we focus on articles 21 and 23 which outline the requirements needed to comply. Visit our website to understand more about NIS2 and how your business could be affected.

NIS2 Article	Ask yourself... and tick when you can confidently answer	How the Veeam Data Platform can help
21-2(a): policies on risk analysis and information system security;	<ul style="list-style-type: none"><input type="radio"/> Do I know what risks I have in my current environment?<input type="radio"/> Do I have insights in internal and external factors?<input type="radio"/> Can I recover within agreed Recovery Time Objective when disaster strikes?	<ul style="list-style-type: none">Foundation: Built-in security and compliance checkAdvanced: Anomaly and trend reportsPremium: Daily readiness reports
21-2(c): business continuity, such as backup management and disaster recovery, and crisis management;	<ul style="list-style-type: none"><input type="radio"/> Do I have backups of all important systems?<input type="radio"/> I moved workloads to the cloud, are they safe?<input type="radio"/> Can I recover quickly from outages without spare resources?<input type="radio"/> Do we have a cybersecurity hygiene policy?	<ul style="list-style-type: none">Foundation: Tags ensure that new workloads are backed-upAdvanced: Full overview of your workloads, anytime, anywherePremium: Recover to Azure as your spare DC
21-2(ii): human resources security, access control policies and asset management;	<ul style="list-style-type: none"><input type="radio"/> Can I keep out non-authorized users?<input type="radio"/> Am I still relying on insecure passwords?<input type="radio"/> Can a rogue administrator impact my recovery options?<input type="radio"/> Have I educated all staff about safely handling data?	<ul style="list-style-type: none">Multi-Factor Authentication and role-based access controlSupport for external Key Management systemsImmutable on-prem and cloud repositories
23-4(a) and (b): Report to CSIRT (...) without undue delay and in any event within 24(a)/72(b) hours of becoming aware of the significant incident,	<ul style="list-style-type: none"><input type="radio"/> How do I know which systems are impacted?<input type="radio"/> How do we handle vulnerabilities and disclosure?<input type="radio"/> How do I report to my Computer Security Incident Response Team (CSIRT)?<input type="radio"/> Can I meet the report deadlines when my systems are down?	<ul style="list-style-type: none">Built-in Malware and YARA rule scanning to identify impacted systemsPreconfigured reports ready to submit to CSIRTBest practices to ensure Veeam report availability

Fill the gaps in your cybersecurity with Veeam

Not in the EU and think you're exempt? Sad news, you're not... NIS2 impacts supply chains and is far reaching. Talk to us today and see how we can help start your journey to compliance now.

LET'S TALK

NIS2 a zálohovací řešení

Duty of Care

Organizace jsou povinny zavést robustní opatření pro řízení rizik a kontinuitu podnikání, aby minimalizovaly kybernetická rizika a dopady. To zahrnuje řízení incidentů, zabezpečení dodavatelského řetězce, zlepšování bezpečnosti sítě a řízení přístupu, šifrování, obnovu systému, nouzové postupy a zřízení týmu pro krizovou reakci.



Data Management and Hygiene

Data tagging & Data locality
Immutable backups
3-2-1-1-0

Security Measures

Zero Trust Frameworks
Cryptography & Encryption
Multi-Factor Authentication
SIEM Integration

Duty to Report

Nezbytné subjekty jsou povinny zavést procesy pro rychlé hlášení významných bezpečnostních incidentů s konkrétními termíny oznámení, například 24hodinovým systémem včasného varování. NIS2 také výrazně klade důraz na firemní odpovědnost, což vyžaduje, aby vedení bylo aktivně zapojeno a znalé kybernetických opatření organizace.



Threat Detection

Threat detection capabilities
Monitoring & Alerts
Malware detection

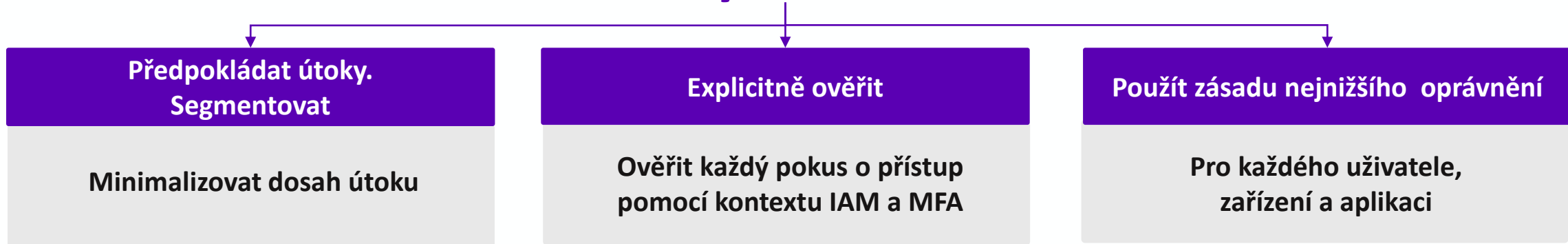
Backup Strategy

3-2-1-1-0
Cryptography & Encryption
Backup validation

Response & Recovery

Incident and Disaster Recovery processes in place
Plan & test for recovery environment and access

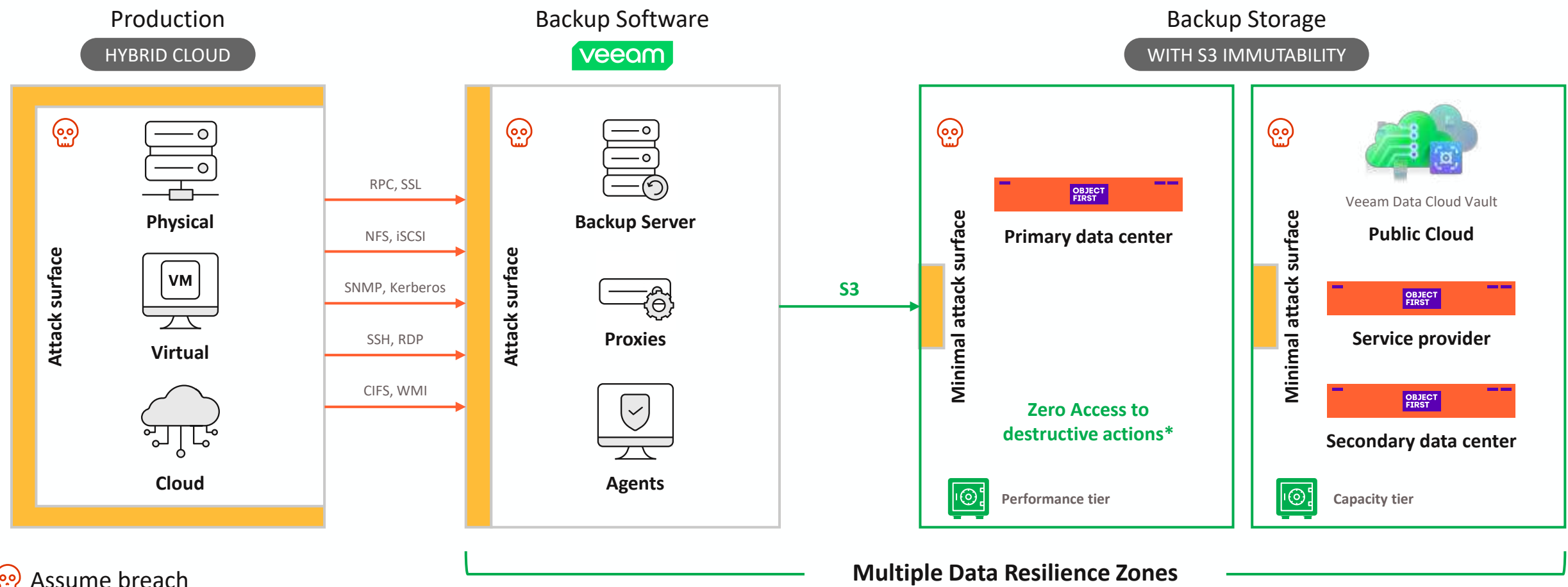
Zásady Zero Trust



Zásady Zero Trust Data Resilience (ZTDR)




Zero Trust Data Resilience (ZTDR) architecture




* Zero Access to destructive actions against the firmware, OS, storage application, or backup data.

Zálohovací úložiště s absolutní immutabilitou


Absolute Immutability 

Bezpečné 

- Zero Trust architektura a S3 objektové úložiště
- Nulový přístup k destruktivním akcím
- Okamžitá neměnnost
- Ověřeno a testováno třetí stranou

Jednoduché 

- Dle Veeam best practices
- 15 min. pro nasazení
- Automatické updaty a optimalizace od Object First

Výkonné 

- Rychlost zápisu až do 8 GB/s
- Supercharged Instant Recovery
- Lineární škálovatelnost kapacity a výkonu, automatický load balancing

Ransomware-proof 

Ověřitelně bezpečné

„Ootbi je navrženo tak, aby chránilo před jakýmikoli útoky na data nebo malwarem: **i když jsou útočníkovi známa všechny důvěrné informace, včetně přihlašovacích údajů správce, útočník nedokáže změnit data uložená v zařízení Ootbi.**“

NCC Group

Posouzení bezpečnosti produktu Ootbi



Formát a kapacita pro každé použití

Kombinujte, přizpůsobujte a škálujte v rámci každého formátu – až 1,7 PB na cluster, celkem 7 PB¹

Pro ROBO, SMB a Edge

8 TB

16 TB

24 TB



Pro datová centra

18 TB

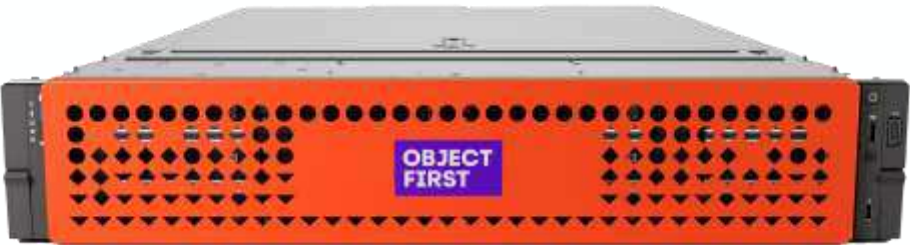
144 TB

36 TB

216 TB

72 TB

432 TB

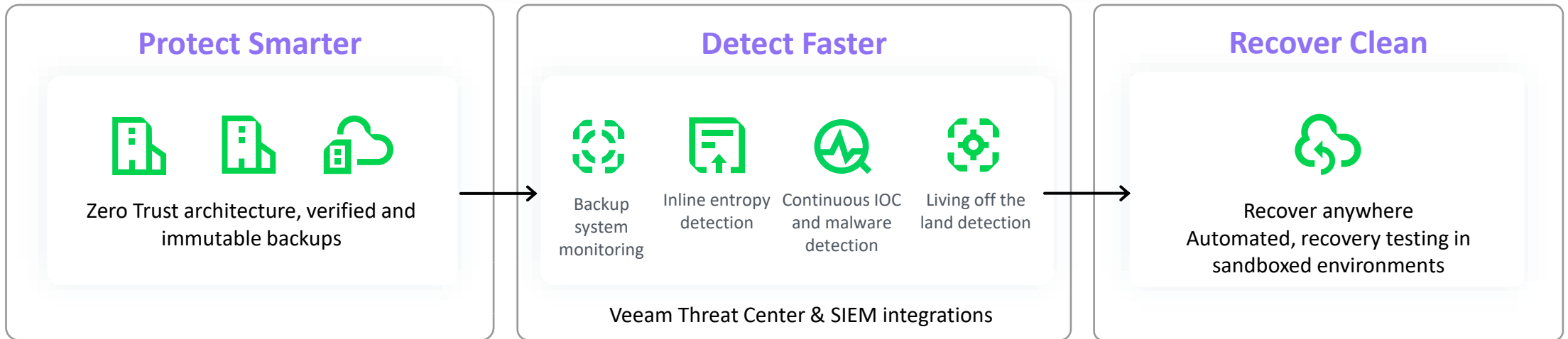


* Kapacita 17 PB v Konfiguraci škálovatelného úložiště záloh (SOBR) Veeam

Veeam Complete Data Resilience



Veeam Intelligence



Veeam Cyber Secure and Coveware Cyber Extortion Readiness & Response

Veeam Data Platform

Secure Backup & Fast Recovery · Proactive Observability & AI · Clean Orchestration & Compliance



Cloud

- AWS
- Azure
- Google Cloud
- IBM Cloud
- Microsoft Entra ID



Virtual

- VMware vSphere
- Microsoft Hyper-V
- Nutanix AHV
- Red Hat Virtualization
- Oracle Linux VM
- Proxmox VE
- Scale HyperCore
- HPE Morpheus VM Essentials



Physical

- Windows
- Linux
- macOS
- AIX
- Solaris



Apps

- Microsoft
- Oracle
- SAP HANA
- PostgreSQL
- IBM DB2
- MySQL
- MongoDB



Unstructured Data

- NAS
- File Share
- Object Storage



Veeam Data Cloud Vault

Secure, Immutable Cloud Storage

Další užitečné zdroje

[Veeam Backup & Replication Security Best Practice Guide](#)

[Veeam Security Knowledge Base Article List](#)

[Ransomware Trends and Proactive Strategies Report 2025](#)

[Veeam Cyber Secure Program](#)

[Veeam University Free](#)

[Veeam University Pro](#)

[Veeam Hands-On Labs](#)



Martin Beran

Veeam Software, System Engineer Advisory
martin.beran@veeam.com



Miroslav Hlúbik

Object First, Territory Sales Manager
miroslav.hlubik@objectfirst.com



Follow us!



Join the community hub:

