Anatomy of a Ransomware Attack

1. Attacker sends a phishing email

2. User receives a link and clicks

3. Malware unpacks and executes

4. Attacker gains control of the public key' required to encrypt files

8. Files are decrypted*

7. When ransom is paid, attacker may deliver 'the private (decryption) key'

6. Attacker demands ransom from user (e.g. Bitcoin)

5. Files get encrypted and user gets ransomware screen

***Note:** There is no guarantee that the attacker will follow through with decryption even if ransom paid.
UNODC does NOT recommend paying a ransom and recommends preventive measures to reduce the risk of compromise.

The perfect storm of data explosion, complexity, and threats:

No one is safe

72.7%

Of organizations fell prey to Ransomware in 2023

Cost across the globe

$40 Billion

Projected costs due to ransomware

Recovery is more expensive

50%
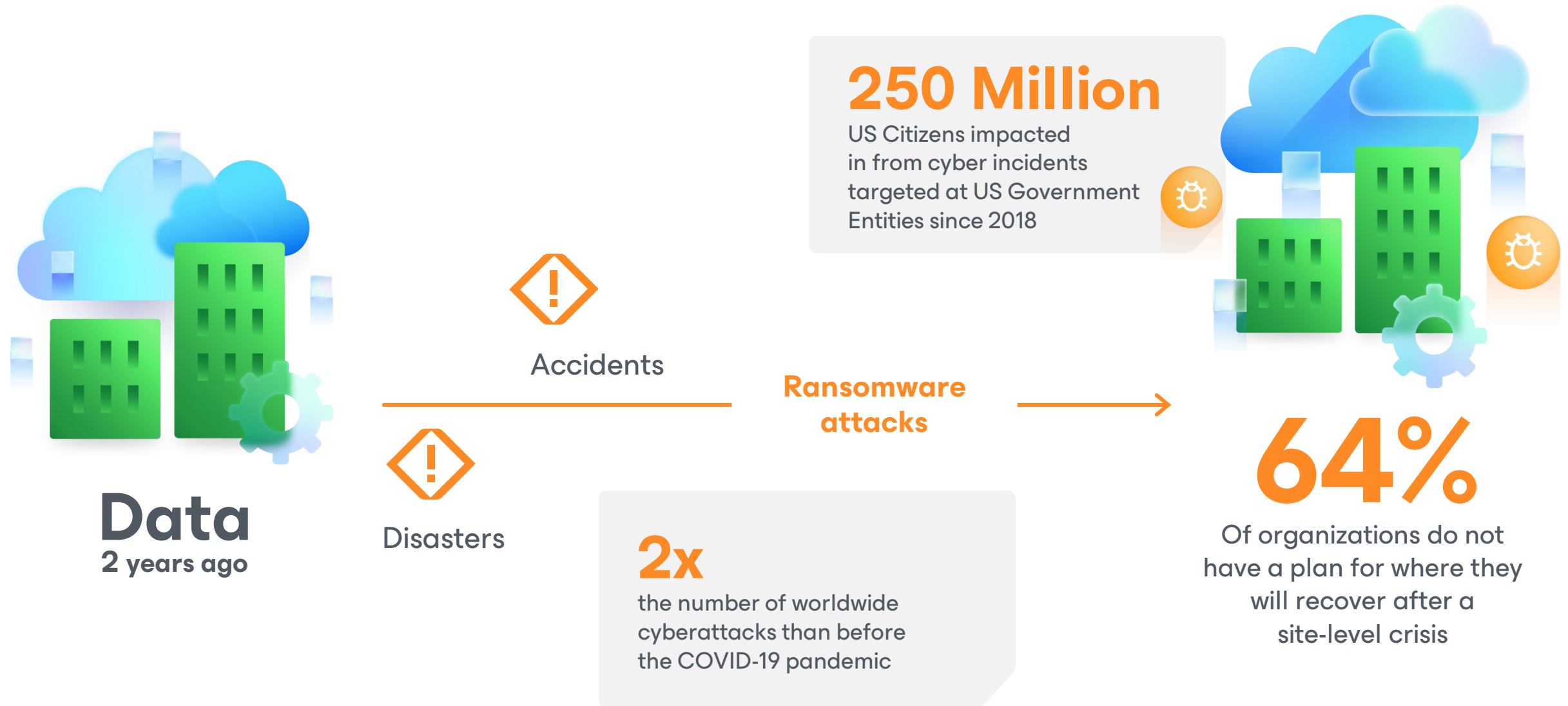
Increase in avg cost of recovery vs 2023

Surge in Ransomware Complexity

1 in 4

27% of organizations paid the ransom and never got their data back

veeam

Data is under constant threat

250 Million
US Citizens impacted in from cyber incidents targeted at US Government Entities since 2018

Accidents

Disasters

Ransomware attacks

2x
the number of worldwide cyberattacks than before the COVID-19 pandemic

Data
2 years ago

64%
Of organizations do not have a plan for where they will recover after a site-level crisis

veeam

The Threat of Cyberattacks to Local Government

Nearly **7 of 10 Govt agencies** reported cyber security incidents

A stunning **98 percent** of attacks against state and local governments led to data encryption, and **99** percent involved attempts to compromise backups.

51% of State and Local Gov backup compromise attempts were successful
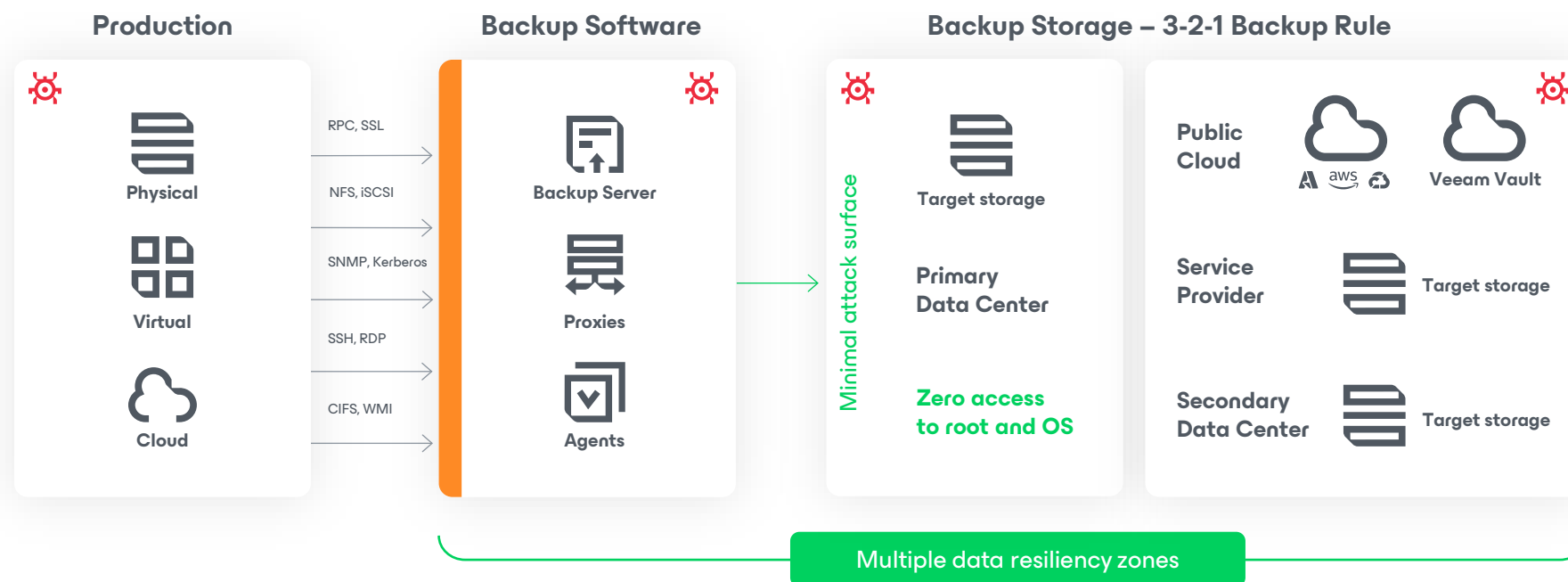
State and Local Governments end up paying on avg **104%** of the ransom demanded

43%

of data **won't** be recoverable post-Ransomware attack

veeam

Hardware-agnostic security with Zero Trust Data Resilience
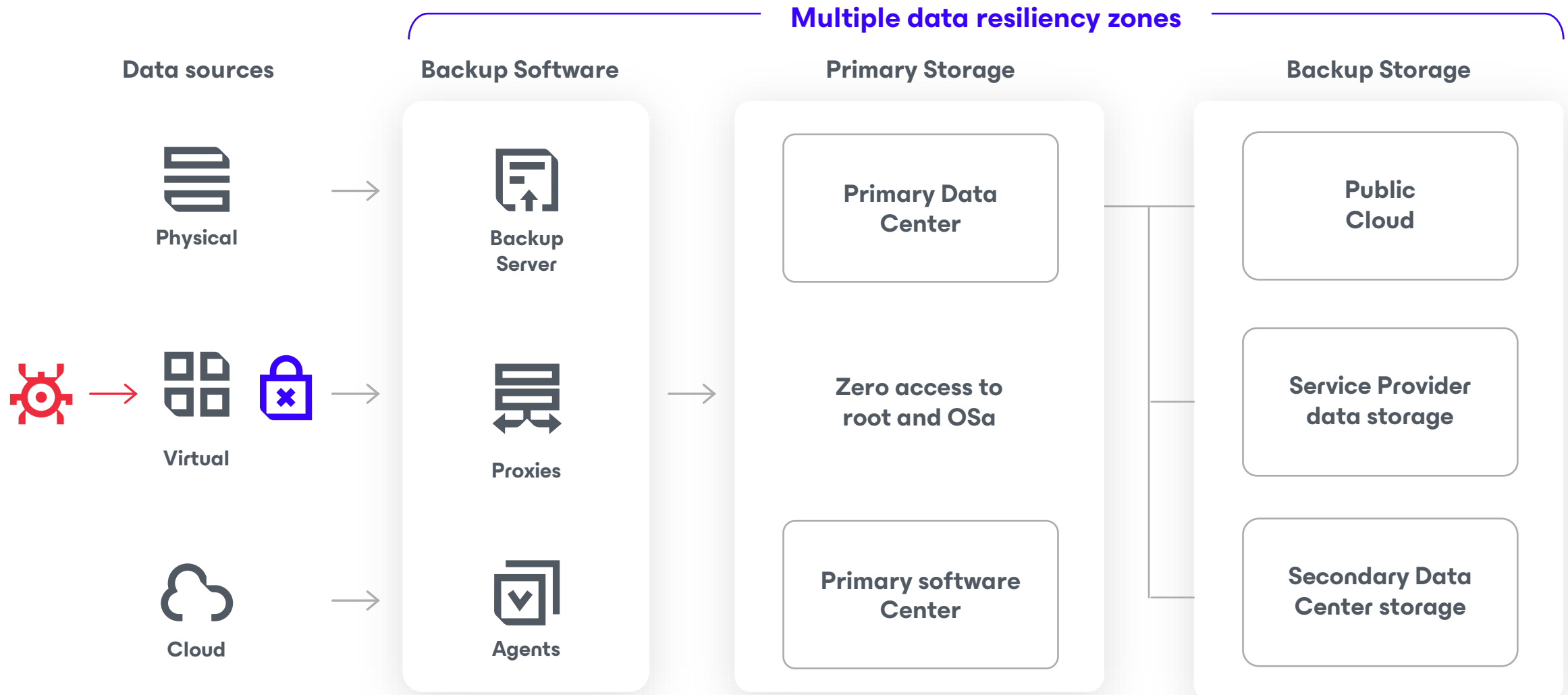
Secure by design with Zero Trust Architecture

Production

- Physical
- Virtual
- Cloud

RPC, SSL
NFS, iSCSI
SNMP, Kerberos
SSH, RDP
CIFS, WMI

Backup Software

- Backup Server
- Proxies
- Agents

Backup Storage – 3-2-1 Backup Rule

Minimal attack surface

Target storage

Primary Data Center

Zero access to root and OS

Public Cloud — AWS — Veeam Vault

Service Provider — Target storage

Secondary Data Center — Target storage

Multiple data resiliency zones

Segmentation of software & storage

Multiple **data resilience zones**

Immutable backup storage

veeam

Hardware-agnostic security with Zero Trust Data Resilience

Multiple data resiliency zones

Data sources

Backup Software

Primary Storage

Backup Storage

Physical

Virtual

Cloud

Backup Server

Proxies

Agents

Primary Data Center

Zero access to root and OSa

Primary software Center

Public Cloud

Service Provider data storage

Secondary Data Center storage

veeam

The Platform that brings data resilience to life

Proactive Threat Assessment | Forensic Triage | Incident Response

Ransomware Patterns & Signals

Data Backup	Data Recovery	Data Security	Data Portability

Data Intelligence

Native APIs

Cloud   Virtual   Physical   Apps   Unstructured data   SaaS   Containers

Cloud Vault

Secure cloud data management

Secure by design with Zero Trust Architecture

veeam
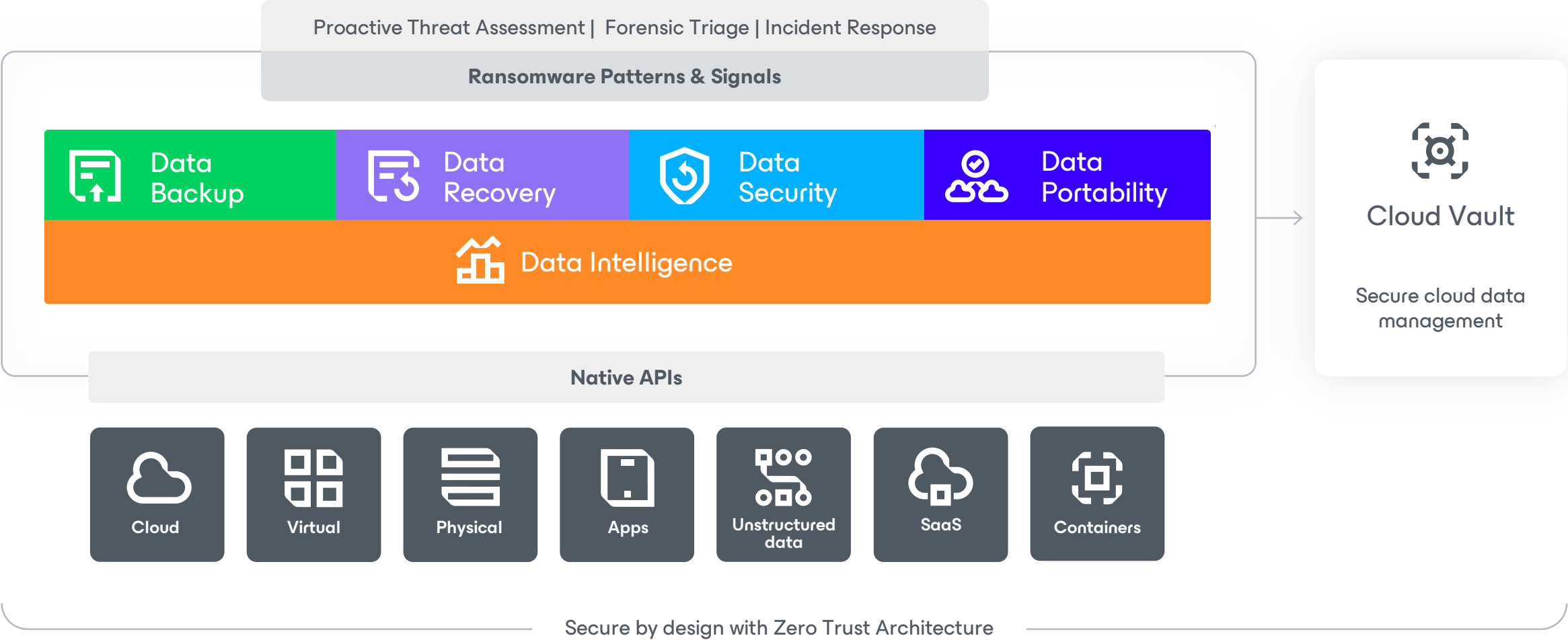
Data Backup

Broad coverage with **platform-native backup**

Optimized RPOs and RTOs with **4-in-1 protection**

Automated recoverability testing **with SureBackup**
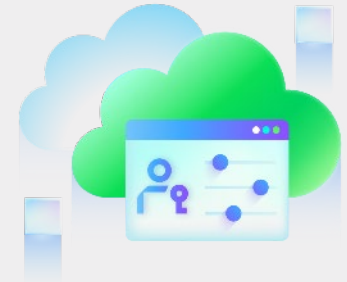
Unified backup management at **enterprise scale**

Simplifies backup and increases recovery speed by 99%, **saving 40 hours** each month

> Veeam enabled us to recapture 40 hours of productivity every month, allowing us to pivot on our strategic roadmap of modernization projects, including hardware refreshes.

City of Rancho Cucamonga

Over **5000 local Govt Agencies** work with Veeam

Data Recovery

Reduced downtime with **Instant Recovery**

Granular **search and recovery** across platforms
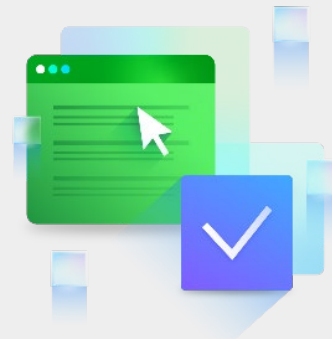
Advanced disaster recovery planning and orchestration

Clean, verified recovery at scale with **Secure Restore**

"It's a great feeling being able to tell city commissioners that business continuity is absolute"

"We finally found a solution that meets the city's data integrity needs. Veeam will be part of the city's lifeblood for the foreseeable future."

City of Sarasota

Guarantees business continuity for the **first time** in the city's history

veeam

Data Portability

Broadest storage support, avoiding vendor lock-in

Migrate and modernize your apps and infrastructure

Recover from anywhere to anywhere

Modern protection for modern workloads

" Veeam is widely recognized for cloud data management, so we know that piece of the puzzle is there when we need it. "

" We're counting on Veeam to help us ensure all data is available whether it's on-prem or in a cloud. "
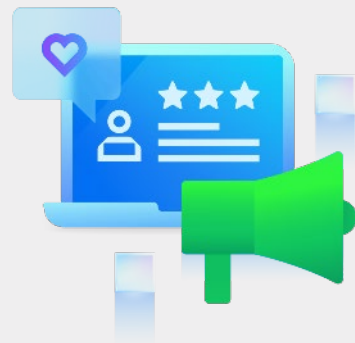
City of New Orleans

Patented Portable Data Format delivers complete Data Freedom that no other vendor can deliver

veeam

Data Intelligence

AI-powered detection and security scoring

Teams get answers faster with **AI Digital Assistant**

Automatic diagnostics and remediation analysis

Backup data reuse for **data mining, dev/test**

Relentlessly Driving Innovation

"Veeam protects data in so many ways — monitoring, alerting, reporting, verifying recoverability and instant recovery for real-time restore."
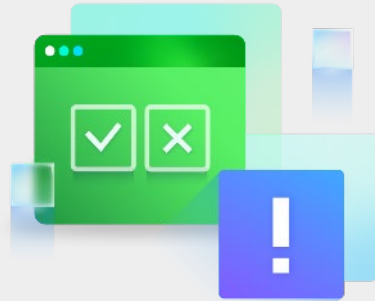
Hanover County

Data Security

Built-in security with a Zero Trust Architecture

End downtime with Incident Response services and tools

Detect threats earlier with proactive threat hunting

Data integrity with immutability everywhere

Veeam's AI-driven threat detection is **the industry benchmark**

Veeam has **integrated the most comprehensive** array of threat detection technologies
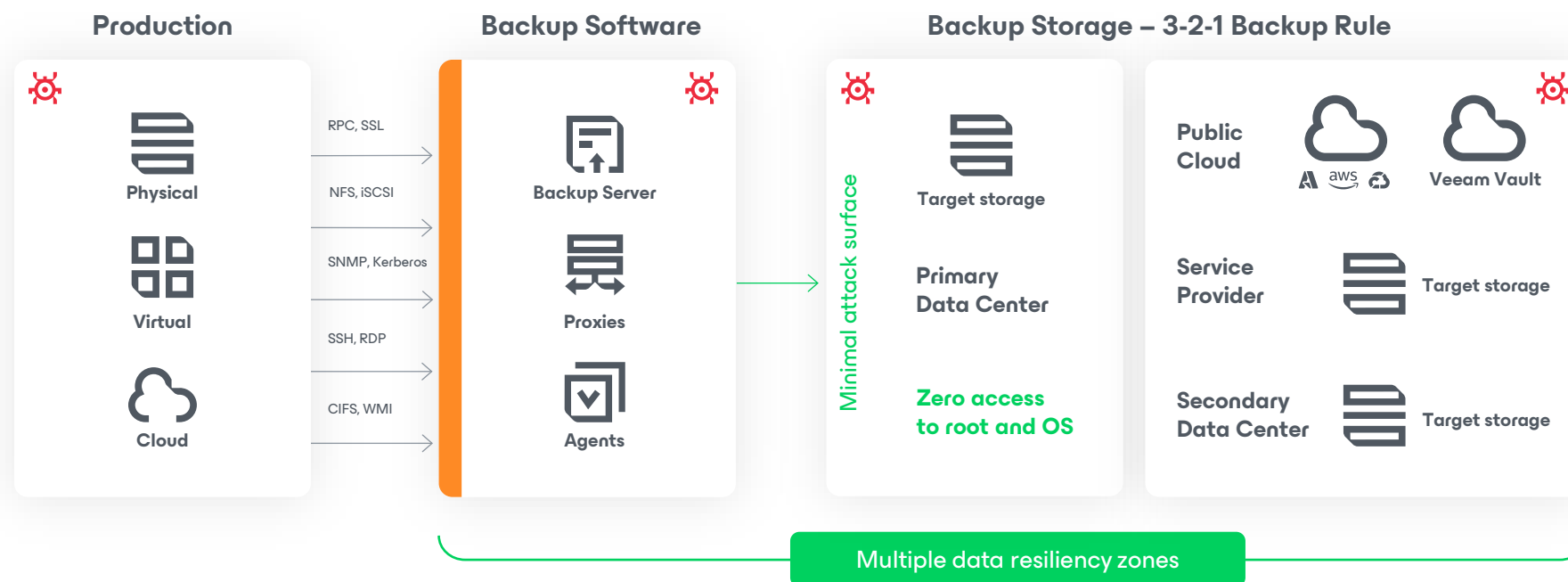
"What I find fascinating about ransomware is that everyone wants to get in front of the problem, which is great, but what do you do when you get hit? Are you truly prepared? What's your business continuity strategy?"

Kern County - CA

"That's why Veeam is our last line of defense. It preserves our business operations."

veeam

Hardware-agnostic security with Zero Trust Data Resilience

Secure by design with Zero Trust Architecture

Production

- Physical
- Virtual
- Cloud

RPC, SSL
NFS, iSCSI
SNMP, Kerberos
SSH, RDP
CIFS, WMI

Backup Software

- Backup Server
- Proxies
- Agents

Backup Storage – 3-2-1 Backup Rule

Minimal attack surface

Target storage

Primary Data Center

Zero access to root and OS

Public Cloud — A, aws, Veeam Vault

Service Provider — Target storage

Secondary Data Center — Target storage

Multiple data resiliency zones

Segmentation of software & storage

Multiple **data resilience zones**

Immutable backup storage

veeam

Veeam Cyber Secure

Pre-incident

- Advanced Architecture and Design
- Documented, pre-tested and orchestrated recovery
- Support Account Manager
- And More

During incident

- Proactive threat detection
- Expert Incident Response with Coveware
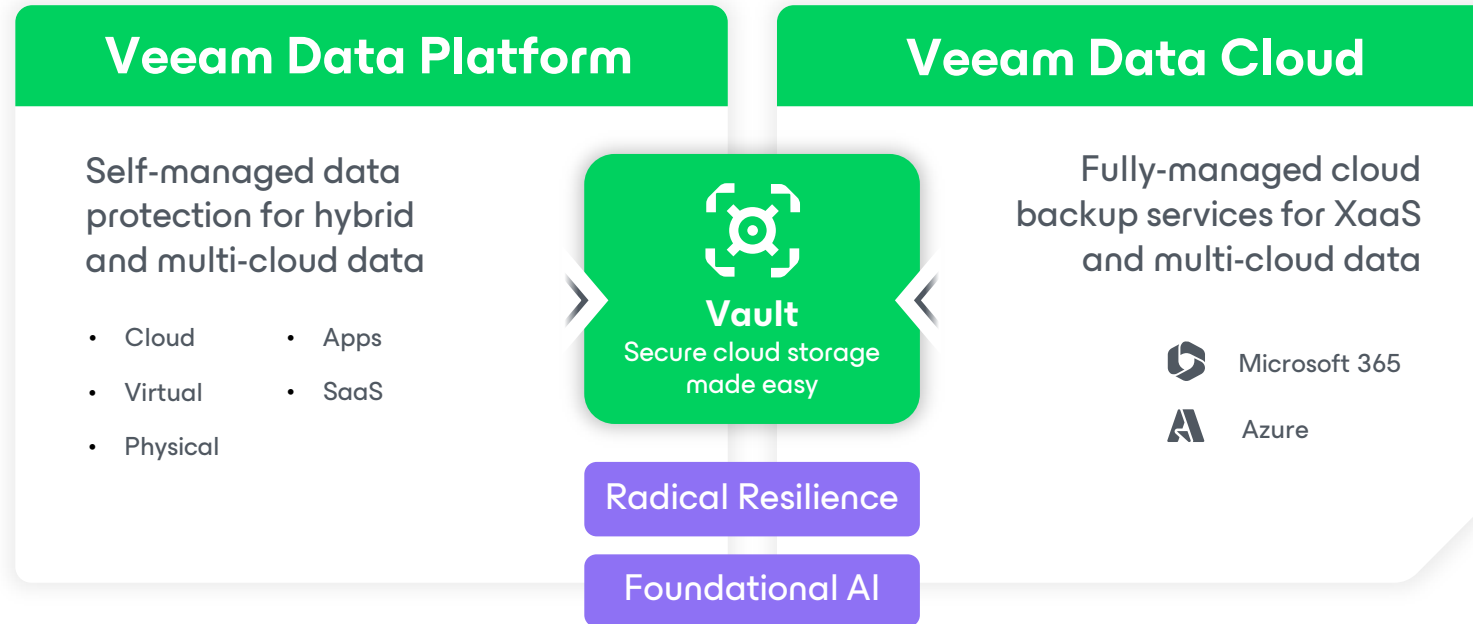- Ransomware SWAT Team with sub 30 minute SLA

Post incident

- De-risk current cyber attack
- Prepare for the one ahead
- Courses and Quarterly tactics, techniques, and procedures (TTPs) analysis for all parties

Veeam Data Cloud Vault

Veeam Data Platform

Self-managed data protection for hybrid and multi-cloud data

- Cloud
- Apps
- Virtual
- SaaS
- Physical

Vault
Secure cloud storage made easy

Radical Resilience

Foundational AI

Veeam Data Cloud

Fully-managed cloud backup services for XaaS and multi-cloud data

- Microsoft 365
- Azure

A fully-managed, secure cloud storage resource on Azure that eliminates the headaches of managing infrastructure and unpredictable cloud cost models.

Predictable
Eliminate bill shock with flat, per-TB pricing on two tiers of cloud storage, inclusive of API calls, restore, and egress charges.

Secure
Safeguard your data on zero trust storage that's always immutable and logically air-gapped from production.
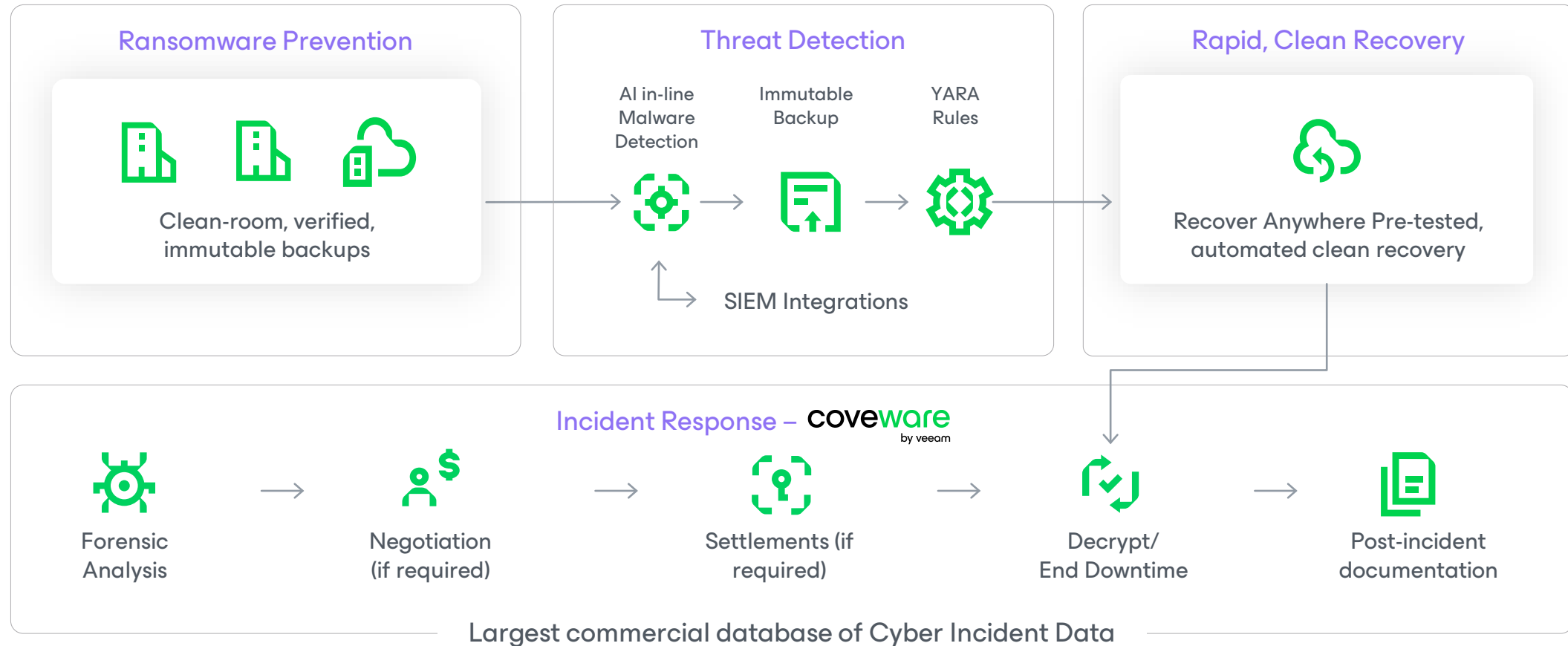
Easy
Access and use on-demand, fully-managed storage with zero config, management, and integration complexities.

Veeam provides the most complete end-to-end ransomware protection and recovery

Veeam Cyber Secure Program
24/7/365 SWAT Team | Health Checks | Ransomware Warranty | Incident Response Retainer

Ransomware Prevention

Clean-room, verified, immutable backups

Threat Detection

AI in-line Malware Detection

Immutable Backup

YARA Rules

SIEM Integrations

Rapid, Clean Recovery

Recover Anywhere Pre-tested, automated clean recovery

Incident Response – coveware by veeam

Forensic Analysis → Negotiation (if required) → Settlements (if required) → Decrypt/ End Downtime → Post-incident documentation

Largest commercial database of Cyber Incident Data

Empowering Government

Transformative Data Resiliency for Strategic Success

Freedom of Choice
Decisions Made Easier:

"Veeam is widely recognized for cloud data management, so we know that piece of the puzzle is there when we need it." "We're counting on Veeam to help us ensure all data is available whether it's on-prem or in a cloud."

City of New Orleans

Digitizing Processes
Digital Leadership:

"Cities serve a digital world, so a city's best defense in a digital world is dependable data protection, and that's exactly what Veeam provides,". "We trust our data is backed up reliably and can be recovered fast. Veeam is the reason we don't lose sleep anymore."

City of Rancho Cucamonga

End-to-End Resiliency
Lives Made Better:

"What I find fascinating about ransomware is that everyone wants to get in front of the problem, which is great, but what do you do when you get hit? Are you truly prepared? What's your business continuity strategy?" "That's why Veeam is our last line of defense. It preserves our business operations."

Kern County

Mission Focused, Customer Centric

Solutions for Government

Turning Knowledge Into Process

veeam

Veeam is #1 in Data Resilience

#1

Gartner
Market Share Analysis: Enterprise Backup and Recovery Software

Gartner
Magic Quadrant, ability to execute

Microsoft 365

aws
Kubernetes & Multi-cloud / Hybrid

IDC
global market share in Data Replication & Protection

IDC
Secure Recovery, 5x faster

Data Portability

veeam