

March 11, 2025 | Washington, DC

XACCELERATE

Advancing Cyber Innovation for Government

Palo Alto + Veeam



UN aviation agency
investigating reports of
possible data breach



Major location data
broker reports hack to
Norwegian authorities



New York Hospital Says
Ransomware Attack Data
Breach Impacts **670,000**



Data Breach — **240,000**
Credit Union Members
Exposed



Massive Health Care
Data Breach Threatens
Millions



US Treasury says
Chinese hackers stole
documents in 'major
incident'



Edtech giant says
hackers accessed
personal data of
students and teachers



US state hit by data
breach as hackers
demand ransom



~~Why didn't they detect it?~~
Why didn't they detect that they detected it?

A Holistic Platform For Delivering SOC Services



Cortex Xpanse

Discovers and reduces the entire **attack surface**

Cross correlates **internal view of assets** with **outside-in** mapping

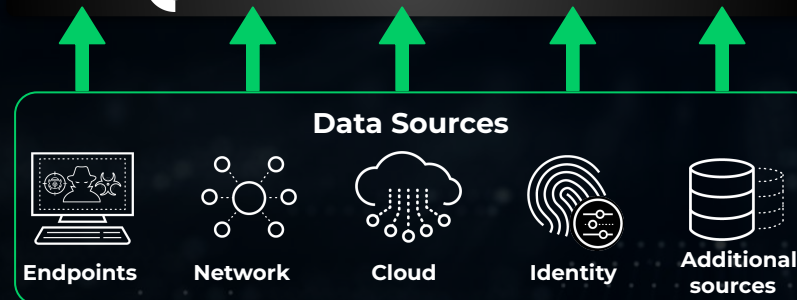
Understands exposure to new attacks and how attacks have unfolded (including **supply chain exposures** and nation-state vulnerabilities)



Cortex XDR



 **Stitched and Normalized**



Cortex XSOAR

Scales and accelerates security operations with automation

Reduces manual steps in your incident response workflow by up to 100%

Easily deploy new automation cases via **extensive SOAR marketplace**

Unified SecOps Platform



Cortex XSIAM

Unify SOC Operations with an integrated **AI-driven platform**

End-to-end workflow automation for security operations

Cortex XSIAM: AI-Driven Security Operations



Easily extend the platform with advanced capabilities

ITDR

TIP

ASM

 MDR

Replaces multiple SOC tools

SIEM

EDR

NDR

SOAR

CDR



Data

~9 PB/day
100s of data sources



AI

7,000+ detectors
(2,400 ML models) + BYOML



Automation

1,000
default playbooks

Single SOC UI
simplifies and accelerates
SOC analyst work

Eliminates Data Silos
through analytics with
full context

AI-Powered Defense
to stop threats
from days → minutes

Automated Operations
to accelerate
SOC outcomes

Data: Unified Tools & Data to Power AI and Automation



Data

4x more data ingested



AI



Automation

Any Data Source



Endpoint



Network



Cloud



Identity

- | | | | |
|------------|---------------|------------------|------------|
| kafka | Microsoft 365 | Google Workspace | tenable |
| infoblox | proofpoint | zscaler | CYBERARK |
| CLOUDFLARE | slack | CISCO | salesforce |
| | | | Dropbox |

Other



Ingest
raw
data



Normalize
data
for AI



Enrich data
with threat
intelligence

**Single, complete
source of
AI-ready data**



Simplified new data source
onboarding

Optimized for efficient
prevention, detection,
response.

AI: AI-Powered Defense to Stop Threats in Minutes



Data



AI



Automation

7,000 detectors and over 2,400 ML models

Single, complete
source of
AI-ready data



Simplified new data source
onboarding

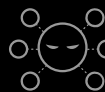
7K Detectors
and over
2.4K+ ML models
continuously advancing



Real-time
prevention



Precise causality
and detection

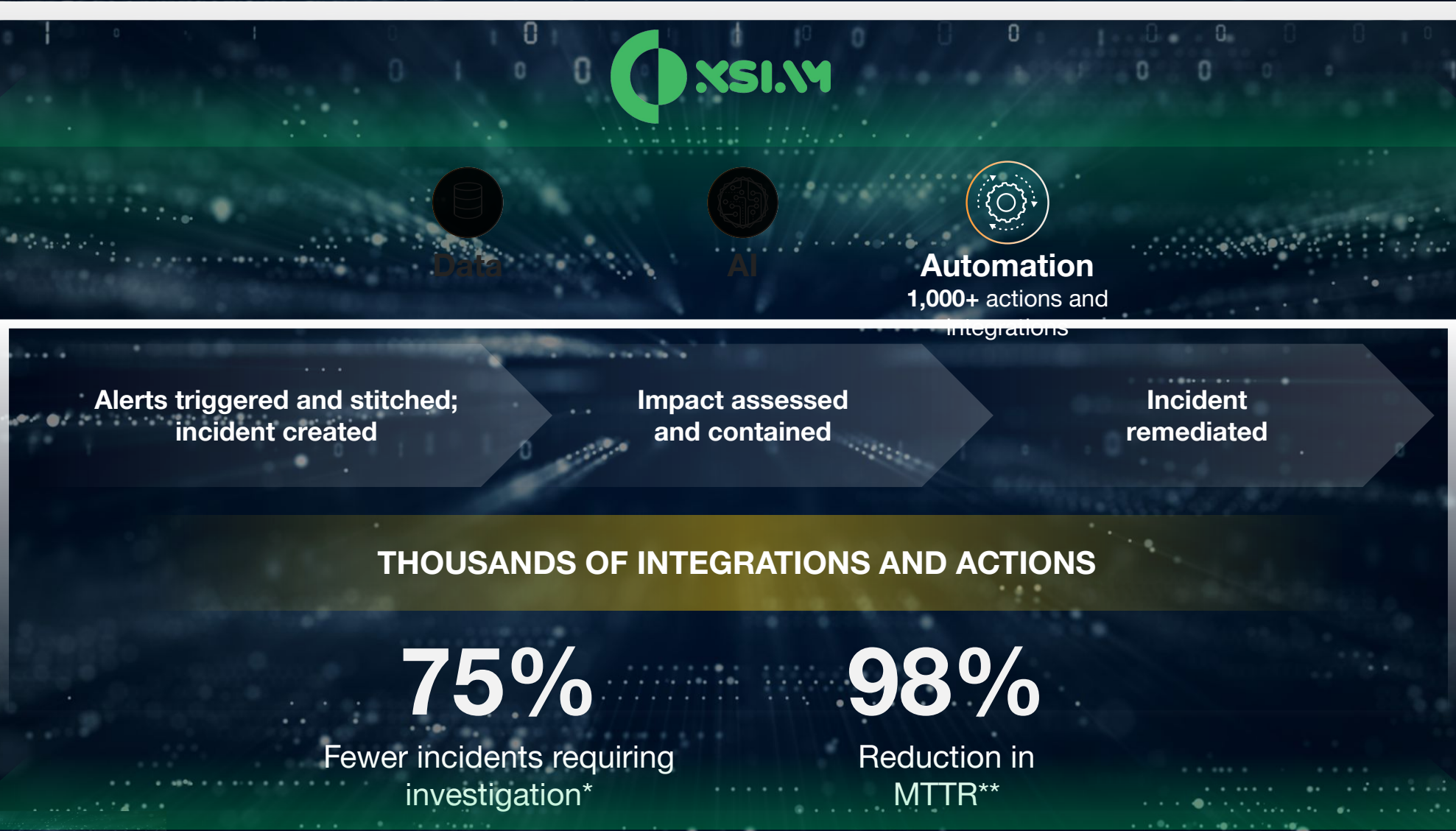


Full context
of threats

100% Detection and industry-low false positives
in MITRE ATT&CK Round 6

Optimized for efficient
prevention, detection,
response.

Automation: Automated Operations to Accelerate SOC Workflows



*Oil and Gas company case study





**Boyne Resorts case study

Integrating the Entire SOC Ecosystem with Dedicated Data Models

ENDPOINT

14+





Data Models

  Microsoft  Cisco 

NETWORK

23+


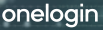

Data Models

 Check Point  Fortinet  Netskope 

IDENTITY

6+

Data Models

 CyberArk  Duo  

1,000+




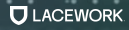


INTEGRATIONS



CLOUD

26+

Data Models

    WIZ 

MSSP



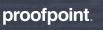

 Deloitte.  orange™ 

and more...

OTHER

35+

Data Models

  Forcepoint  Salesforce  ServiceNow

Syslog Collector Apache Kafka Collector CSV Collector Netflow Collector
Database Collector FTP Collector Files and Folders Collector SNMP Collector

Veeam is
purpose-built
for powering
data resilience



Veeam Data Platform

Recovery Orchestration

Monitoring & Analytics

Backup & Recovery

Native APIs

Platform
Extensions

aws AWS

A Azure

Google Cloud

Kubernetes



Cloud



Virtual



Physical



Apps



SaaS

Microsoft 365

Salesforce

On-Premises • In the Cloud • XaaS



New for 2024

Virtual/Database

- Proxmox VE
- MongoDB

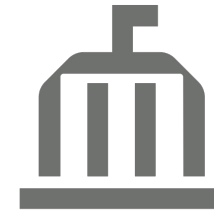
Cloud

- Amazon FSx
- Amazon RedShift
- Azure Cosmos DB
- Azure Data Lake Storage Gen2

The Problem

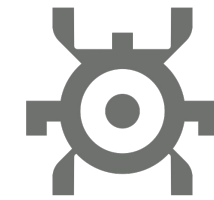
■ Data Infrastructure

- Cyberattacks are common
- Attempts to access infrastructure are frequent, including backups
- Large number of tactics, techniques, and procedures (TTPs) utilized by threat actors
- IoCs are difficult to identify
- Unpredictable dwell time (between compromise and attack)



75%

of organizations suffered at least one ransomware attack



96%

of cyber attacks target backups

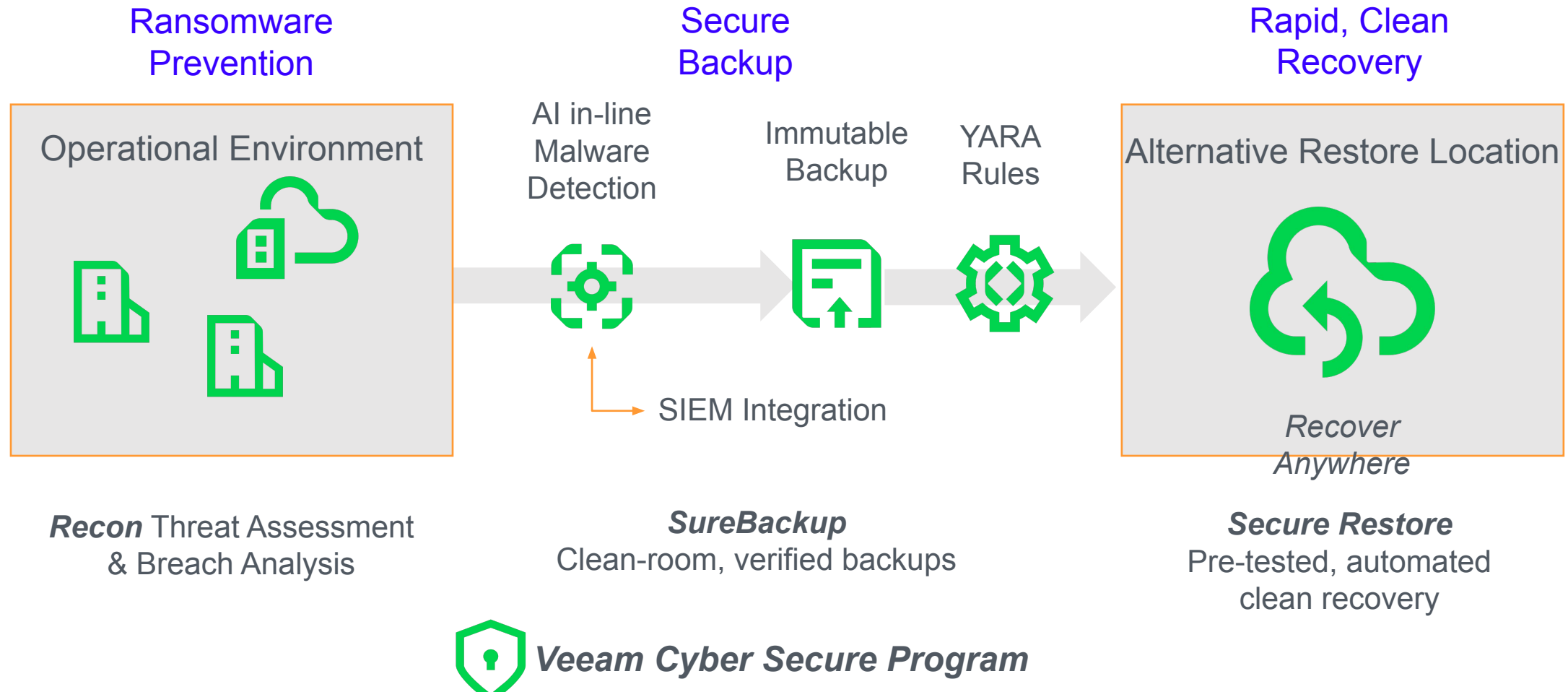


68%

of financial impact attributed to costs other than the ransom payment

Veeam Data Platform Provides Cyber Resilience

The complete end-to-end ransomware defense



Veeam Cyber Resilient Ecosystem

Security information
and event
management (SIEM)

SOPHOS

paloalto
NETWORKS

splunk>

Secure Restore

Bitdefender

eset

Microsoft
Defender

SOPHOS

Symantec
by Broadcom

Trellix

YARA – rule-based detection

veeam

Recon

coveaware
by veeam

Ransomware detection

Bitdefender

eset

Microsoft
Defender

SOPHOS

Symantec.
by Broadcom

Trellix

veeam

Incident Response

veeam
Cyber
Secure

with

coveaware
by veeam

Readiness

DARKTRACE

kyndryl

PAESSLER
THE MONITORING EXPERTS

OPENVPN

WIREGUARD

Security Orchestration,
Automation and
Response (SOAR)

servicenow.

paloalto
NETWORKS

Progress
Flowmon

Cisco XDR

veeam
Incident API

Storage Cyber Events
Detection

veeam
Incident API

Veeam Ready Immutability

NUTANIX

NetApp

DELL

MINIO

BACKBLAZE

PURESTORAGE

CLOUDIAN

ORACLE

DATACORE

II-II SYSTEMS

FAST LTA

Synology

HITACHI

Impossible
Cloud

Infortrend

OSNEXUS

iTernity

NEXSAN

Quest

IBM

QNAP

Quantum

SCALITY

OVHcloud

Red Hat

RSTOR

POINT
software & system

Qumulo

SEAGATE

SPECTRA

SOFTIRON

Ugloo

SUSE

SwiftStack

zadara

OBJECT
FIRST

SWARM
software & system

STONEFLY

wasabi

VAST

Tape/WORM

DELL

FAST LTA

IBM

SPECTRA

Quest

FALCONSTOR

OVERLAND
TANDBERG

ORACLE

Quantum

StarWind

Storage
Integrations

Hewlett Packard
Enterprise

DATACORE

vmware

FUJITSU

Lenovo

IBM

cisco

Microsoft

NetApp

inspur

NUTANIX

Tintri

HITACHI

INFINIDAT

DELL

NEC

PURESTORAGE

HUAWEI

Veeam Integrated
Immutability

aws

Azure

IBM Cloud

wasabi

Encryption/KMS

ENTRUST

Fortanix

IBM Security

THALES

aws

Azure

Google Cloud

Storage & Backup Compliance Monitoring

continuity

veeam

The background is a dark blue, almost black, space filled with glowing white and light blue particles. These particles are arranged in a way that suggests a complex network or data flow, with many small dots connected by thin, faint lines. Some larger, brighter clusters of dots are visible, and there are horizontal bands of slightly more concentrated particles near the top and bottom. The overall effect is one of a high-tech, digital environment.

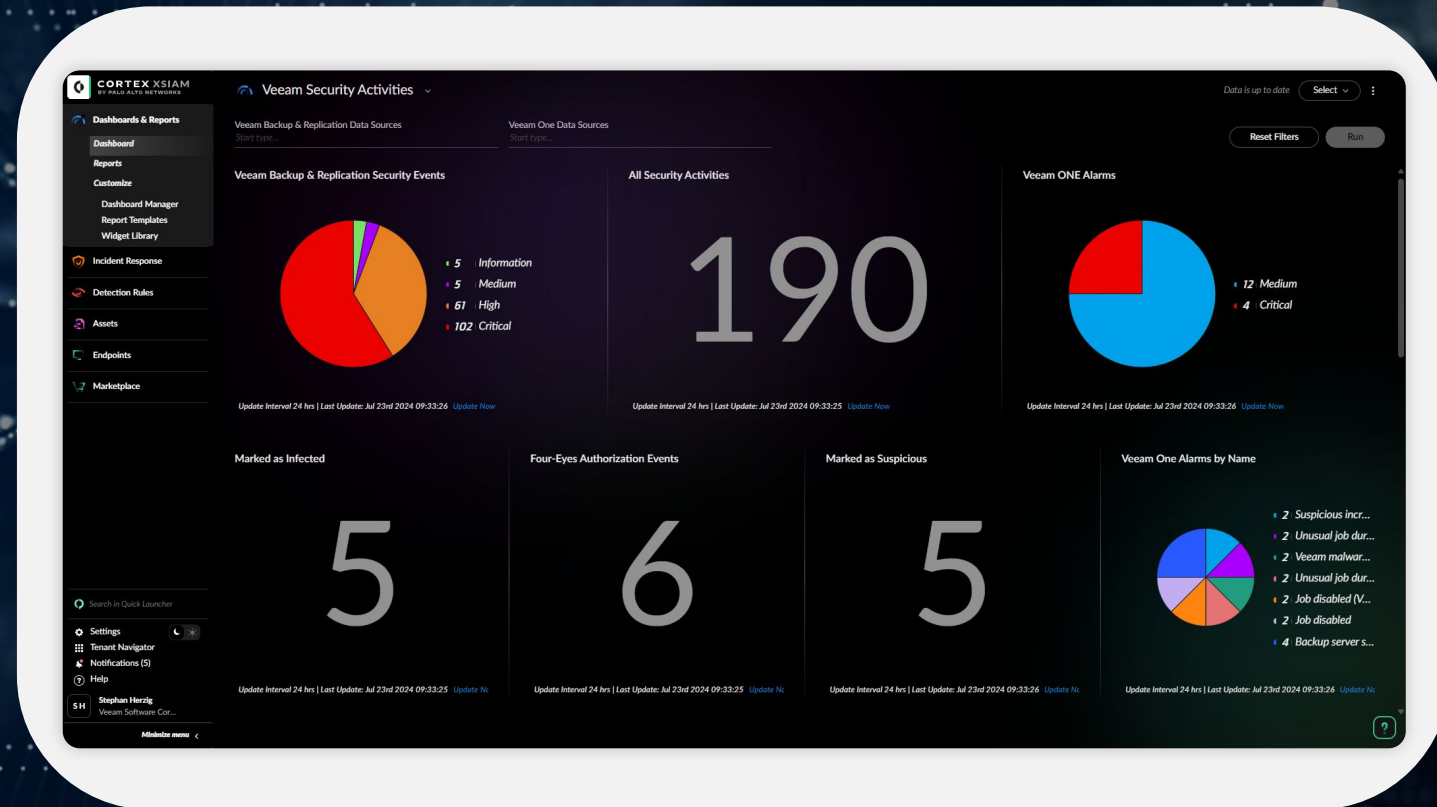
Veeam App for Palo Alto Networks XSIAM

Veeam App for Palo Alto Networks XSIAM

- Veeam developed security marketplace App for Palo Alto's SIEM

Veeam is a Pilot Partner delivering the first 3rd party developed App incl:

- Syslog ingest with events from Veeam Backup & Replication and Veeam ONE
- Pre-defined Veeam Monitoring Dashboard
- Pre-defined Veeam Security Dashboard
- Pre-created parser and event filtering
- Support for both Veeam Backup & Replication as well as Veeam ONE syslog ingest
- Documented correlation rules



Palo Alto Networks XSIAM + Veeam

■ Palo Alto Cortex XSIAM protects and monitors your environment, now including Veeam

- Veeam Backup & Replication and Veeam ONE use industry-standard Syslog to send application events to Palo Alto Cortex XSIAM Broker VM
- XSIAM Broker VM sends events to Palo Alto Cortex XSIAM
- Veeam App for Palo Alto XSIAM parses incoming Syslog data for display on detailed dashboards



The background is a dark blue, almost black, space filled with abstract digital elements. At the top, there's a horizontal band of faint binary code (0s and 1s). Below this, numerous glowing white and light blue dots are connected by thin, radiating lines, creating a sense of a vast, interconnected network or data flow. The overall effect is futuristic and high-tech.

Veeam Appfor Palo Alto Networks XSOAR

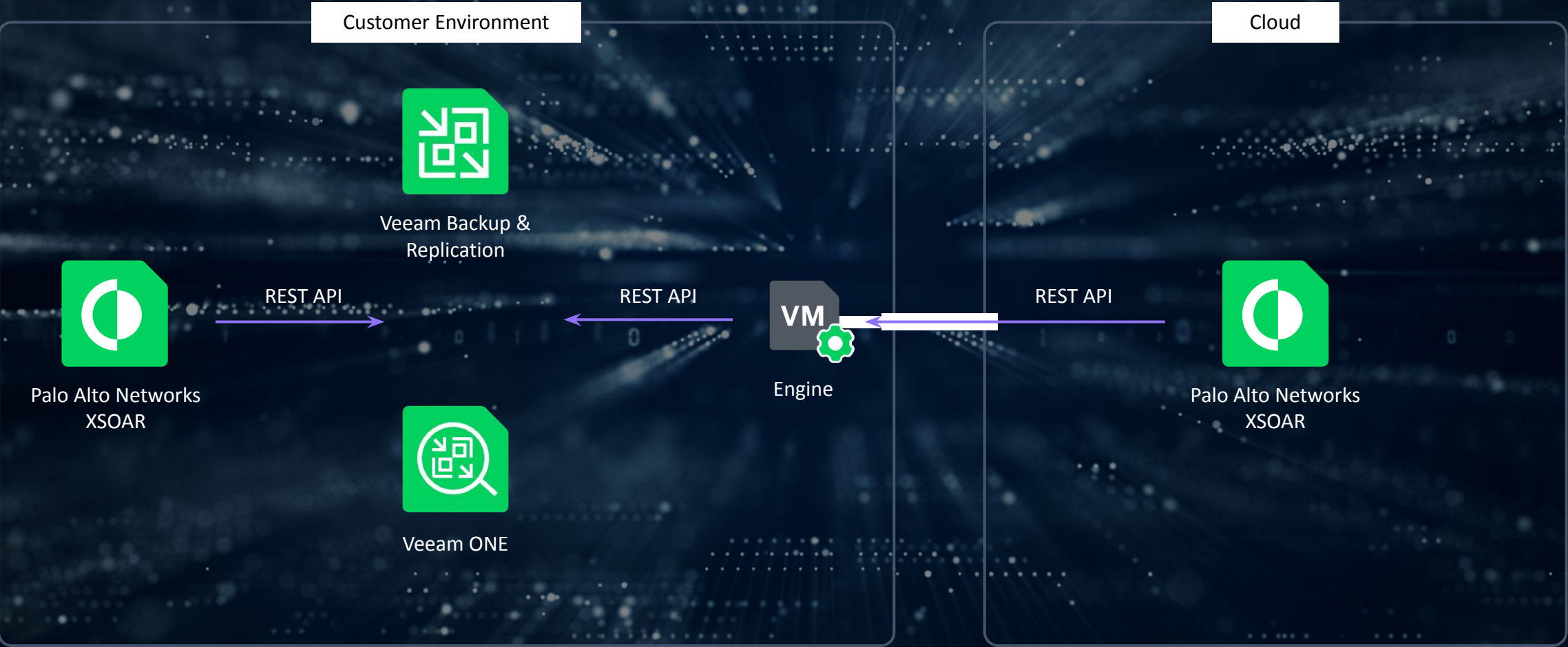
Veeam App for Palo Alto Networks XSOAR

First ever Veeam developed security marketplace App with API level integration

- Bi-directional API-level connection to both Veeam Backup & Replication and Veeam ONE
- Pre-defined Incident Dashboard
- Veeam Malware event handling with Palo Alto Incident creation
- Additional Incident handling (e. g. for Configuration Backup too old, Repositories running out of space)
- Playbooks for SOC:
 - Start Veeam Instant VM recovery Playbook to
 - Start Veeam Configuration Backup
 - Acknowledge and resolve Veeam ONE alerts
- Functions:
 - Trigger Veeam Incident API from Palo Alto events
 - Query available “clean” restore points



Solution diagram — Veeam App for Palo Alto Networks XSOAR



Veeam App for Palo Alto Networks XSOAR – Incidents

- Incidents get created for the following events:
 - **Veeam Backup & Replication**
 - Malware Detection (Inline/Malware Extensions/Deletions/Incident API)
 - AV/YARA scan detections
 - Configuration Backup not executed for 30 days (default)
 - Repository Free Space below 200 GB (default)
 - **Veeam ONE**
 - Veeam ONE Alerts with Status Error/Warning
 - Backup Server security & compliance state
 - Suspicious incremental backup size
 - Unusual Job Duration
 - and more - see documentation



Available Playbooks

Start Instant VM Recovery

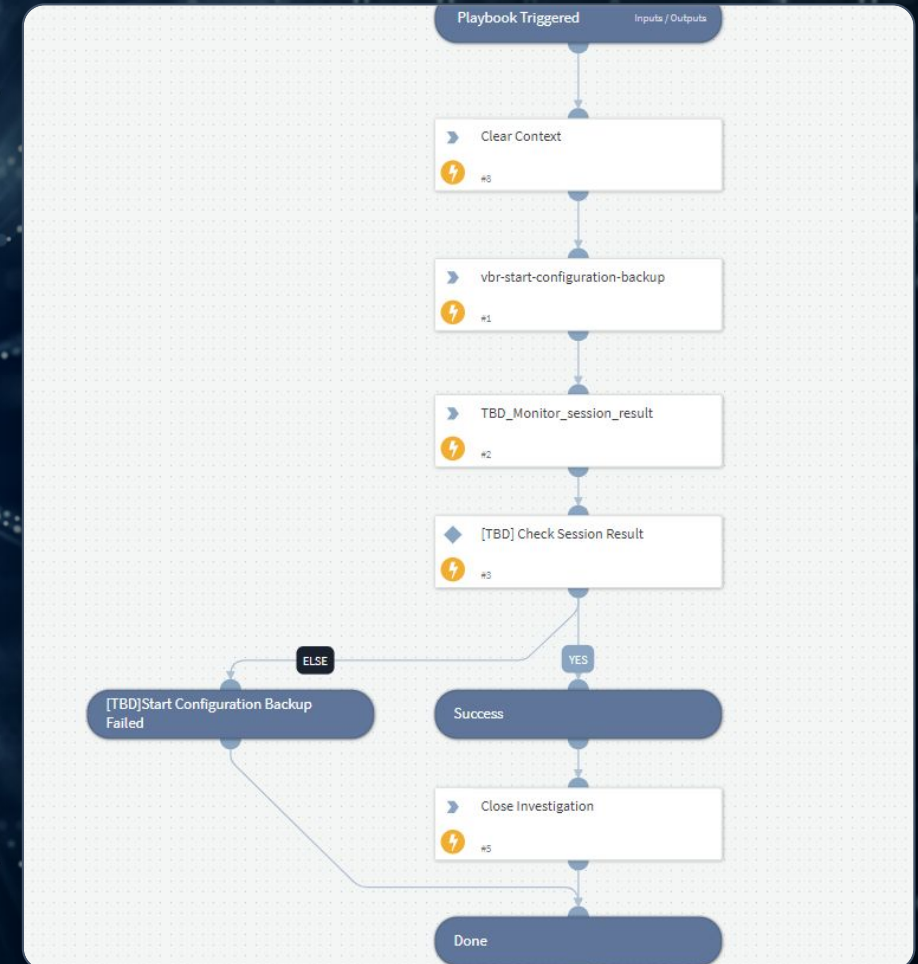
- Start Instant Recovery Manually/Start Instant VM Recovery Automatically
- This Playbook triggers an Instant VM recovery from an XSOAR Incident. There is a Playbook that retrieves the parameters automatically or the customer has the choice to enter the desired parameters manually. Before the Instant Recovery starts the customer gets asked if an AV scan should be done.

Start Configuration Backup

- Starts a Veeam Backup & Replication Configuration Backup

Acknowledge Veeam ONE Alarm

- Acknowledges a reported Veeam ONE Alert



The background is a dark blue gradient filled with abstract digital elements. At the top, there are horizontal bands of binary code (0s and 1s). Below these, numerous small white dots are connected by thin, glowing lines, creating a network or particle trail effect that radiates from the center. The overall aesthetic is high-tech and futuristic.

DEMO

Palo Alto Apps