NUTANIX™

Protecting against Ransomware in a Hybrid Cloud World

Gregor Davidson CISSP
Solutions Architect - NetSec
gregor@Nutanix.com

SEPTEMBER 2021

Hybrid cloud is today's operating model of choice

92% Selected multi cloud as their ideal IT operating model[↧]

Say "security" is top concern[↟] **81%**

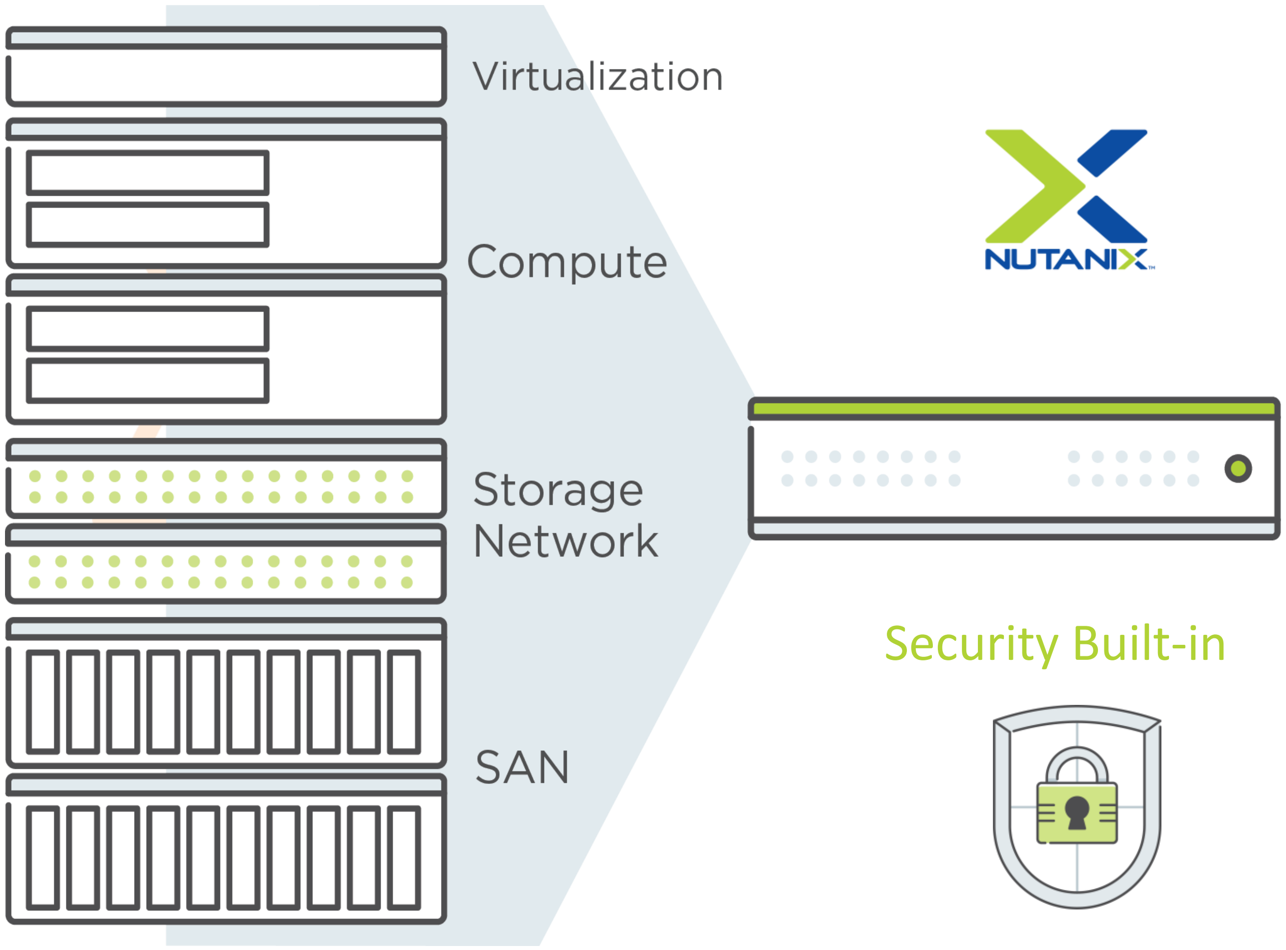
$3.86M Average Total Cost of a Data Breach

Claimed they would stop doing business after data breach **70%**

[↟] Flexera State of the Cloud Report 2021
[↧] Nutanix Enterprise Cloud Index 2019

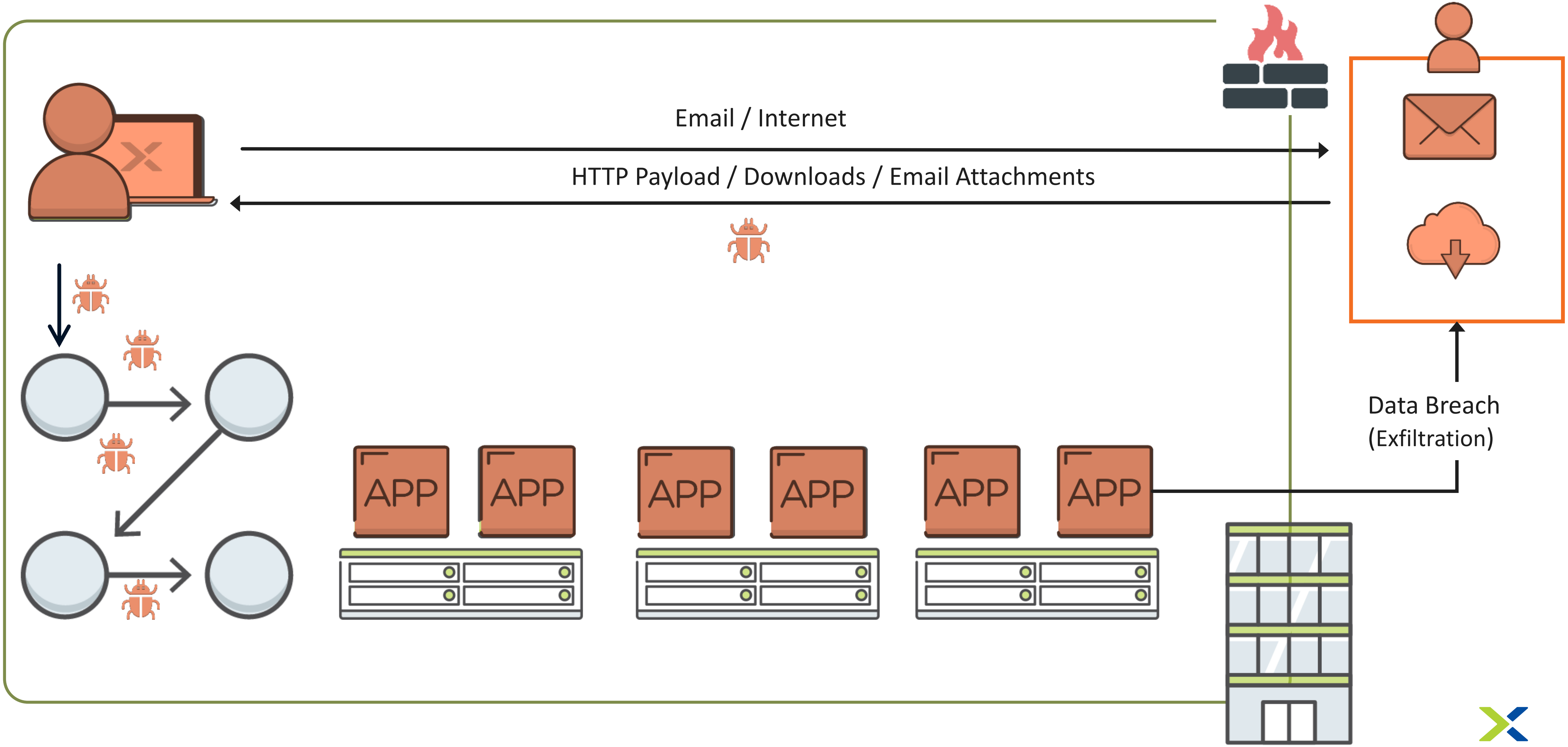
A Better Approach to Security

Infrastructure that simplifies operations and security



- ✓ Continuous Compliance
  - ✓ Beam
- ✓ Micro-segmentation
- ✓ Network Segmentation
- ✓ Authentication, RBAC, Auditing
- ✓ Cluster Lockdown
- ✓ 1-Click Security Patching
- ✓ Security Configuration Management Automation
- ✓ Secure Hypervisor
- ✓ Unstructured Data Analytics
- ✓ Native Key Manager
- ✓ Data-at-Rest Encryption
- ✓ Data Protection

Anatomy of a Modern Attack



Why does Microsegmentation help?

APPLICATION-CENTRIC SECURITY / ZERO TRUST

Insider Incidents Up ~50%

The volume of incidents due to insiders continues to rise.

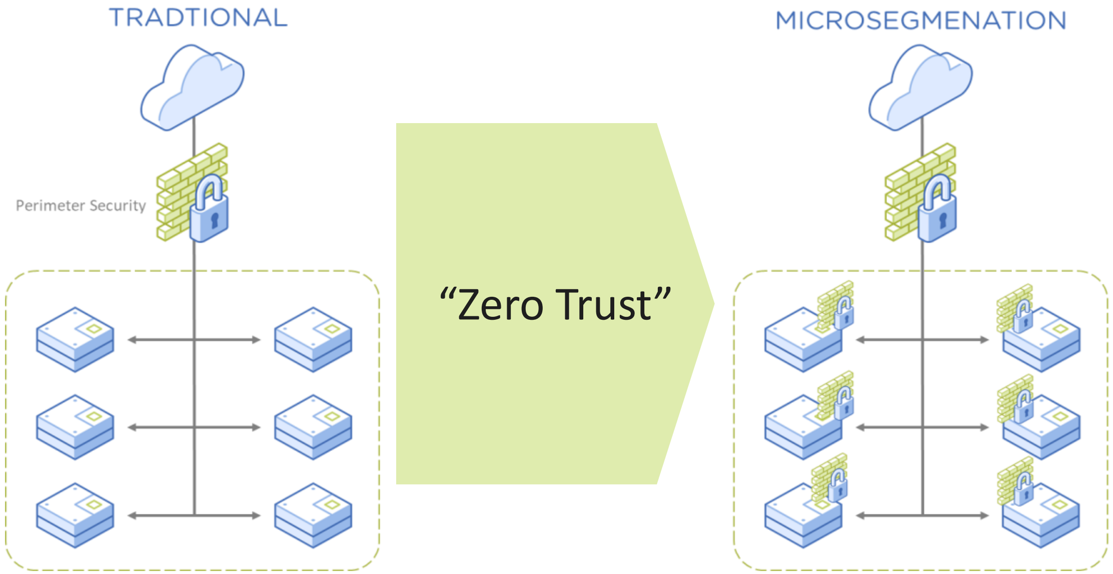
More than half are due to negligence vs malice.

"The Real Cost of Insider Threats in 2020", Ponemon Institute

75% Don't Focus on Prevention

A balanced approach to the entire security lifecycle is required. Prevention, Detection, Containment, and Recovery.

'Preventing Cyberattack Penetration Can Save Enterprises Up To $1.4 Million", Ponemon Institute



Zero Trust Models are Needed

"Organizations should not automatically trust anything inside or outside its perimeters…"

-John Kindervag, former principal analyst at Forrester Research

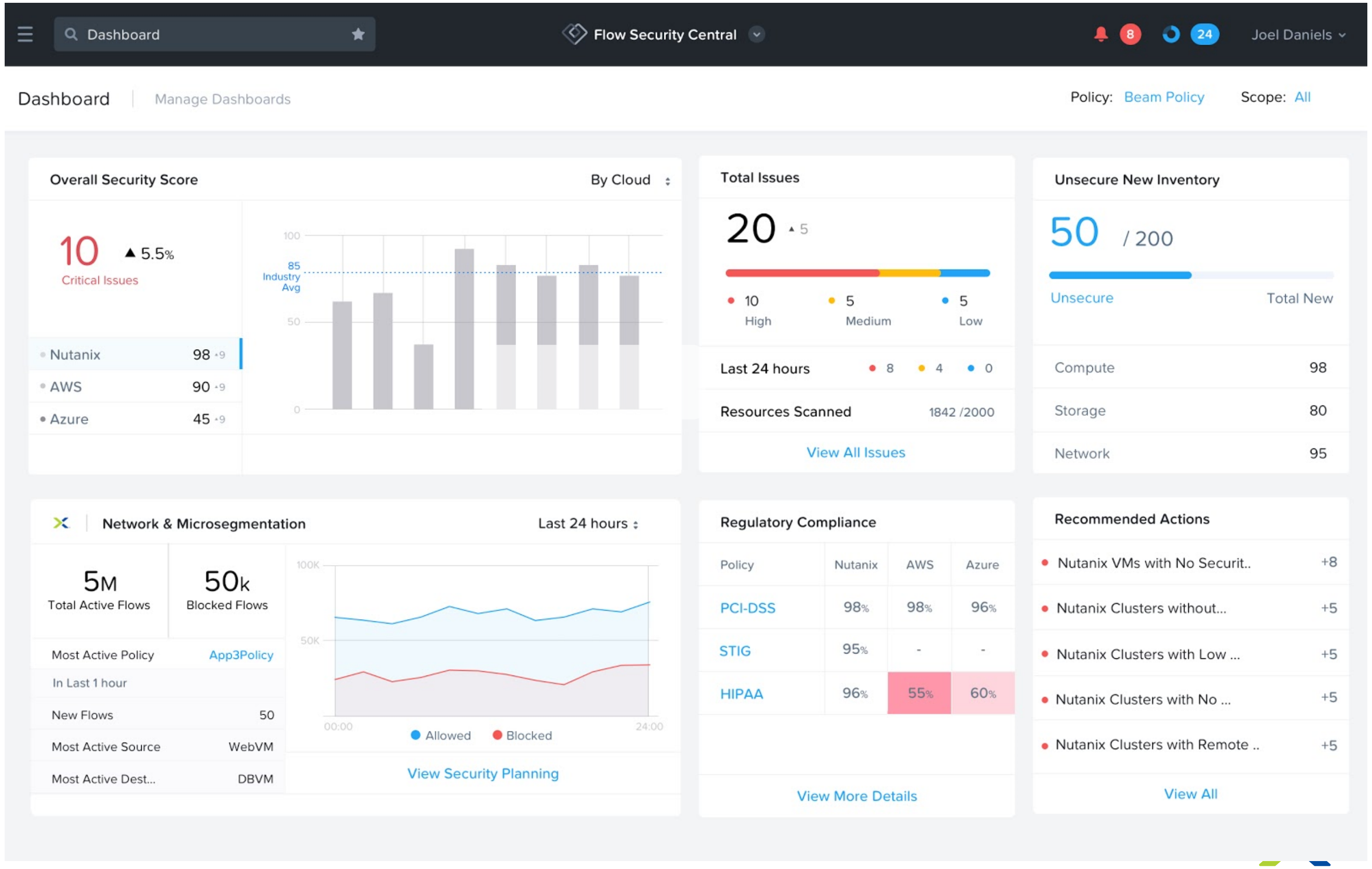
Insights and Monitoring

MONITORING AND VISIBILITY – multi-cloud dashboards, asset inventory, reporting, and alerts

AUDIT AND REMEDIATION – insights on Nutanix environments and public clouds using real-time, automated security audits

COMPLIANCE – continuously monitor your environment, automate compliance checks, and address vulnerabilities

SECURITY PLANNING – detailed traffic visualization and workload categorization for microsegmentation



Dashboard | Manage Dashboards

Policy: Beam Policy Scope: All

Overall Security Score By Cloud

10 ▲ 5.5%
Critical Issues

Nutanix	98 ▴9
AWS	90 ▴9
Azure	45 ▴9

Total Issues

20 ▴5

● 10 High ● 5 Medium ● 5 Low

Last 24 hours ● 8 ● 4 ● 0

Resources Scanned 1842 /2000

View All Issues

Unsecure New Inventory

50 / 200

Unsecure Total New

Compute	98
Storage	80
Network	95

Network & Microsegmentation Last 24 hours

5M Total Active Flows

50k Blocked Flows

Most Active Policy	App3Policy
In Last 1 hour	
New Flows	50
Most Active Source	WebVM
Most Active Dest...	DBVM

View Security Planning

Regulatory Compliance

Policy	Nutanix	AWS	Azure
PCI-DSS	98%	98%	96%
STIG	95%	-	-
HIPAA	96%	55%	60%

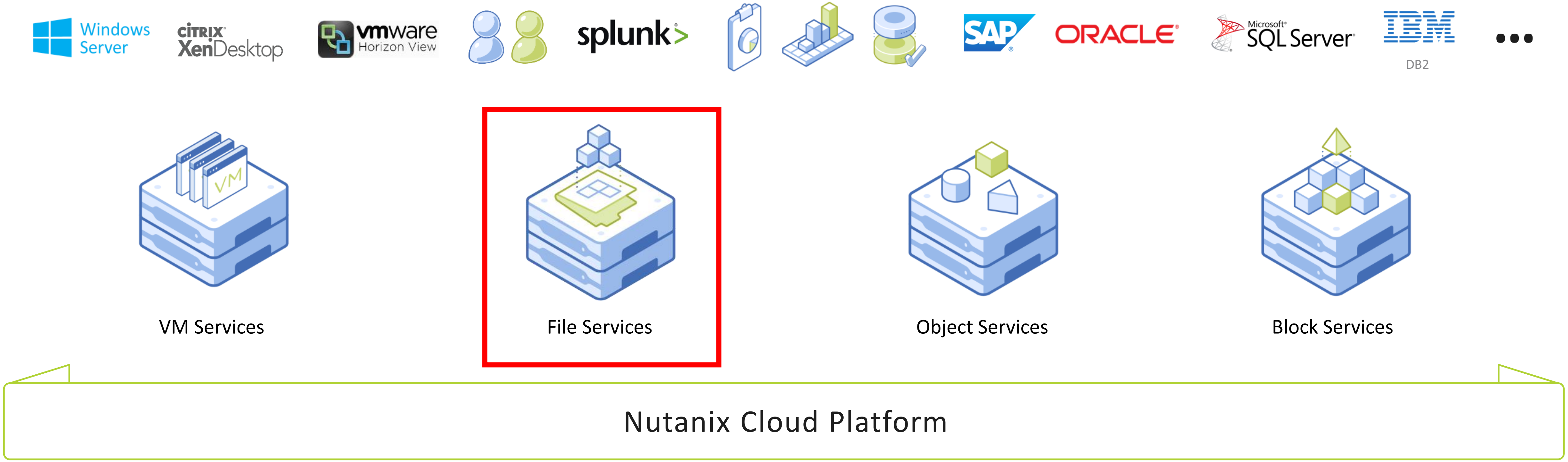
View More Details

Recommended Actions

● Nutanix VMs with No Securit..	+8
● Nutanix Clusters without...	+5
● Nutanix Clusters with Low ...	+5
● Nutanix Clusters with No ...	+5
● Nutanix Clusters with Remote ..	+5

View All

File Storage is a key workload



VM Services

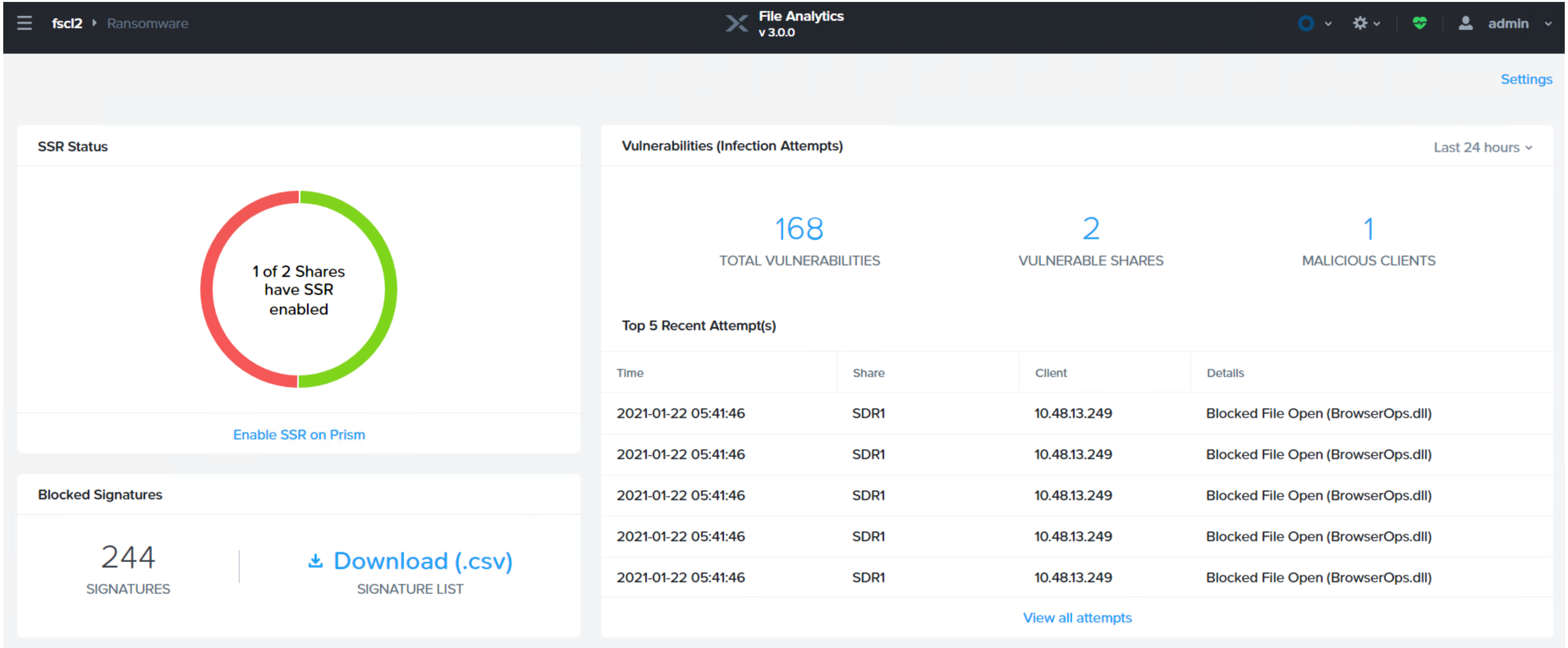
File Services

Object Services

Block Services

Nutanix Cloud Platform

Ransomware Dashboard



SSR Status

1 of 2 Shares have SSR enabled

Enable SSR on Prism

Blocked Signatures

244 SIGNATURES

Download (.csv) SIGNATURE LIST

Vulnerabilities (Infection Attempts)

Last 24 hours

168 TOTAL VULNERABILITIES

2 VULNERABLE SHARES

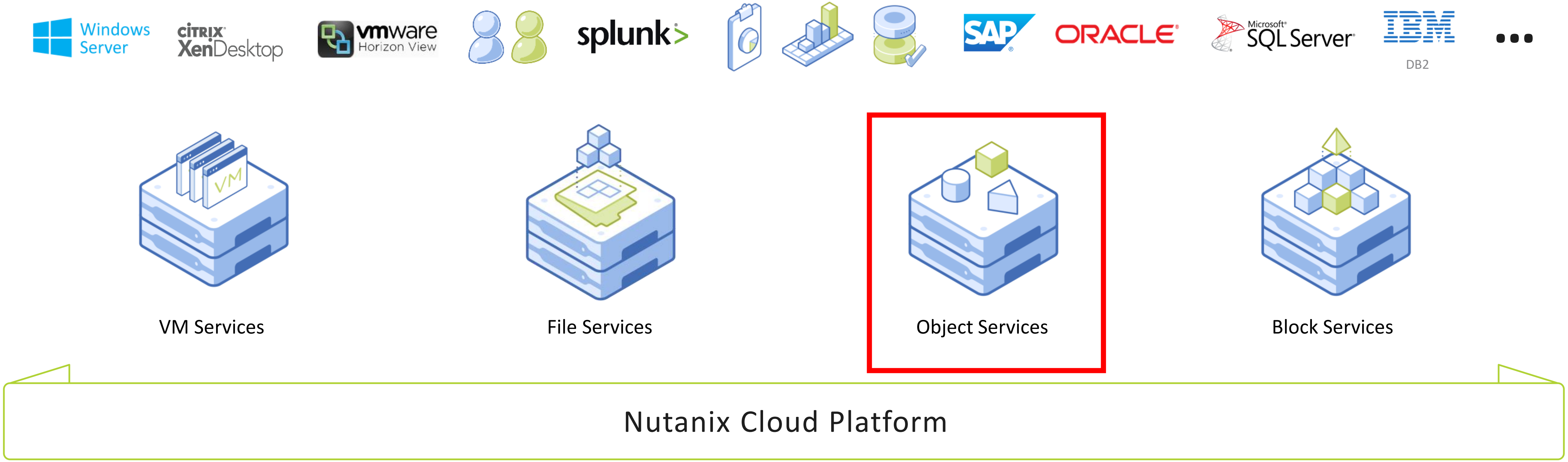
1 MALICIOUS CLIENTS

Top 5 Recent Attempt(s)

Time	Share	Client	Details
2021-01-22 05:41:46	SDR1	10.48.13.249	Blocked File Open (BrowserOps.dll)
2021-01-22 05:41:46	SDR1	10.48.13.249	Blocked File Open (BrowserOps.dll)
2021-01-22 05:41:46	SDR1	10.48.13.249	Blocked File Open (BrowserOps.dll)
2021-01-22 05:41:46	SDR1	10.48.13.249	Blocked File Open (BrowserOps.dll)
2021-01-22 05:41:46	SDR1	10.48.13.249	Blocked File Open (BrowserOps.dll)

View all attempts

Object Services for Immutable Storage



VM Services

File Services

Object Services

Block Services

Nutanix Cloud Platform

Protect Backups From Ransomware

Immutable Objects WORM storage
for critical data and backups

Detection

Prevention

Recovery

Enable WORM at a bucket level

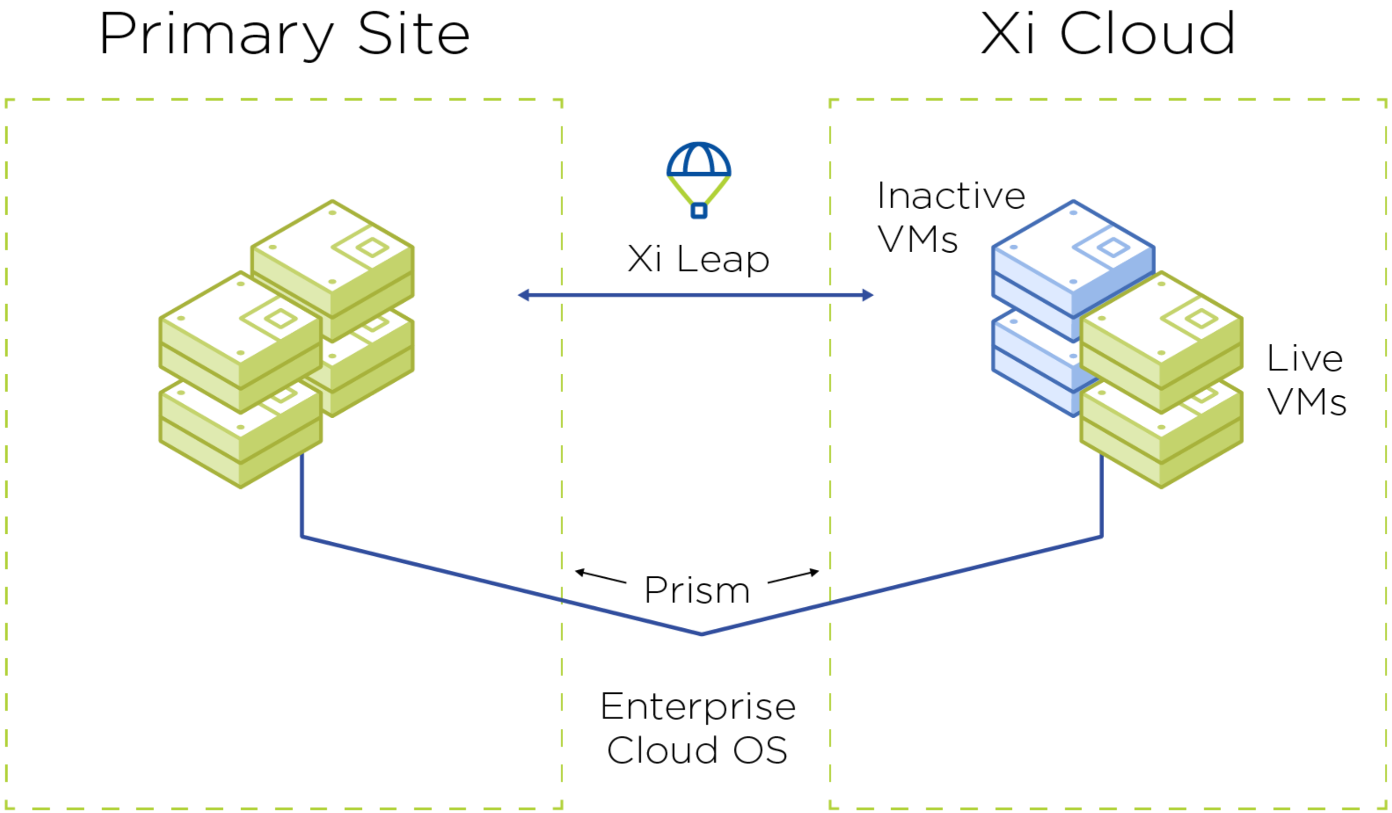
Strict Compliance WORM – cannot be disabled

WORM duration may be extended (but not reduced)

Object level lock

Independently validated (by Cohasset)

Natively Integrated Cloud DR



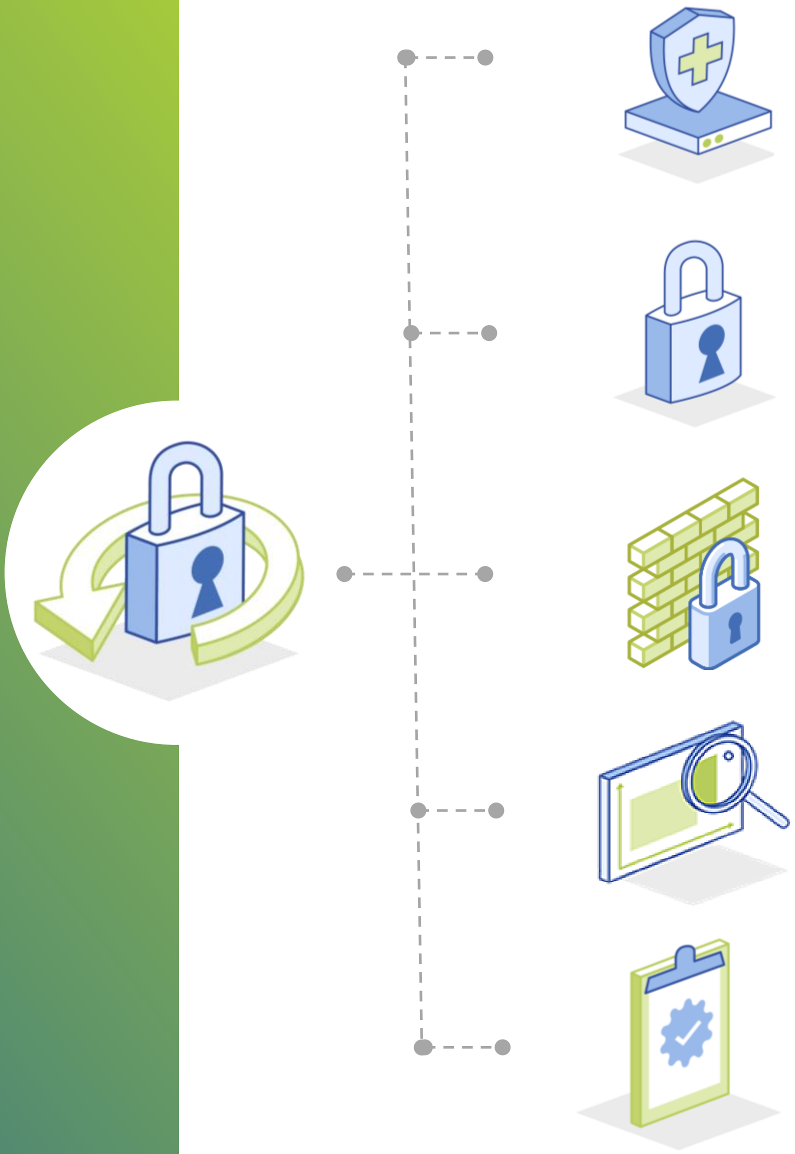
Eliminate the need for dedicated DR site

Subscription service managed from Prism

One-click failover, failback and testing

Keep Your Data and Applications Safe

With a defense in depth approach, Nutanix provides a secure and robust private cloud platform along with multicloud services to protect your critical applications and data



Secure the Platform with automated and self healing secure configurations

Protect data with native data-at-rest encryption, key management, and access control

Prevent breaches through network segmentation and application policy controls

Detect and Remediate security configuration errors on premises or in public clouds

Audit and Report on regulatory compliance policies such as PCI-DSS, HIPAA, NIST and more

Thank You