

alhambra
leave IT in our hands

VERITAS™

Protégete del ransomware con una receta infalible





Ransomware ... bla, bla, bla



José María Ochoa

Area Manager | Cybersecurity – OneseQ
aQuantum Cybersecurity Research Consultant
Comité operativo de Cloud Security (CSA)
Cibercooperante INCIBE
Ethical Hacking & CISO
Lead Auditor 27001



08:00 am de un día cualquiera

Un email entrante cuando enciendes tu equipo y haces login ...

con un solo mensaje contundente ...

“TU PASSWORD ES “Choco22!” hemos accedido a todas tus cuentas y tenemos información muy sensible y la divulgaremos en 24 horas. Sabemos todo lo que has hecho. Contactaremos en breve

Hasta entonces mantendremos **CIFRADOS** todos tus archivos”

Después solo otro mensaje de correo:

“El rescate serán 50.000€”

PD: ¡vaya nombre que le has puesto a tu perro!

Your Computer is Locked !



Your importing files are encrypted !

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so much time.

You have only 3 days to submit the payment. After that the price will be doubled.

Also if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. Go online for more information.

Please check the current price of Bitcoin and buy some bitcoins. And send the correct amount to the address specified in this window. Once the payment is checked, you can start decrypting your files by getting the DecryptionCode.

Send 0.5 Bitcoin to



Insert DecryptionCode here

DECRYPT

¿Estamos preparados para prevenirlo?

¿estamos preparados para detectarlo?

¿Estamos preparados para responder?

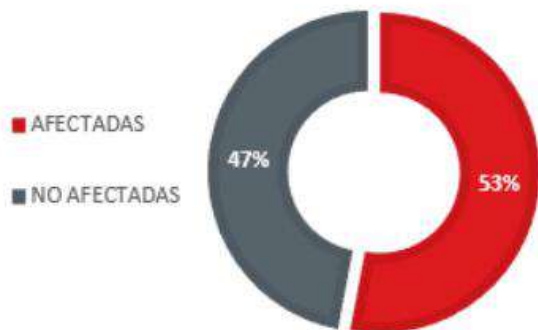
¿sabemos que es imposible que sea cierto?



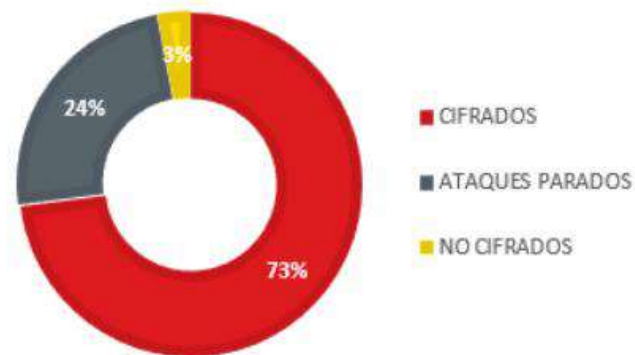


Primer pensamiento ... ¡no puede ser!

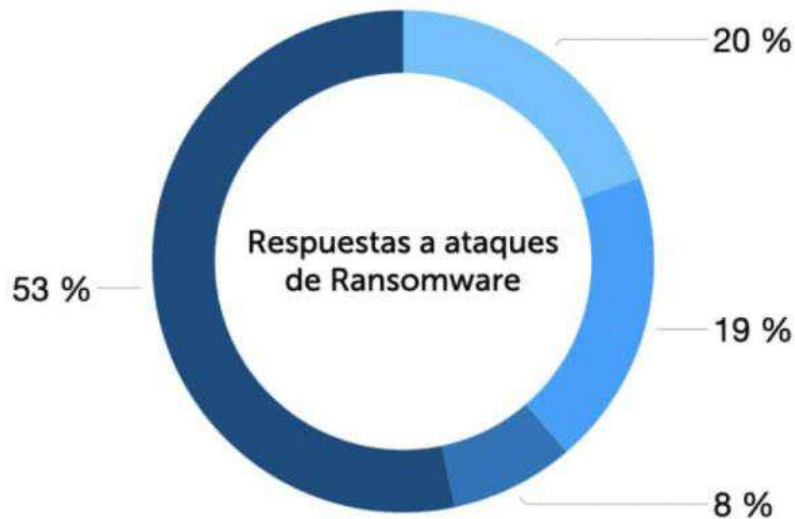
EMPRESAS QUE HAN SUFRIDO UN INCIDENTE DE RANSOMWARE



ÉXITO EN EL CIFRADO DE DATOS DE UN ATAQUE POR RANSOMWARE



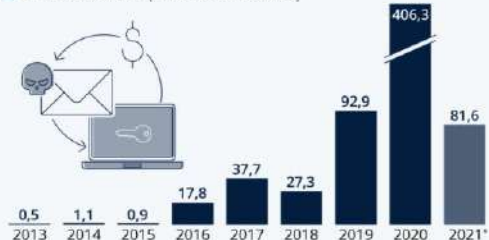
Segundo pensamiento ...



- Pagaron el rescate, pero perdieron los datos.
- Pagaron el rescate y recuperaron los datos.
- No pagaron el rescate y perdieron los datos.
- No pagaron el rescate, pero recuperaron los datos.

Los ataques de ransomware y el pago con criptomonedas

Valor total de las criptomonedas recibidas por direcciones de ransomware (en mill. de dólares)



Criptomonedas Incluidas: Bitcoin Cash, Bitcoin, Ethereum, Tether.

* Hasta el 10 de mayo de 2021.

Fuente: chainalysis.com

Y encima ... no solo pierdo la disponibilidad sino ...



Empezamos a recordar todo lo que hemos implantado



Pero hacer cosas no es gestionar cosas ...

¡La gobernanza IT la base! con el objetivo de elevar los niveles de control y capacitación de los sistema de seguridad IT. Con ello se provoca un **incremento en la madurez de la gestión de la seguridad de la información** en el ecosistema de tu organización.



La maduración de una organización hacia la gobernanza de seguridad IT implica la **plena operacionalización/gestión de los servicios de ciberinteligencia** internos y externos.

Y en muchas ocasiones nos olvidamos ...



Capacidad de Recuperar

Dotar a la organización de planes de resiliencia y recuperación de capacidades y servicios impactados por un evento de seguridad.

- ¿Hicimos un esquema correcto de respaldo?
- ¿Revisamos de verdad el esquema antiguo?
- ¿De verdad?
- ¿De verdad?
- ...

- ¿Realizamos test de recuperaciones parciales, totales?
- ¿Tenemos documentado un BCP?
- ¿Tenemos documentado un IR?
- ¿Tenemos documentado IT sobre impacto de Ransomware?

Hemos ido a muchas charlas ... y nos han martilleado con

SÓLO EL 24% DE LOS ATAQUES SE DETECTAN A TIEMPO

Como sucede en cualquier industria, los delincuentes, con menos costes y más propensos a compartir información entre ellos, van siempre un paso por delante. En esta línea, el responsable de seguridad de Cisco ha destacado como "sólo el 24% de los ataques que recibe una compañía son detectados a tiempo". "En los últimos 10-12 años somos igual de torpes a la hora de reaccionar ante una amenaza", ha añadido.



Compromise



Discover



Recover

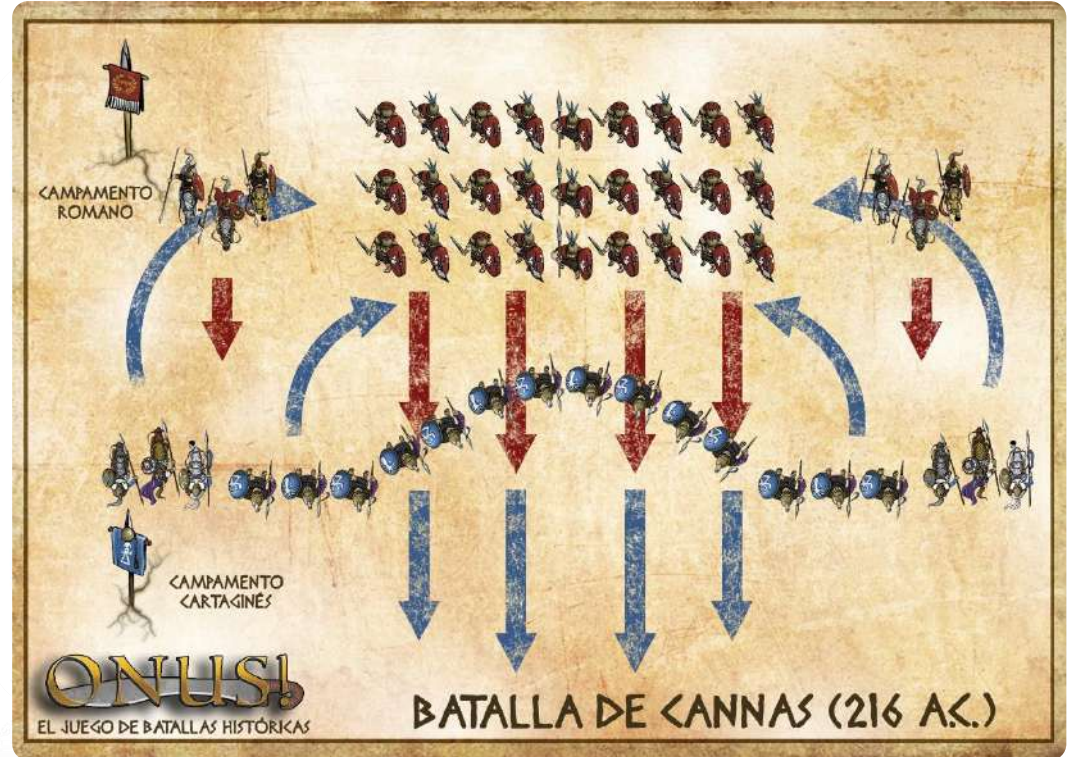


La DETECCIÓN y el TIEMPO
DE RESPUESTA



... y nos han insistido en

Ser **CONSCIENTES** del **RIESGO** y
DISEÑAR una **ESTRATEGIA**



y siempre nos referencian ... NIST

5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

4 RESPOND

Develop a plan for disasters and information security incidents

1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity



3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

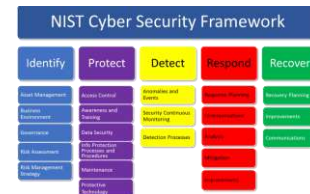
Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees



E incluso ya tiran la toalla y me piden lo básico ... muy básico ☹️

Buenas prácticas para la realización de copias de seguridad



Identificar la información que queremos salvaguardar



Establecer la manera en la que haremos la copia



Almacenar la información cifrada en una ubicación distinta a la principal



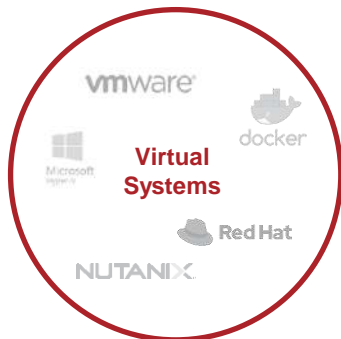
Plan de pruebas periódicas de restauración de copias

... pero si entramos en harina para el servicio de BackUp

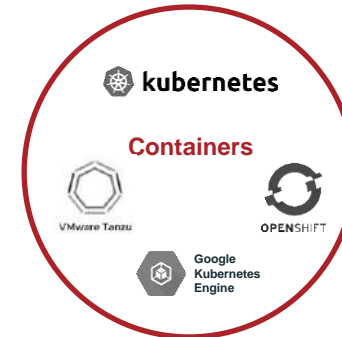
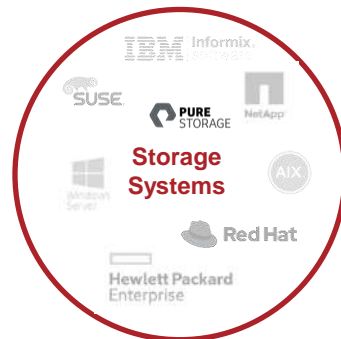
La solución de backup tiene que pivotar sobre varios pilares (al menos):

1. Tiene que **estar bien diseñada** ... no solo por producto, sino por esquema de seguridad (segmentación del servicio, hardening del servicio, etc ...)
2. Tiene que ser **inmutable** frente a ataques de Ransomware. Es frecuente que el propio cifrado de datos, cifre los backups, y esto puede ser un desastre porque perdemos nuestros backups más cercanos y como mucho podremos tirar de los backups más lejanos (si los tenemos) y probablemente en dispositivos y tecnología con más lentitud y con la pérdida de datos (RPO) que conlleva.
3. Una solución **pensada para restaurar en tiempo y forma**. Restaurar ficheros o restores normales no nos vale en caso de un ataque de Ransomware. Granularidad, velocidad, etc ... son claves.





NetBackup Unmatched Flexibility



The background features a dark blue hexagonal grid pattern. Several hexagons contain a white padlock icon, symbolizing security or data protection. The grid is composed of thin white lines connecting the vertices of the hexagons.

alhambra

VERITAS™

www.alhambraIT.com | www.veritas.com



Inmunidad Contra Ransomware

Santiago Sánchez
System Engineer | Veritas



Who Are We

15x

A LEADER IN GARTNER'S MQ
FOR DATA CENTER BACKUP
AND RECOVERY SOLUTIONS



#1

MARKET SHARE FOR BACKUP
AND RECOVERY SOFTWARE

6,000+



Employees
Worldwide

20,000+



Global
Partners

80,000+



Global
Customers

2,000+



Developers
Worldwide

2,140+



Global
Patents

800+



Supported
Workloads

380+PB



Driven AWS
Consumption

100+EB



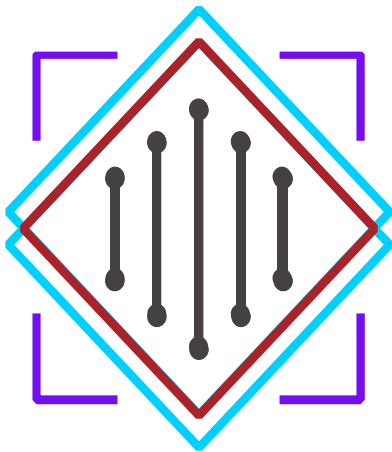
Data Under
Management

87%



Fortune Global 500
Trust Us

Our portfolio



VERITAS™

ENTERPRISE DATA SERVICES

P L A T F O R M



AVAILABILITY



PROTECTION



INSIGHTS

Traditional Data Challenges



Cloud

92% of organizations' strategy involves a transition to cloud, and over 1/3 note migration complexity is a challenge



Costs

By 2020, IDC estimates we'll see 44 zettabyte (10^{21}), causing an increase in storage demand and cost



Big data

By 2020, IDC estimates 37% of data will deliver value if analysed, resulting in an \$430B in productivity gains.



Compliance

Gartner estimates that more than 80 % of enterprise data is unstructured and likely to contain personally identifiable information (PII)



Business continuity

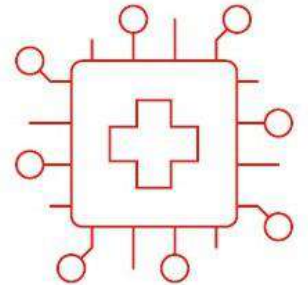
According to a research report by the Ponemon Institute, a data centre outage costs around \$9,000 per minute.

NEW Data challenges



Ransomware now commonplace

Around one-in-six of those attacked was hit with a ransom and more than half (58%) paid up.



It's no longer a question of IF but WHEN

Every

11 seconds

an organization is hit by a Ransomware attack

USD1.85M

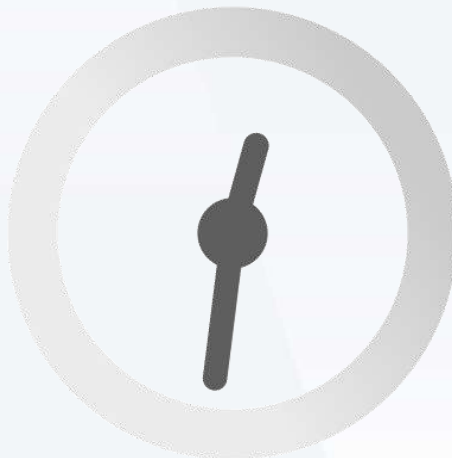
average cost (people, process, technology) of Ransomware

42%

of organizations have been hit by Ransomware

20%

company data would be unrecoverable in the event of a complete data loss



Email attacks remain **#1** delivery method

1 in 10

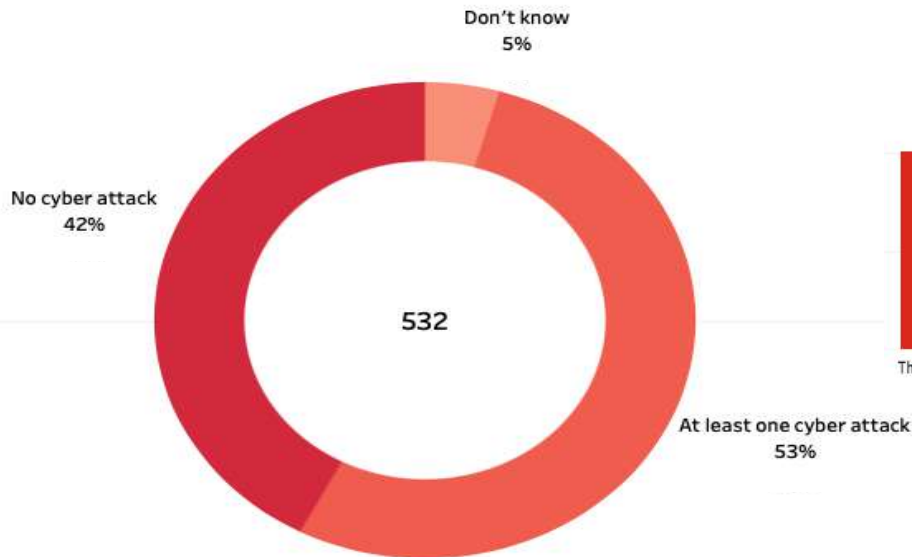
organizations unable to recover

64%

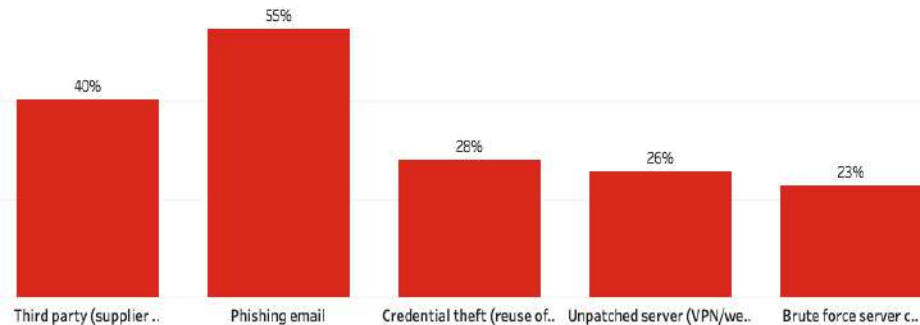
of organizations have not kept up with security measures.

Ransomware

Spain Cyber Attacks 2021



Spain Methods entry Ransomware



El 'ransomware' fue la amenaza más detectada del globo en el último trimestre

Ransomware Challenges Articulated by Customers

How can I reduce the chance an attack is successful?

Things to think about:

- Malware already present
- 35%¹ of data is dark
- 39%² feel security hasn't kept up in last 12 months

If an attack is successful, how can I limit any disruptions?

Things to think about:

- Hackers target backups
- Downtime: \$2.3M/hr³
- 38%² report being down for a week or longer

How do I know I am recovering from clean data?

Thing to think about:

- DDoS + ransomware
- Days-weeks-months of dormancy before attack
- 60%² pay ransoms

Solved by a multi-layered strategy based on best practices

What is The Zero Trust Security Model?

Not trusting any devices—or users—by default, even if they're inside the corporate network.

! **Institute Identity and Access Management (IAM)**

controls (for both users and machines)

- Multi-Factor Authentication (MFA)
- Role-Based Access Control (RBAC)

! **Encrypt data** both in-flight and at-rest to reduce data exfiltration leverage (use data loss prevention software).

! **Limit access to backups** (no one with access to primary data should also have access to backups).

! **Implement security analytics** to monitor for and mitigate malicious activity.

“

Zero Trust... is useful as a shorthand way of describing an approach where implicit trust is removed from all computing infrastructure. Instead, trust levels are explicitly and continuously calculated and adapted to allow **just-in-time, just-enough-access** to enterprise resources.”

Neil MacDonald

VP Analyst, Gartner

Protect all data from all sources

Detect threats as well as signs of threats

Recover to anywhere from anywhere



New standards and certifications

Procurement requirements

- FAR/DFARS compliance
- Section 508 VPAT compliance
- Foreign Ownership, Control or Influence compliance
- Trade Agreements Act compliance

Operational requirements and/or certification programs

- DISA STIG compliance
- AWS GovCloud, AWS C2S, Azure Government Cloud
- NIST SP 800-53, NIST SP800-37 RMF, ICD 503, NIST 800-171
- FIPS 140-2 level 1 validated
- Suppliers Declaration of Conformity for IPv6/USGv6
- Energy Star Certified
- Verified U.S. Support
- Common Criteria certified
- DSCA Agreement
- Multi-Factor Authentication



A Multi-Layered Approach based on Zero-trust

1



Protect

- ✓ Support more enterprise workloads than any other
- ✓ Bullet-proof intrusion prevention
- ✓ Industry-leading immutable storage options

2



Detect

- ✓ Cost-efficient malware scanning
- ✓ Near real-time, AI-based anomaly detection
- ✓ Total infrastructure visibility edge to core to cloud

3

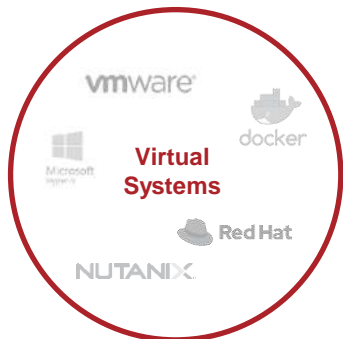


Recover

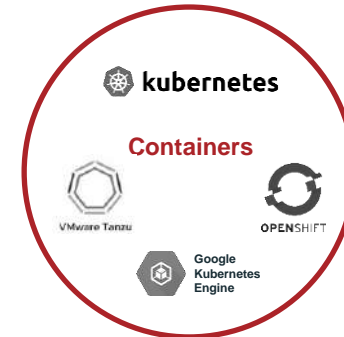
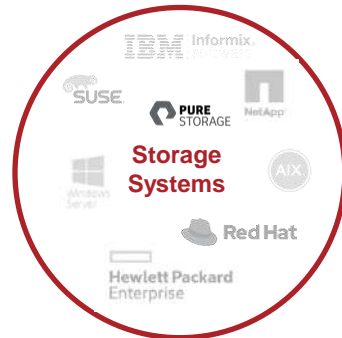
- ✓ Automated recovery orchestration to anywhere, cloud & bare metal
- ✓ Non-disruptive recovery testing
- ✓ Instant access recovery and roll-back

STEP 1:
Protect





NetBackup Unmatched Flexibility



How Veritas Safeguards Your Data



Appliances

APPLIANCE STRATEGY



Scalability

Scale with data growth.



Resiliency

Enhance resiliency and performance.



Simplicity

Converged solutions for complex data management problems.



Efficiency

Deliver operational efficiency and insight.



AGILE.
SCALABLE.
INTEGRATED.

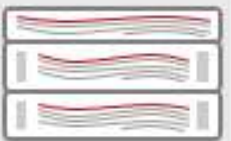


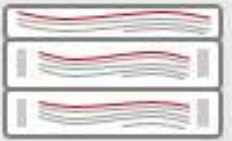


Simplify enterprise data
management with NetBackup
Appliance solutions.

Security Features in NetBackup Appliance

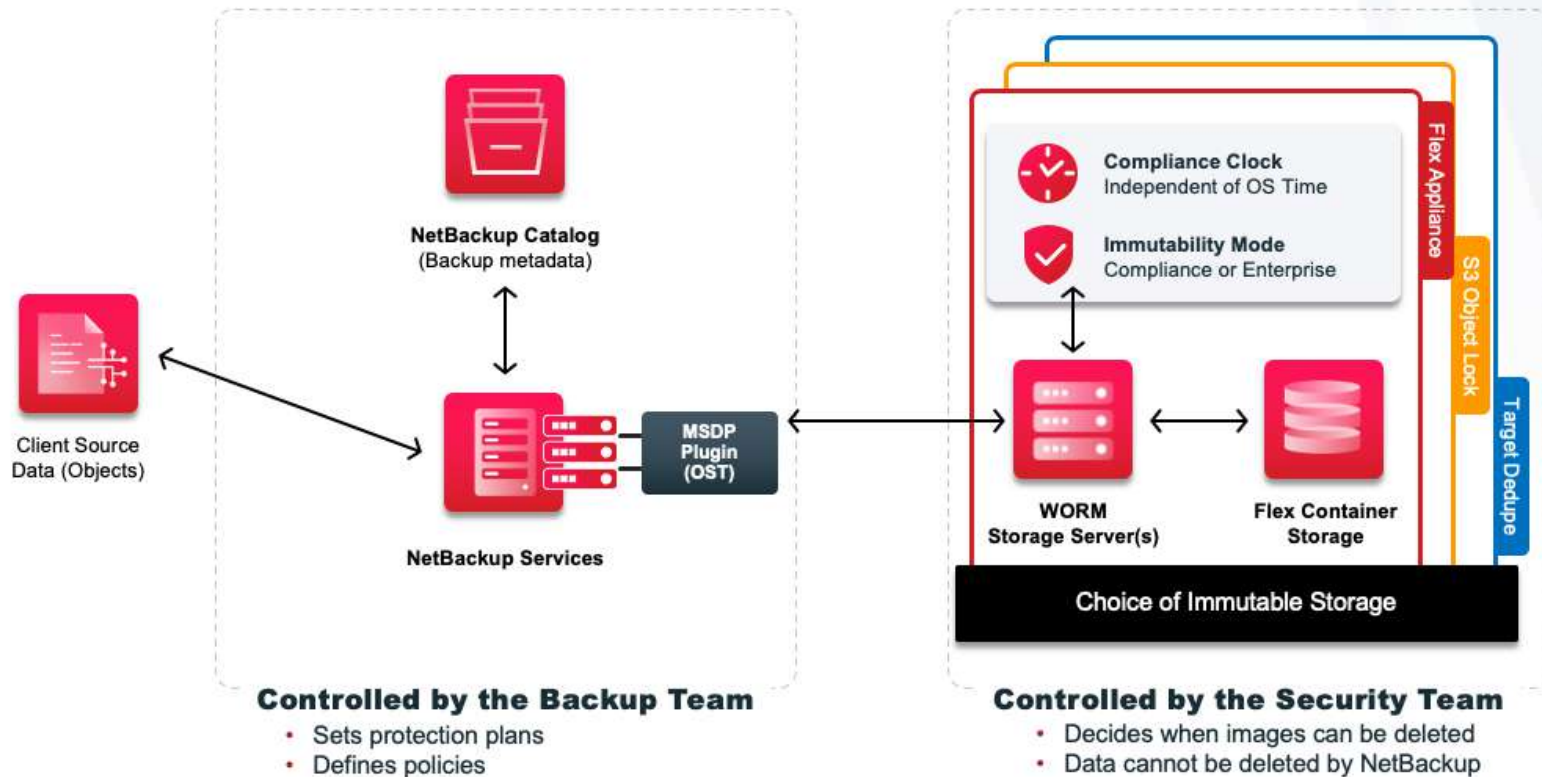
New NetBackup Appliance Security Features

DISA STIG	FIPS 140-2	RBAC	IPv6	Firewall	SDCS
 <p>DISA</p> <p>STIG</p> <p>Security Technical Implementation Guides</p>	 <p>FIPS 140-2</p> <p>Federal Information Processing Standard</p>	 <p>Role Based Access Control</p>	 <p>IPv6 READY</p> <p>IPv6 Support</p>	 <p>Control incoming and outgoing network traffic</p>	 <p>Symantec Data Center Security</p>
<p>System Hardening</p>	<p>Cryptographic- Based Security</p>	<p>Access Control</p>	<p>Communication s Protocol</p>	<p>Network Security</p>	<p>IDS/IPS</p>

Appliances family

NetBackup 5250 Appliance	NetBackup 5350 Appliance	Flex 5150 Appliance	Flex 5250 Appliance	Flex 5350 Appliance	Access 3340 Appliance
					
<ul style="list-style-type: none"> ✓ Master or Master/Media ✓ 429 TiB maximum storage 	<ul style="list-style-type: none"> ✓ High performance Media Server ✓ 1,920 TiB maximum storage 	<ul style="list-style-type: none"> ✓ Simplified appliance solution ✓ Cost-effective design ✓ Smaller workloads 	<ul style="list-style-type: none"> ✓ Flexibility and agility ✓ <u>Inmutable Storage</u> ✓ Multiple NetBackup roles on one appliance 	<ul style="list-style-type: none"> ✓ Long-term data retention ✓ 2,544 TiB maximum storage 	
<p>POSITIONING SUMMARY: Predictable high-performance data protection for moderate workloads.</p>	<p>POSITIONING SUMMARY: Predictable highest performance data protection for enterprise workloads.</p>	<p>POSITIONING SUMMARY: Streamlined protection for remote or branch office locations.</p>	<p>POSITIONING SUMMARY: Predictable high-performance data protection for moderate workloads.</p>	<p>POSITIONING SUMMARY: Run multiple Veritas software products on a single, flexible, converged solution.</p>	<p>POSITIONING SUMMARY: Long-term data storage and archiving as tape and public cloud alternative.</p>

Inmutable Storage



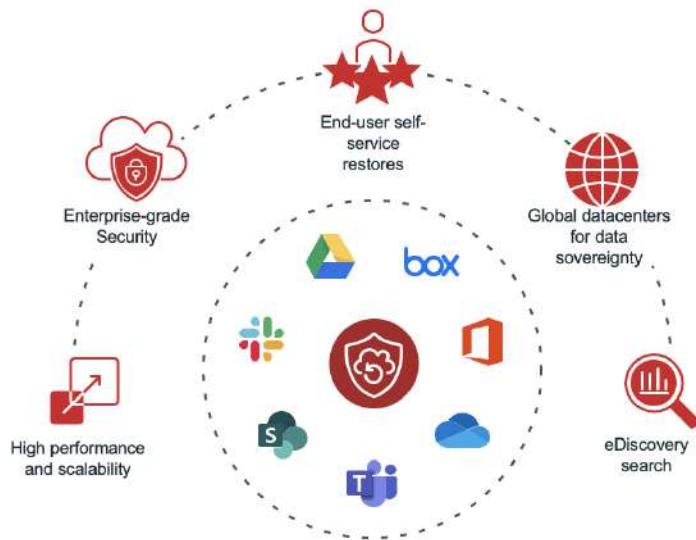
Controlled by the Backup Team

- Sets protection plans
- Defines policies

Controlled by the Security Team

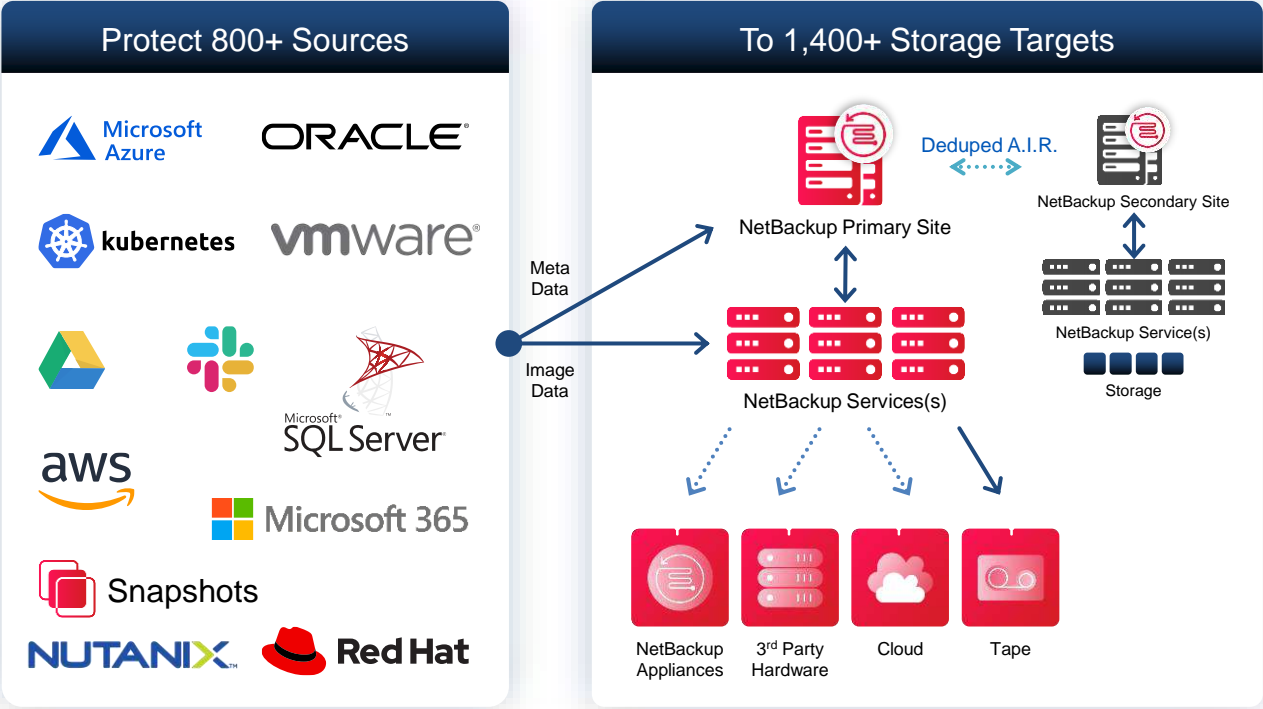
- Decides when images can be deleted
- Data cannot be deleted by NetBackup

SaaS platforms



- **Automatic data protection** for new users, mailboxes, and folders requires no action on your part
- **Time and bandwidth savings** from copying only data that has changed since the last backup
- **Flexible restore options** whether to its original location or to an alternate location of your choice
- **Granular restore** of a single file, email message, or Teams chat – or a select group of objects. NetBackup SaaS Protection also supports bulk restores

Step 1: Protect



= Immutable/Encrypted Storage

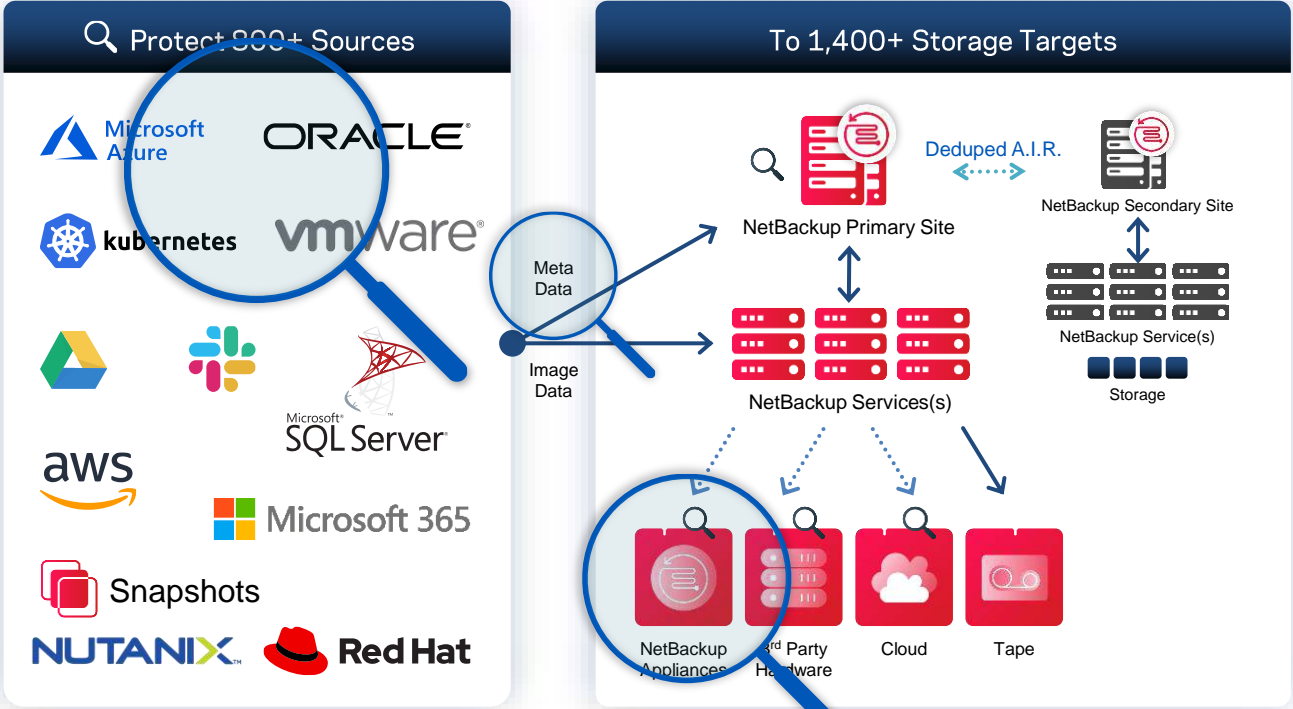
= Detection Capabilities

.....> = Dedupe



STEP 2:
Detect

Step 2: Detect



= Immutable/Encrypted Storage

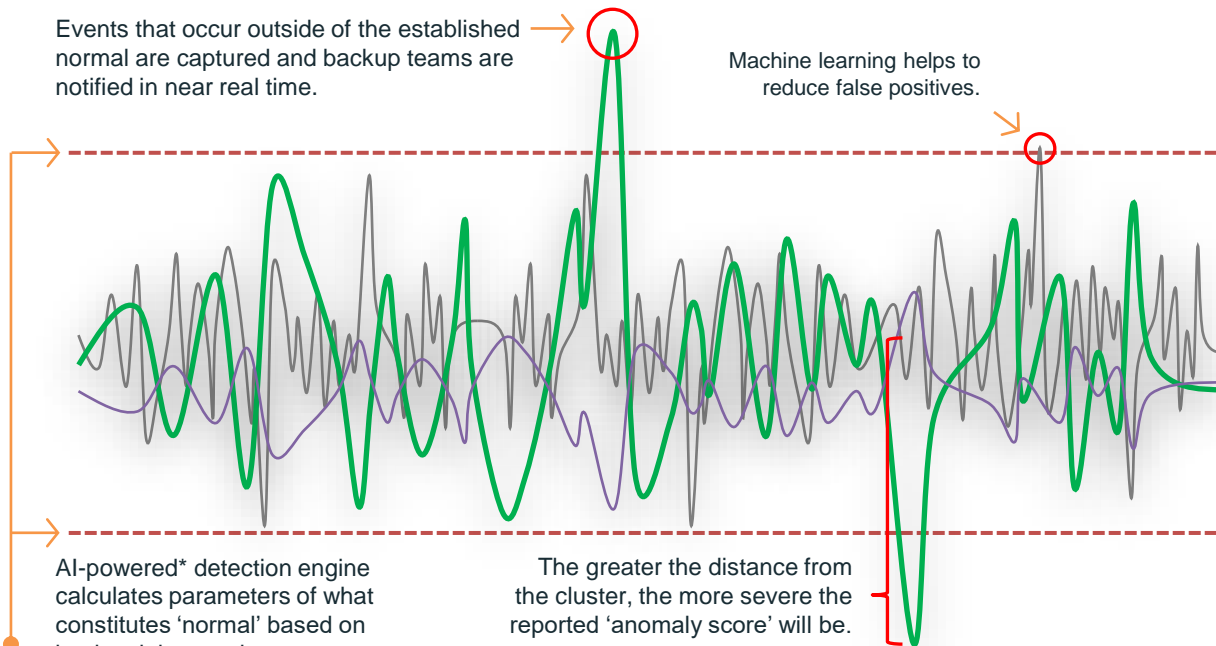
= Detection Capabilities

.....> = Dedupe

Understanding Anomaly Detection

Events that occur outside of the established normal are captured and backup teams are notified in near real time.

Machine learning helps to reduce false positives.



AI-powered* detection engine calculates parameters of what constitutes 'normal' based on backup job metadata patterns over time and auto-adjusts for custom backup policies.

The greater the distance from the cluster, the more severe the reported 'anomaly score' will be.

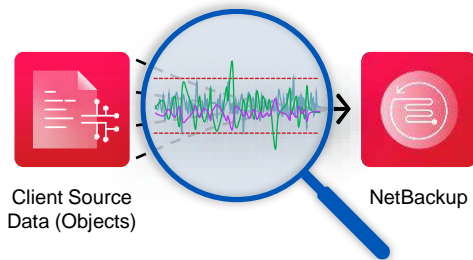
AI-Powered Anomaly Detection Engine in NetBackup

- Mine enormous amounts of data
- Automate monitoring and reporting
- Gain actionable insights
- Report based on several criteria
- Establish early warning of an attack

* Machine learning model takes advantage of data pre-seeding using nbdeployutil. AI is powered by DBSCAN algorithm.

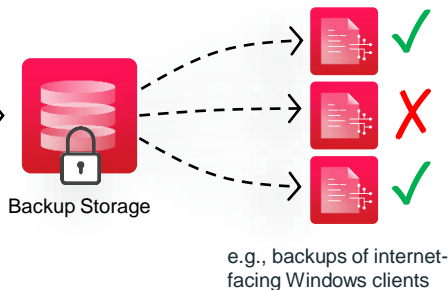
High-Level Overview of Malware Detection in NetBackup

During Backup



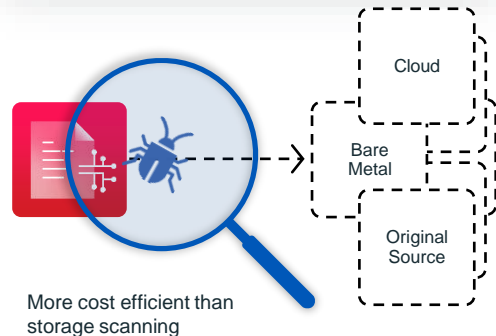
Anomaly detection in near real-time

Post Backup



Spot-checking of known high-risk areas

Before Restore



Scanning before restore to ensure clean data

Advance Your Risk Intelligence with Machine Learning

Predict an Information Crisis **Before** it Occurs

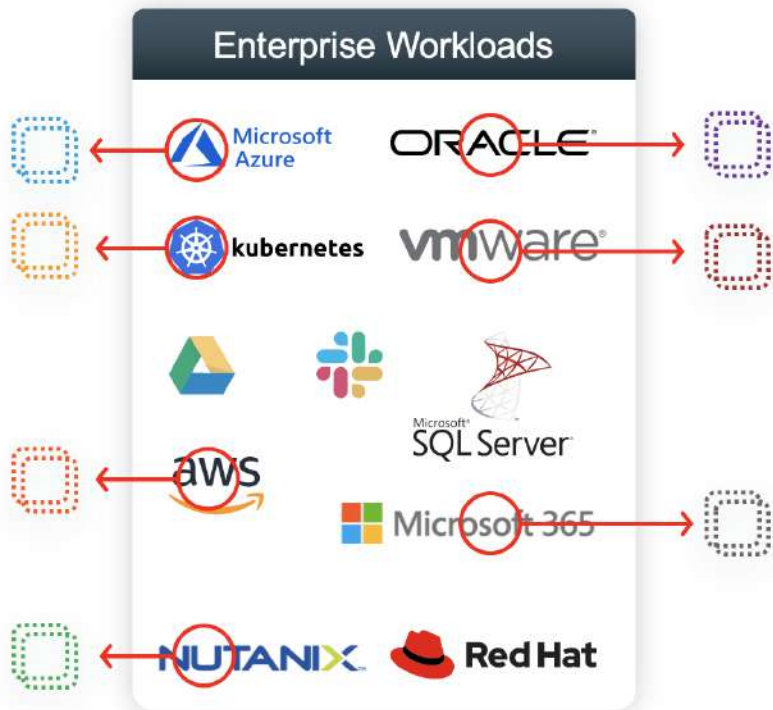
- Scans, audits, detects and alerts on ransomware
- Reviews impacted files and compromised accounts with built-in ransomware templates
- Locks down suspicious accounts and restores data

The screenshot displays the Veritas Data Insight web interface. The main navigation bar includes 'Workspace', 'Policies', 'Reports', 'Workflows', and 'Settings'. The left sidebar shows a list of policies, with 'User Activity Deviation Policy' selected and highlighted in yellow. The main content area is titled 'Create: User Activity Deviation Policy' and contains several tabs: 'Policy Information', 'Configure Policy', 'Data Selection', 'User Selection', and 'User attribute query'. The 'Configure Policy' tab is active, showing configuration options for the policy. The text reads: 'Select the options below to configure User Activity Deviation Policy'. Under 'Time range:', it says 'Select time range for weekly baseline: Last 4 weeks'. Under 'Threshold Configuration:', it says 'Allowed activity deviation: 3 times of standard deviation'. Under 'Additional Condition:', it says 'Alert only if accesses per day per user on selected data set exceed: 100'.

STEP 3:
Recover



Optimizing for Recovery, Not just Backup



Copy of important data? ✓

Optimized recovery experience? ✗

Multiple disparate backup solutions by design create a **complicated recovery experience**—especially when multiple systems are compromised.

Additional considerations:

- Skills/training gaps
- Lost storage dedupe efficiencies
- No global data visibility/oversight

Support for RPO & RTO Requirements

- NetBackup Resiliency
- NetBackup Instant Rollback for VMware
- Continuous Data Protection (CDP) for VMware
- Instant Access: VM and SQL
- Cloud and On-Premise Snapshots
- Bare Metal Recovery (BMR)
- Traditional Recovery

The screenshot displays the Veritas NetBackup VMware interface. On the left is a navigation sidebar with options like Dashboard, Jobs, VMware, Cloud, Protection Plans, Security, RBAC, Certificates, Security Events, Hours, Tokens, and Usage. The main area shows a table of virtual machines under the 'VMware' section.

Virtual machine	Server	Protected by	Last discovered	Status
win2k16-test VMware_3618056B-853D-6c18-5746-1...	minkon-vm096.engiza.veritas.com	VM Group Protection Plan	September 10, 2018 3:24 PM	
Tiny-Linux VMware_36180610-7943-c136-a224-e4...	minkon-vm096.engiza.veritas.com	Not protected	September 10, 2018 3:24 PM	
dotNetTestVM-8 VMware_361809127-3019-33a0-5826-e...	minkon-vm096.engiza.veritas.com	VM Group Protection Plan	September 10, 2018 3:24 PM	Today at 6:02 PM ✓
Tiny-Linux-personal-test VMware_36180a072-ad10-4f03-c2a8-91...	minkon-vm096.engiza.veritas.com	VM Group Protection Plan	September 10, 2018 3:24 PM	Today at 6:02 PM ✓
Tiny-Linux-9gittest VMware_36180b64-432a-8533-2e40-8...	minkon-vm096.engiza.veritas.com	VM Group Protection Plan	September 10, 2018 3:24 PM	Today at 6:01 PM ✓
win-eg VMware_36180c5a-2560-ba7a-5a24-8f...	minkon-vm096.engiza.veritas.com	Not protected	September 10, 2018 3:24 PM	
my clients25 VMware_36180e61-852a-6ca5-c0ab-0f...	minkon-vm096.engiza.veritas.com	Single VM Protection Plan	September 10, 2018 3:24 PM	Today at 6:00 PM ✓
fbactestvm-8 VMware_36180f61-852a-6ca5-c0ab-0f...	minkon-vm096.engiza.veritas.com	VM Group Protection Plan	September 10, 2018 3:24 PM	Today at 6:03 PM ✓
VM3D SwrSA) %2502 Le_p-1 (h... VMware_36180961-49f5-1803-0a81-e9...	minkon-vm096.engiza.veritas.com	Not protected	September 10, 2018 3:24 PM	
test123-win-%2502-%2503-%1f-%... VMware_36180913-4d17-e814-8a48-ea...	minkon-vm096.engiza.veritas.com	VM Group Protection Plan	September 10, 2018 3:24 PM	Today at 6:03 PM ✓
AdiTestVM-DoNotTouchThis VMware_36180a072-ad10-4f03-c2a8-92b...	minkon-vm096.engiza.veritas.com	Not protected	September 10, 2018 3:24 PM	
redhat6.6-ai_test_Phoenix_copy VMware_36180964-554b-8106-1c76-c...	minkon-vm096.engiza.veritas.com	VM Group Protection Plan	September 10, 2018 3:24 PM	
Prodactio-Test VMware_36180a072-ad10-4f03-c2a8-92b...	minkon-vm096.engiza.veritas.com	Not protected	September 10, 2018 3:24 PM	
vCenter5.5 (minkon-vm069) VMware_36180a072-ad10-4f03-c2a8-92b...	minkon-vm096.engiza.veritas.com	Not protected	September 10, 2018 3:24 PM	
VeritasLabe01-01 VMware_36180a072-ad10-4f03-c2a8-92b...	minkon-vm096.engiza.veritas.com	Not protected	September 10, 2018 3:24 PM	
VeritasLabe01-01 VMware_36180a072-ad10-4f03-c2a8-92b...	minkon-vm096.engiza.veritas.com	Not protected	September 10, 2018 3:24 PM	

Your Plan is Only as Good as Your Last Test!

57%

of organizations haven't tested their DR plans within the last two months.¹

Don't be them.

¹ Source: Ransomware Resiliency Report, Veritas, 2020

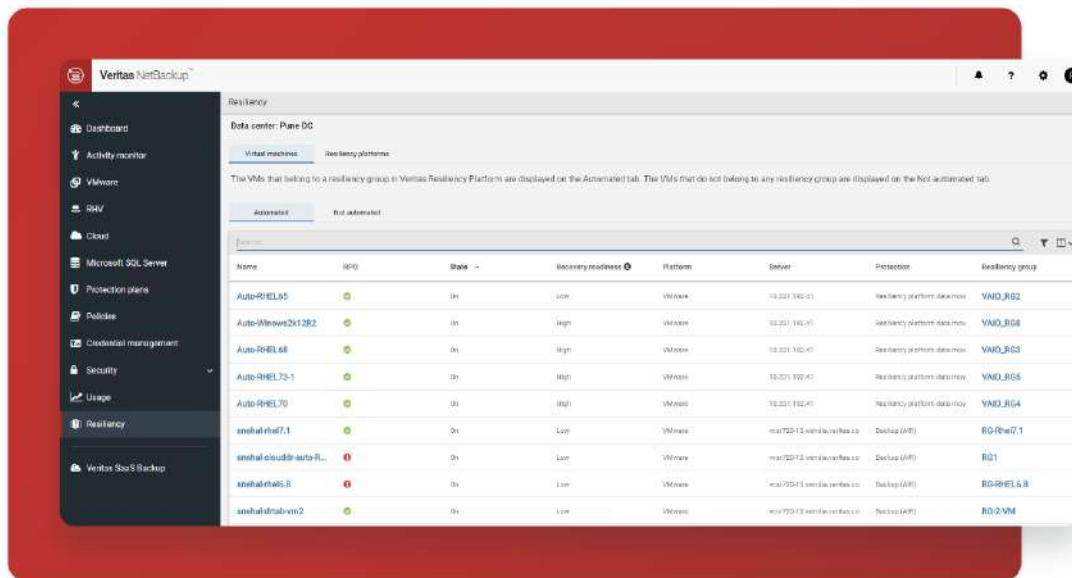
Veritas can help you:

- Set up one-click, non disrupted disaster recovery testing
- Create an immutable data vault (IDV)
- Effectively utilize an isolated recovery environment (IRE)
- Ensure confidence that ransomware **recovery will be successful** when it counts

Veritas had a 100% recovery success rate for customers that were hit by a ransomware attack in 2020.

Tracking toward a repeat in 2021!

Automated Recovery Orchestration



The screenshot displays the Veritas NetBackup Resiliency interface. The left sidebar contains navigation options: Dashboard, Activity monitor, VMware, RSHV, Cloud, Microsoft SQL Server, Protection plans, Policies, Credential management, Security, Usage, Resiliency, and Veritas SaaS Backup. The main content area is titled 'Resiliency' and shows 'Data center: Plane DC'. It includes tabs for 'Virtual machines' and 'Resiliency platforms'. A text block states: 'The VMs that belong to a resiliency group in Veritas Resiliency Platform are displayed on the Automated tab. The VMs that do not belong to any resiliency group are displayed on the Not automated tab.' Below this, there are two tabs: 'Automated' (selected) and 'Not automated'. A table lists the VMs with columns for Name, RPO, State, Recovery readiness, Platform, Server, Protection, and Resiliency group.

Name	RPO	State	Recovery readiness	Platform	Server	Protection	Resiliency group
Auto-RHEL65	0h	On	Low	Windows	10.221.142.41	Resiliency platform data-mov	VM0_RIS2
Auto-Windows2k12R2	0h	On	High	Windows	10.221.142.41	Resiliency platform data-mov	VM0_RIS6
Auto-RHEL68	0h	On	High	Windows	10.221.142.41	Resiliency platform data-mov	VM0_RIS3
Auto-RHEL73-1	0h	On	High	Windows	10.221.142.41	Resiliency platform data-mov	VM0_RIS5
Auto-RHEL70	0h	On	High	Windows	10.221.142.41	Resiliency platform data-mov	VM0_RIS4
smhahel7.1	0h	On	Low	Windows	msr72013.msrfa.veritas.co	Backup (APR)	RD-Rhel7.1
smhahelcud@-acta-RL	0h	On	Low	Windows	msr72013.msrfa.veritas.co	Backup (APR)	RD1
smhahel6.8	0h	On	Low	Windows	msr72013.msrfa.veritas.co	Backup (APR)	RD-RHEL & R
smhahelrdbvm2	0h	On	Low	Windows	msr72013.msrfa.veritas.co	Backup (APR)	RD-2-VM

NetBackup Resiliency

- Automation and orchestration
- Full RPO coverage
- Test, Validate, Disinfect

“With NetBackup, we can restore lost data from backups with a success rate of 100%.”
– Large European Hospital

Recap: Achieving Ransomware Immunity

What customers want to know:

La seguridad digital es como preparar una buena comida ...

How do I know I am recovering from clean data?

Best practices to ensure desired outcomes:

- ✓ **UP** Don't
 - ✓ **AL** Keep
 - ✓ **AC** App
 - ✓ **OR** Lim
 - ✓ **UN** Detect anomalies and malware across data and infrastructure.
- ... Precisas conocer la receta, disponer de los ingredientes adecuados y tener buena práctica !!!**

The background features a repeating pattern of hexagons. Each hexagon contains a small, light-colored padlock icon. The hexagons are arranged in a grid, with some appearing slightly more prominent than others, creating a subtle depth effect.

alhambra

VERITAS™

www.alhambraIT.com | www.veritas.com

alhambra
leave IT in our hands

VERITAS™

OneseQ by Alhambra IT

OneseQ
by alhambra

Jose María Ochoa
Area Manager | OneseQ





leave IT in our hands

Hemos unido dos mundos desde la BASE

Especialista en IT
Integración de
sistemas,
comunicaciones,
desarrollo, formación,
etc ...
Más de 30 años

Ciberseguridad

OneseQ
by alhambra

Hemos puesto el SOC en el centro de los servicios



Para un IR hay dos conceptos CLAVE

Incident Response (IR)
CSIRT

Threat Hunting

El propio concepto de Incident Response

Incident Response (IR) CSIRT

Un **IR** permite atender la incidencia lo antes posible, conteniendo los daños para que no se extiendan, y aplicando las soluciones casi de forma inmediata. Para ello **es muy conveniente contar con un Equipo de Respuesta**, también denominado *Computer Security Incident Response Team*, o **CSIRT**. No obstante, la confección del plan requiere de un **equipo de IT maduro y experimentado**, lo que no excluye que se deba preparar desde el primer momento.

Nuestra ventaja

Incident Response
(IR)
CSIRT

Miembros del equipo de respuesta a incidentes

En esencia, un equipo de respuesta a incidentes debe estar formado por:

- **Coordinador de respuesta a incidentes:** El administrador de respuesta a incidentes supervisa y prioriza las acciones durante la detección, análisis y contención de un incidente. También son responsables de transmitir los requisitos especiales de los incidentes de alta gravedad al resto de la empresa.
- **Analistas de seguridad:** el administrador cuenta con el respaldo de un equipo de analistas de seguridad que trabajan directamente con la red afectada para investigar la hora, la ubicación y los detalles de un incidente. Hay dos tipos de analistas:
 - Analistas de Triage: Filtre los falsos positivos y observe posibles intrusiones.
 - Analistas forenses: recupere los artefactos clave y mantenga la integridad de la evidencia para garantizar una investigación forense sólida.
- **Investigadores de amenazas:** los investigadores de amenazas complementan a los analistas de seguridad al proporcionar inteligencia y contexto de amenazas para un incidente.
- **Técnicos multidisciplinares:** Es imprescindible conocimiento y soporte de ingeniería de todos los sistemas implicados en la arquitectura IT de la compañía.

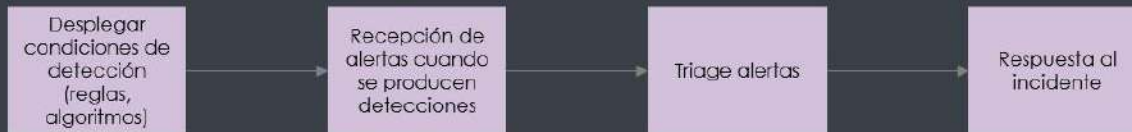
El otro concepto importantísimo

Alerta Temprana

Threat Hunting

Diferencias según Gartner

Threat Detection



Threat Hunting



Gartner 2017 How to Hunt for Security Threats.
Anton Chuvakin, 6 April 2017. ID: G00327290.

Y una despliegue global | generación de CONOCIMIENTO



RED de SOC



SOC Propios y socios

Madrid

Brasil

Santa Cruz de Tenerife



SOC Colaboradores

Barcelona

Chile

Casa Blanca (Marruecos)

Dubai (Emiratos Árabes)

Riyadh (Arabia Saudí)



Y con una red de conocimiento | generación de VALOR



Objetivos

Desde la creación de **OneseQ** se marca como objetivo y valor complementario, la incorporación de la colaboración con centros y fuentes exteriores de información de cibervigilancia y cooperación entre SOC's mediante la generación de estrechas alianzas con un partner estratégico adicional con implantación de SOC, que brinda su apoyo y coordinación de los centros de operaciones internacionales, aportando visibilidad y fuentes de datos en todo el tránsito del servicio de alerta temprana de incidentes.



Colaboraciones

INCIBE
CCN
FIRST
APWG
ISMFORUM
APTAN



Acreditaciones



Con mucho que aportar | OneseQ

¿Qué valor aportamos desde el SOC de OneseQ?

- > El servicio de nuestro SOC se basa en **tecnologías que ayudan a gestionar grandes cantidades de datos** e interpretarlos como eventos o incidentes de seguridad
- > Es operado por **personal muy cualificado** en servicios de ciberseguridad
- > **Múltiples SOC**s en distintas zonas geográficas (**implantación internacional**)
- > Nuestros SOCs además operan y **colaboran compartiendo información con otros SOC**s
- > Al ser operadores virtuales de comunicaciones, OneseQ posee un **NOC (Network Operation Center)** con una experiencia de más de **20 años**
- > Operado con tecnología **multi-SIEM y macro-correlación sobre tecnología cloud** que se ofrece en modo SaaS y tarificado por EPS (Eventos Por Segundo)
- > Tenemos las **máximas acreditaciones** en buenas prácticas y seguridad IT

The background features a dark blue hexagonal grid pattern. Several hexagons within the grid contain a white padlock icon, symbolizing security or data protection.

alhambra

VERITAS™

www.alhambraIT.com | www.veritas.com



Alhambra IT y Veritas

Julio Saíz
Business Developer Manager | Alhambra IT



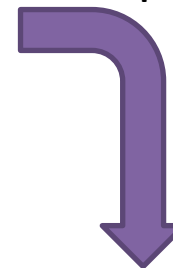
Alhambra IT como partner de Veritas



ACREDITACIONES EN VERITAS	
VSE	71
APTARE IT Analytics	7
Veritas Access 7.4	7
Veritas Backup Exec 21	6
Veritas Data Insight 6.1	7
Veritas eDiscovery Platform 9.0	7
Veritas Enterprise Vault.cloud	7
Veritas Flex Appliance 2.0	2
Veritas Fundamentals	7
Veritas Merge1	7
Veritas NetBackup Appliance 3.x	7
Veritas NetBackup SaaS Protection	7
VSE+	36
APTARE IT Analytics	8
Veritas Access 7.4	6
Veritas Backup Exec 20.4	7
Veritas eDiscovery Platform 9.0	2
Veritas Enterprise Vault.cloud	7
Veritas NetBackup Appliance 3.x	6



En proceso



<https://netbackupguru.es/netbackup-immutable-storage/>

Alhambra IT como cliente de Veritas

alhambra
leave IT in our hands

alhambra
cloud



Madrid-1 | Madrid-2 | París | Miami

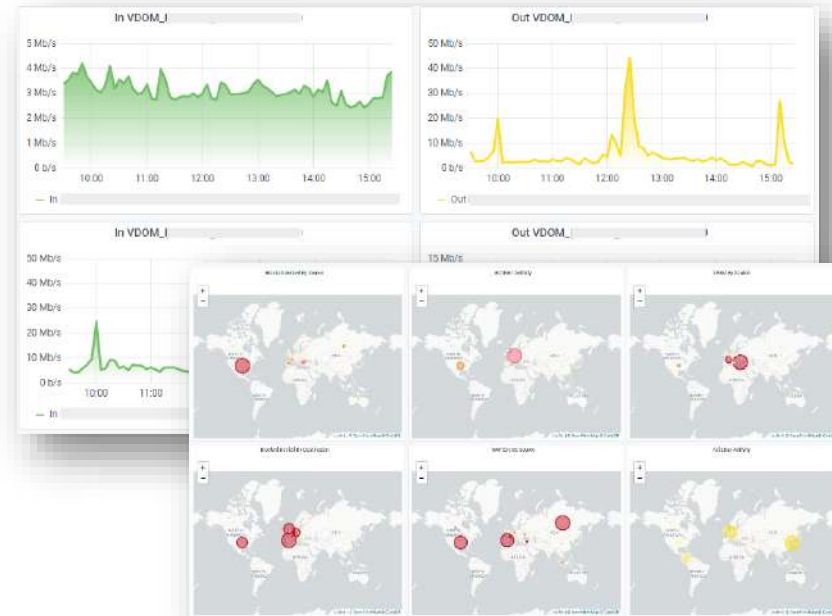


Cloud dedicado y diseñado para el mundo empresarial Empresa a Empresa

VERITAS

Equipo Técnico

AlhambraIT dispone de un centro NOC/SOC 24x7 y Servicios Profesionales, con especializaciones certificadas y amplia experiencia en consultoría, integración y mantenimientos de soluciones tecnológicas.



Alhambra IT como proveedor de servicios gestionados

Servicio de Backup

Servicio de Repositorio Offsite

Servicio de Replicación

Servicio de Disaster Recovery

Servicios MultiCloud

The background features a repeating pattern of hexagons. Each hexagon contains a small, light-colored padlock icon. The hexagons are arranged in a grid, with some appearing slightly more prominent than others, creating a subtle depth effect. The overall color palette is a range of blues, from light to dark.

alhambra

VERITAS™

www.alhambraIT.com | www.veritas.com

alhambra



VERITAS