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, viedos, databases an 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 waster your time.Nobody can recover your files without our decrytionservice

Can I Recover My Files?

Sure. We garantee that you can recover all your flies 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 month.

How Do I Pay?

Payment is accepted in Bitcoin only. Go online for more information.
Please check the current price of Bitcoin an 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 DecrytionCode.

Send 0.5 Bitcoin to

bitcoin ACCEPTED HERE

bitcoin ACCEPTED HERE

Insert DecryptionCode here

DECRYPT

¿Estamos preparados para prevenirlo?

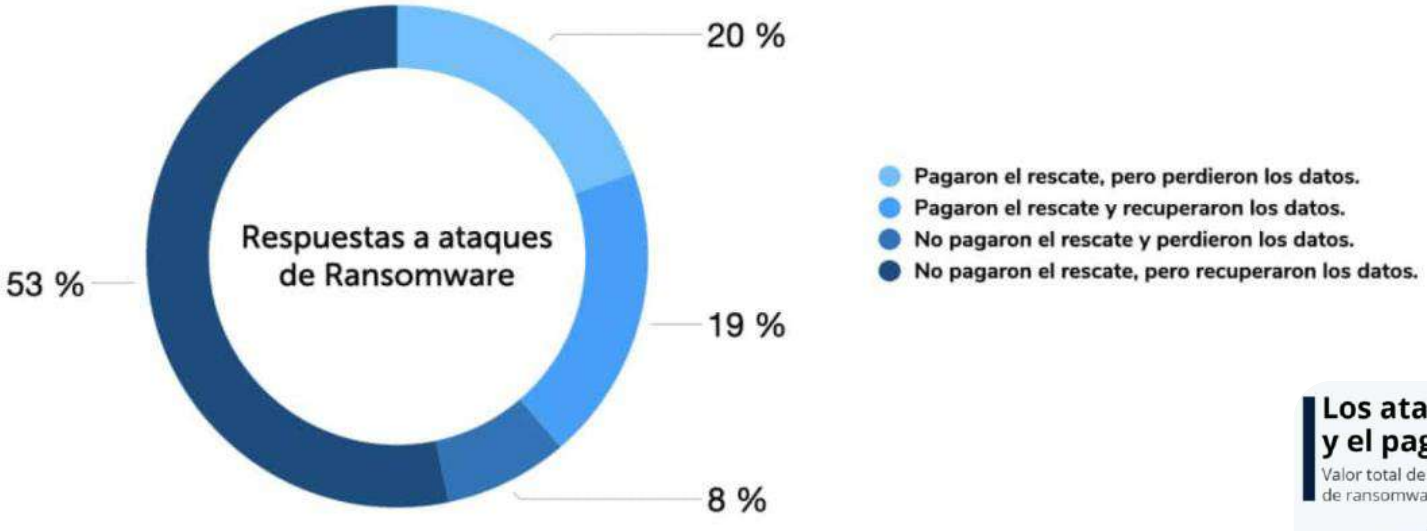
¿estamos preparados para detectarlo?

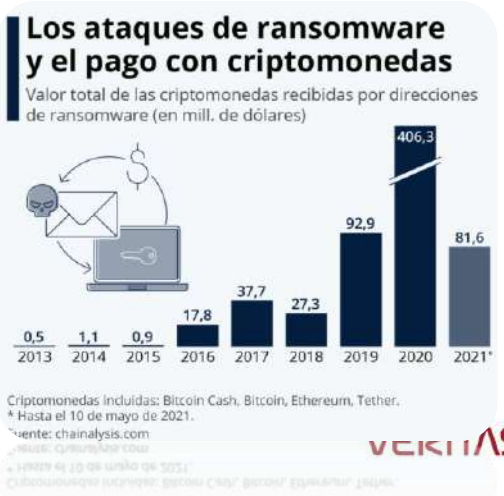
¿Estamos preparados para responder?

¿sabemos que es imposible que sea cierto?

Primer pensamiento … ¡no puede ser!

Segundo pensamiento …





Y encima … no solo pierdo la disponibilidad sino …

Empezamos a recordar todo lo que hemos implantado

alhambra
leave IT in our hands

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 …

- ¿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

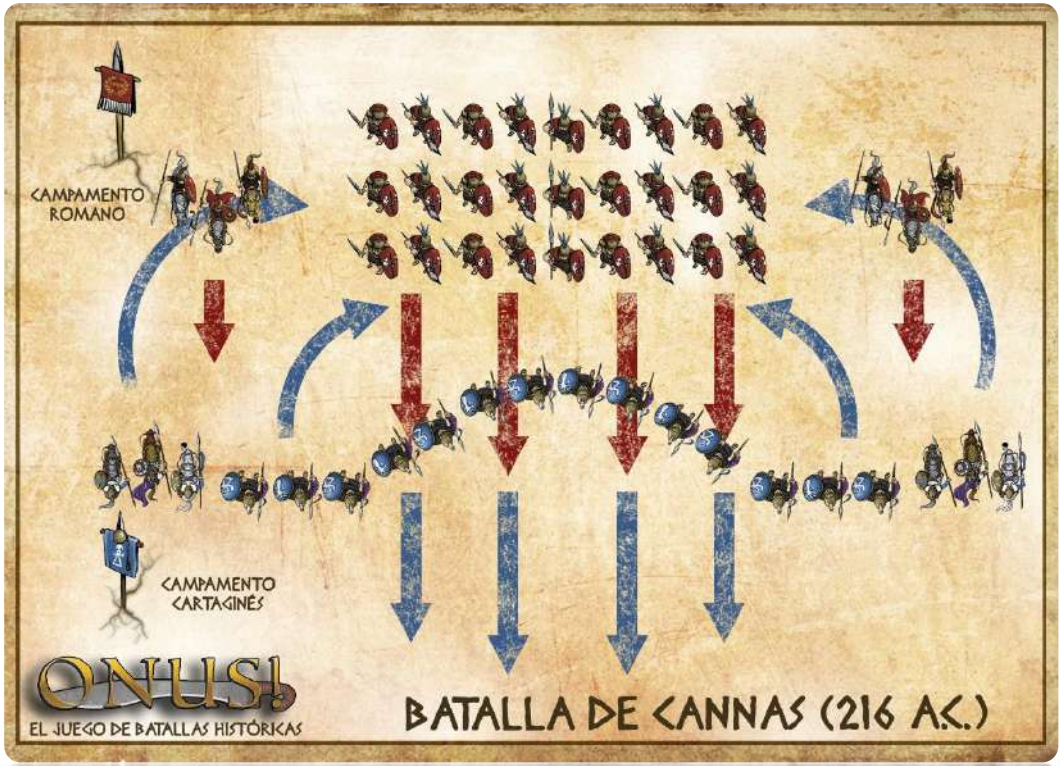
SÓLO EL 24% DE LOS ATAQUES SE DETECTAN A TIEMPO

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.

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

alhambra
leave IT in our hands

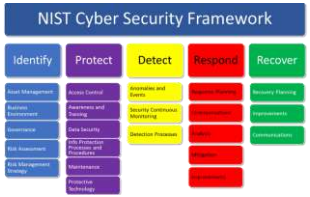
1 IDENTIFY

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



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

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

4 RESPOND

Develop a plan for disasters and information security incidents

3 DETECT

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

Maintain and monitor logs

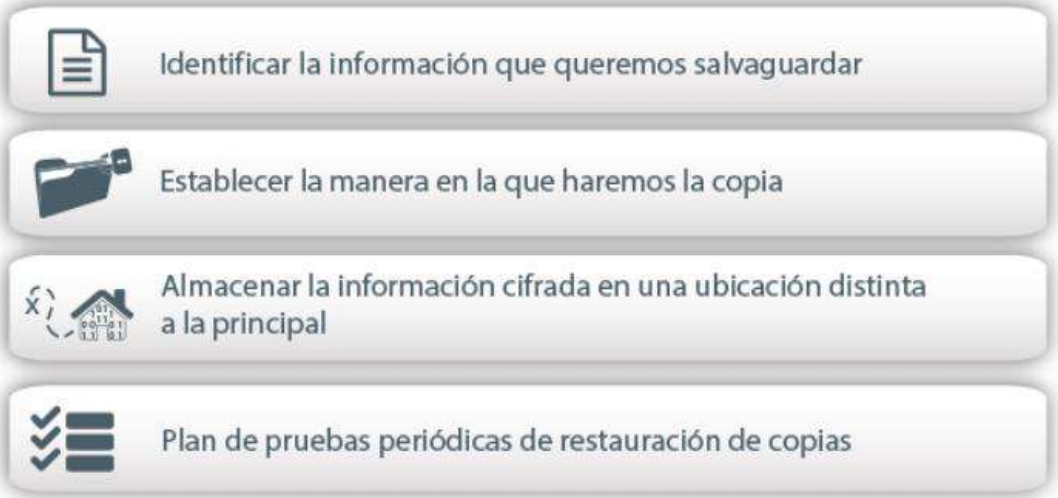
ERITAS

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

alhambra
leave IT in our hands

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Buenas prácticas para la realización de copias de seguridad



VERITAS

… pero si entramos en harina para el servicio de BackUp

alhambra
leave IT in our hands

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

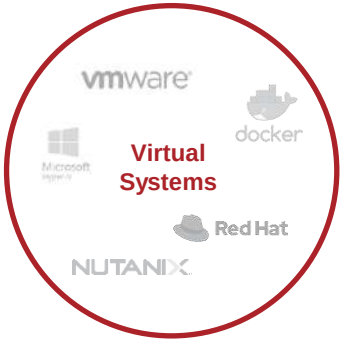
1. Tiene que **estar bien diseñada** … no solo por producto, sino por esquema de seguridad (segmentación del servicio, harderización del servicio, etc …)

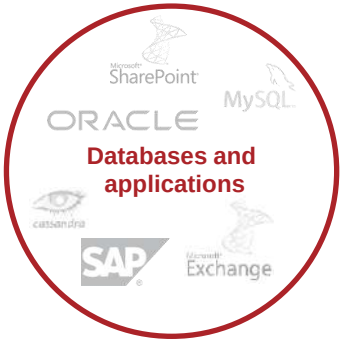
2. Tiene que ser **inmutable** frente a ataques de Ransomware. Es frecuente que el propio cifrado de datos, cifre los backups, y esto puede ser un desastre porque perdemos nuestros backups más cercanos y como mucho podremos tirar de los backups más lejanos (si los tenemos) y probablemente en dispositivos 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.

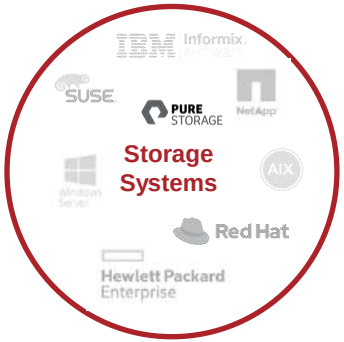
VERITAS

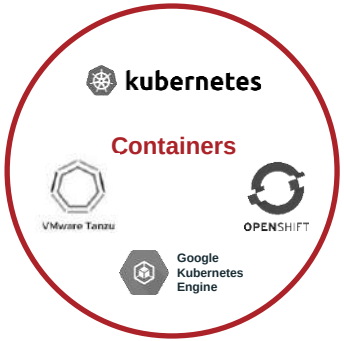
alhambra
leave IT in our hands





NetBackup
Unmatched Flexibility





VERITAS

www.alhambraIT.com | www.veritas.com

alhambra
leave IT in our hands

VERITAS

Inmunidad Contra Ransomware

Santiago Sánchez
System Engineer | Veritas

Who Are We

alhambra
leave IT in our hands

15x

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

VERITAS

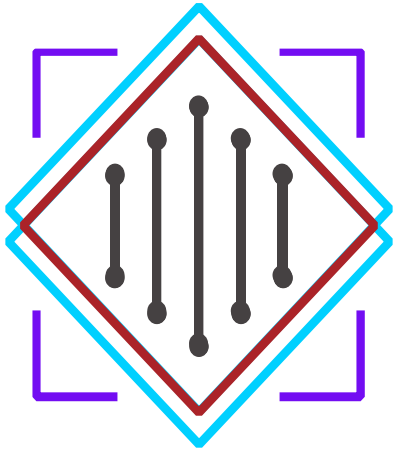
#1

MARKET SHARE FOR BACKUP AND RECOVERY SOFTWARE

6,000+	20,000+	80,000+	2,000+	2,140+	800+	380+PB	100+EB	87%
Employees Worldwide	Global Partners	Global Customers	Developers Worldwide	Global Patents	Supported Workloads	Driven AWS Consumption	Data Under Management	Fortune Global 500 Trust Us

Our portfolio

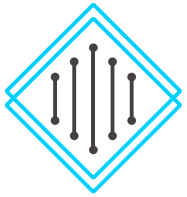
alhambra
leave IT in our hands



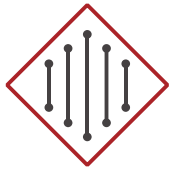
VERITAS™

ENTERPRISE DATA SERVICES

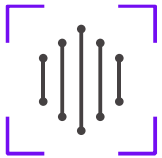
PLATFORM



AVAILABILITY



PROTECTION



INSIGHTS

VERITAS

Traditional Data Challenges

alhambra
leave IT in our hands

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

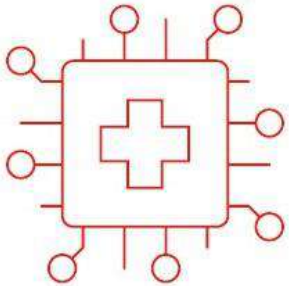
According to a research report by the Ponemon Institute, a data centre outage costs around $9,000 per minute.

VERITAS

NEW Data challenges

alhambra
leave IT in our hands

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



VERITAS

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

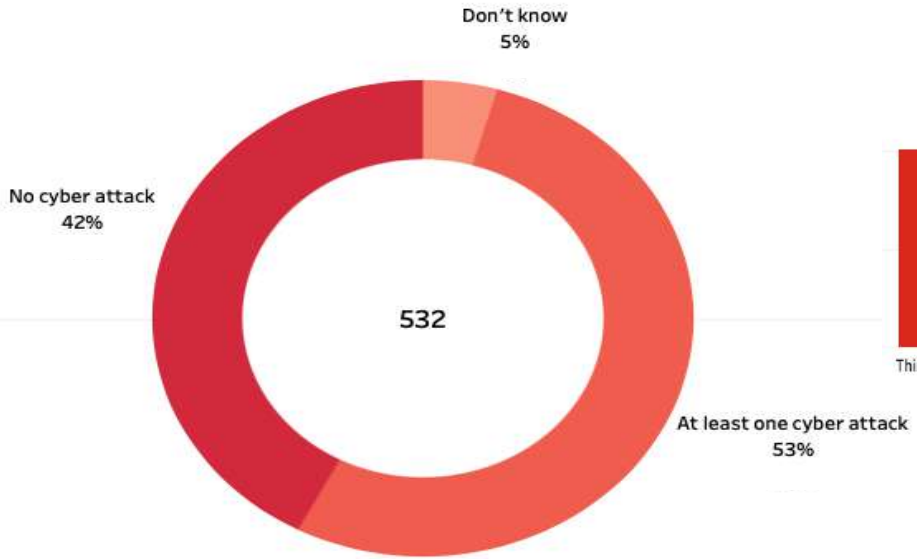
64%

of organizations have not kept up with security measures

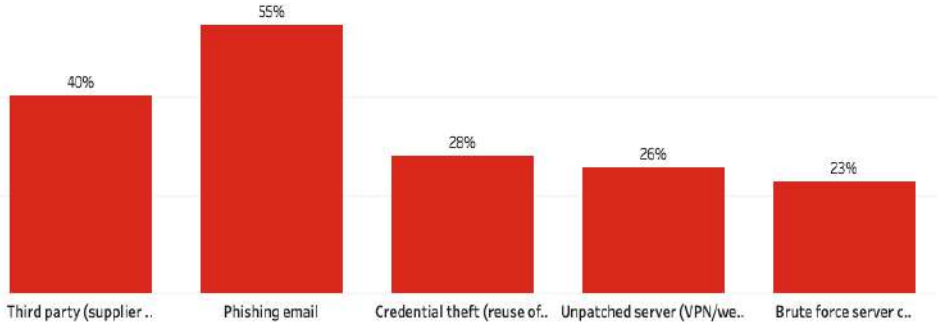
VERITAS

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

alhambra
leave IT in our hands

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/hr[3]
- 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

VERITAS

What is The Zero Trust Security Model?

alhambra
leave IT in our hands

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**

VERITAS

alhambra
leave IT in our hands

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

alhambra
leave IT in our hands

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

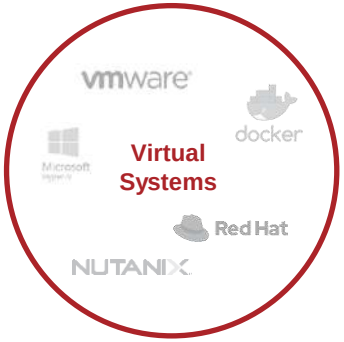
- ✓ Automated recovery orchestration to anywhere, cloud & bare metal
- ✓ Non-disruptive recovery testing
- ✓ Instant access recovery and roll-back

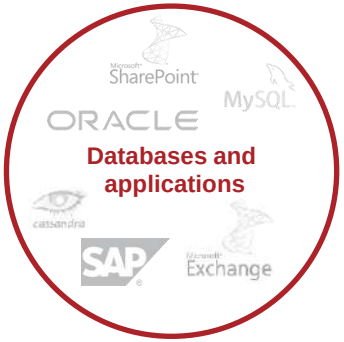
VERITAS

STEP 1:

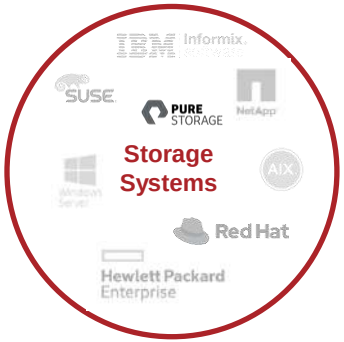
Protect

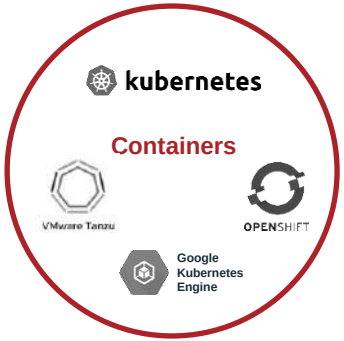
alhambra
leave IT in our hands





NetBackup
Unmatched Flexibility





VERITAS

How Veritas Safeguards Your Data

Appliances

alhambra
leave IT in our hands

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.

VERITAS

Security Features in NetBackup Appliance

alhambra
leave IT in our hands

New NetBackup Appliance Security Features

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

VERITAS

Appliances family

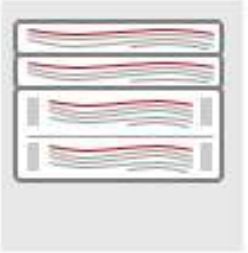
alhambra
leave IT in our hands

NetBackup 5250 Appliance

- ✓ Master or Master/Media
- ✓ 429 TiB maximum storage

POSITIONING SUMMARY:
Predictable high-performance data protection for moderate workloads.

NetBackup 5350 Appliance



- ✓ High performance Media Server
- ✓ 1,920 TiB maximum storage

POSITIONING SUMMARY:
Predictable highest performance data protection for enterprise workloads.

Flex 5150 Appliance

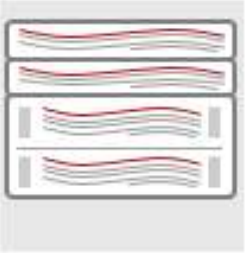
- ✓ Simplified appliance solution
- ✓ Cost-effective design
- ✓ Smaller workloads

POSITIONING SUMMARY:
Streamlined protection for remote or branch office locations.

Flex 5250 Appliance

POSITIONING SUMMARY:
Predictable high-performance data protection for moderate workloads.

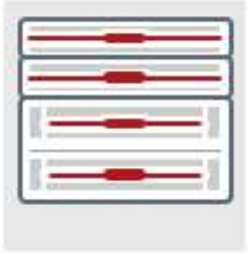
Flex 5350 Appliance



- ✓ Flexibility and agility
- ✓ Inmutable Storage
- ✓ Multiple NetBackup roles on one appliance

POSITIONING SUMMARY:
Run multiple Veritas software products on a single, flexible, converged solution.

Access 3340 Appliance

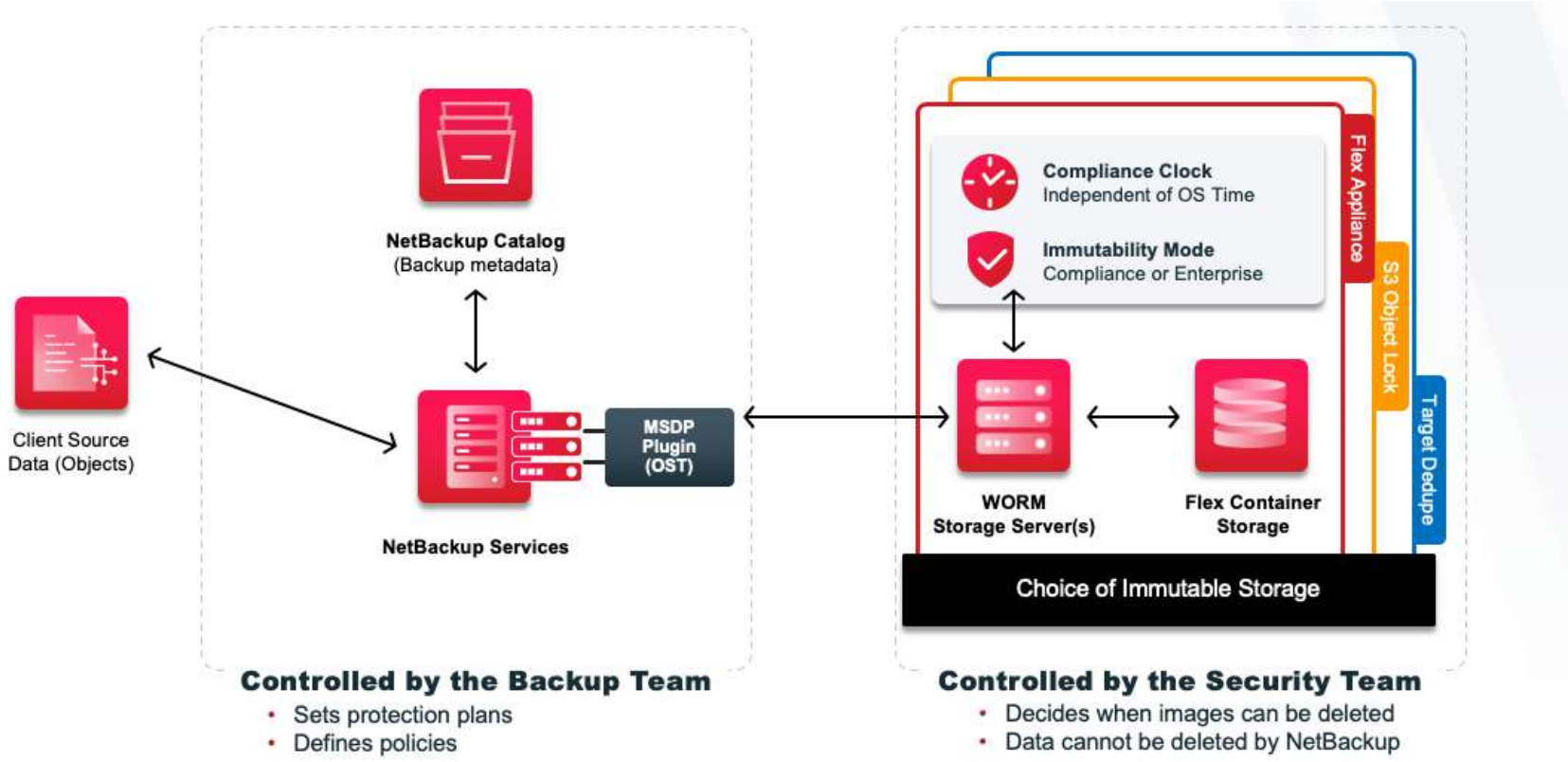


- ✓ Long-term data retention
- ✓ 2,544 TiB maximum storage

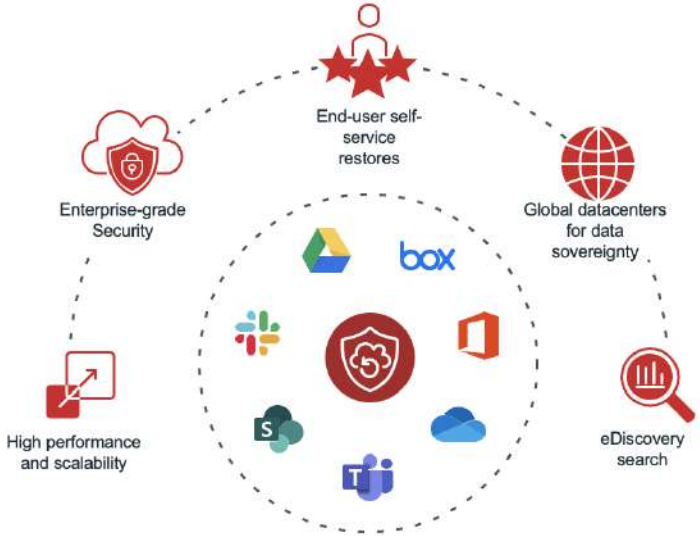
POSITIONING SUMMARY:
Long-term data storage and archiving as tape and public cloud alternative.

VERITAS

Inmutable Storage

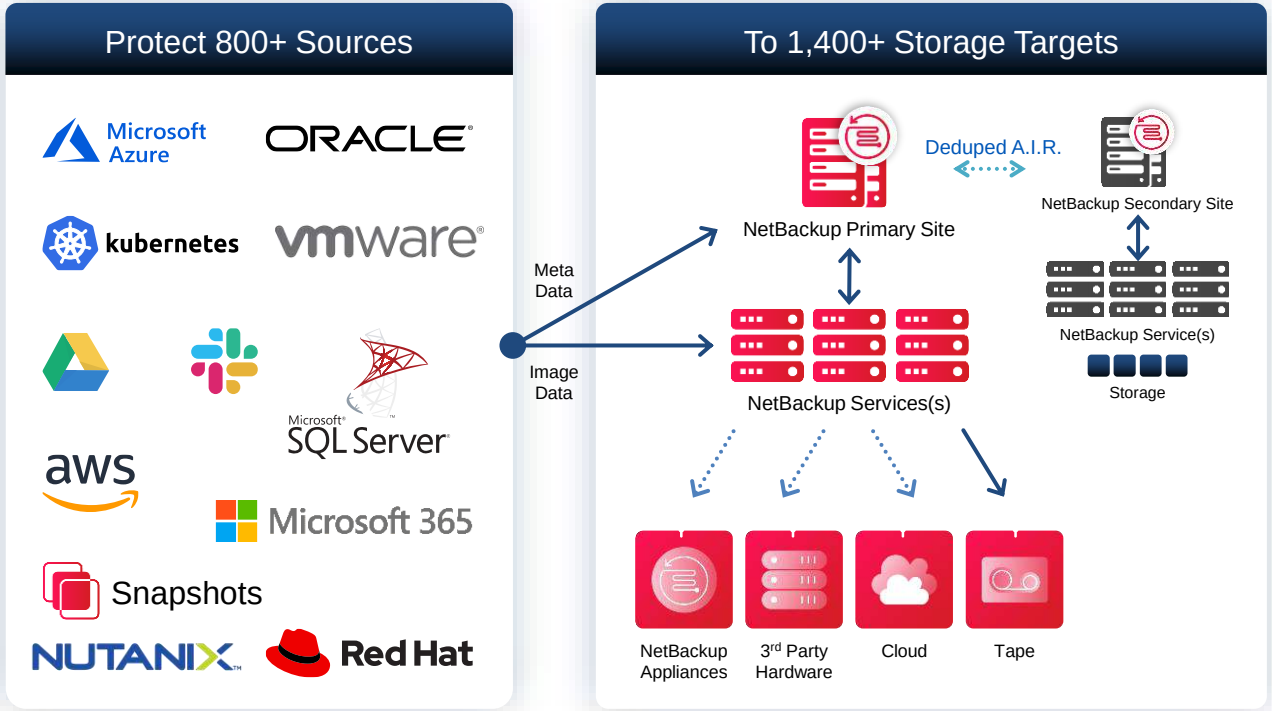


SaaS platforms



- **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

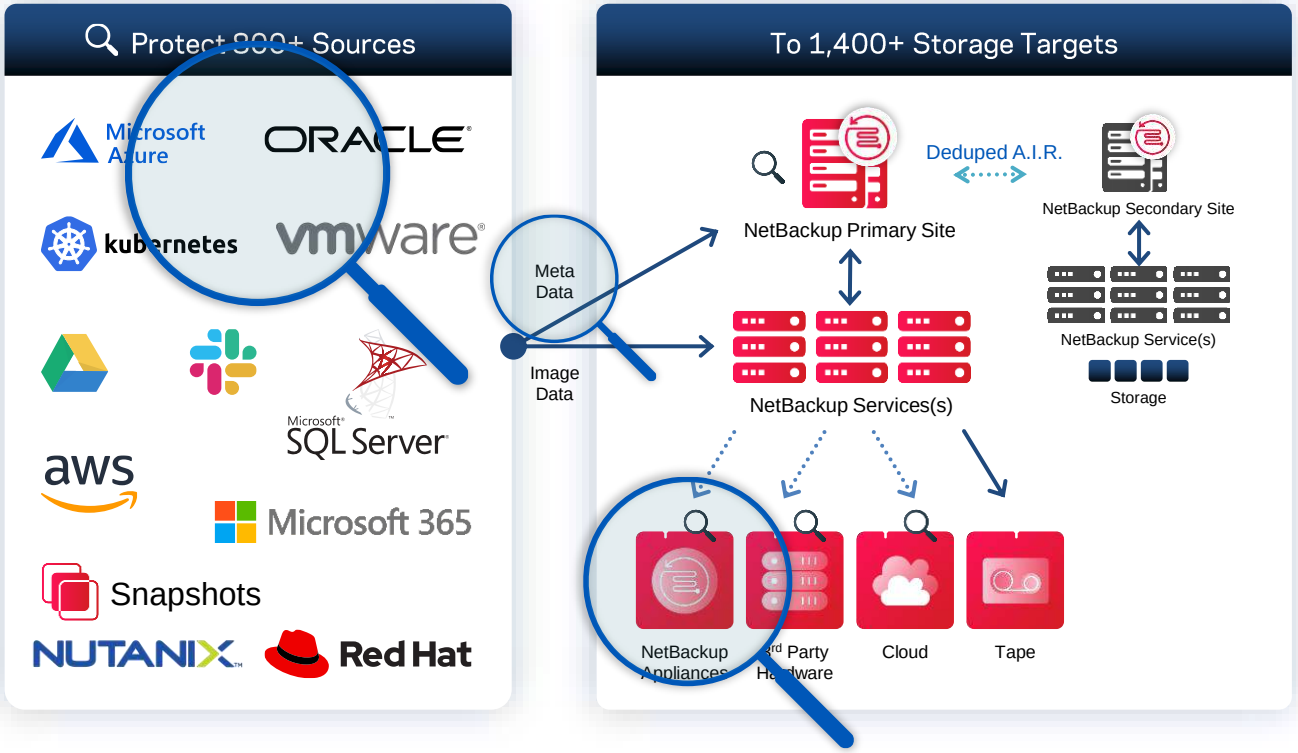


= Immutable/Encrypted Storage = Detection Capabilities = Dedupe

STEP 2:

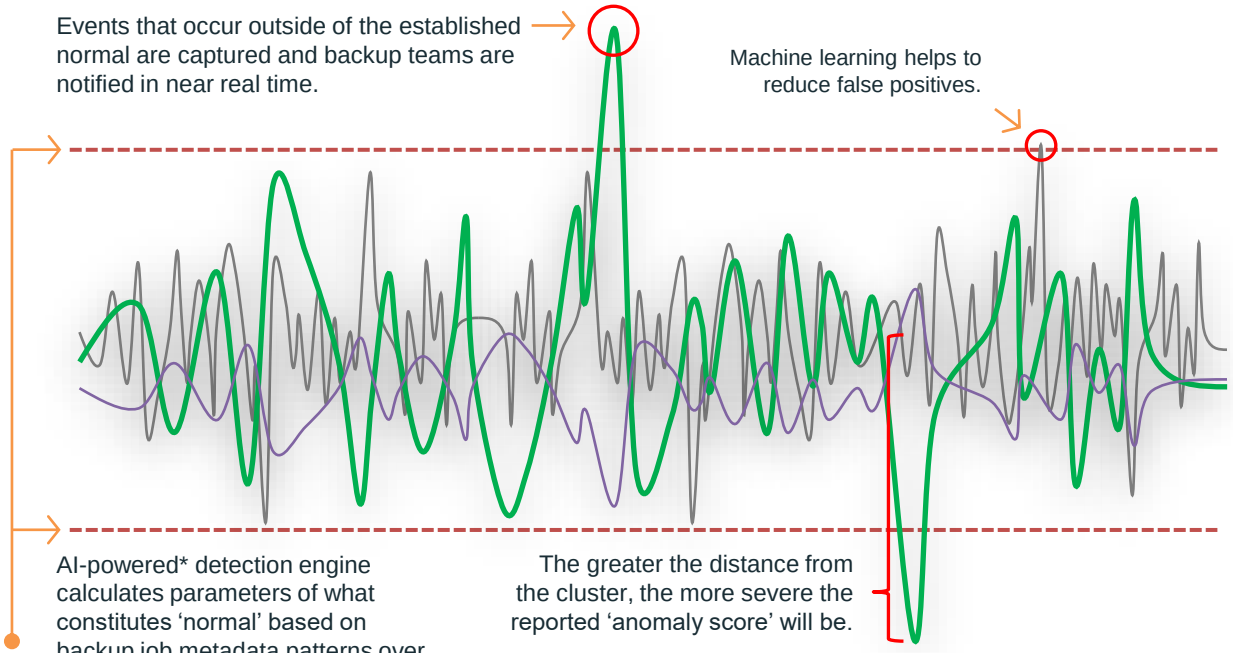
Detect

Step 2: Detect



= Immutable/Encrypted Storage = Detection Capabilities = Dedupe

Understanding Anomaly Detection



AI-Powered Anomaly Detection Engine in NetBackup

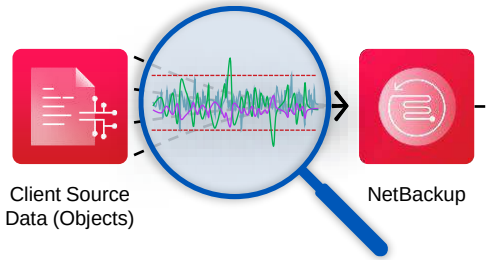
- Mine enormous amounts of data
- Automate monitoring and reporting
- Gain actionable insights
- Report based on several criteria
- Establish early warning of an attack

* 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

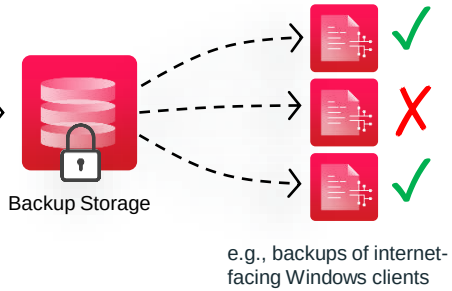
alhambra
leave IT in our hands

During Backup



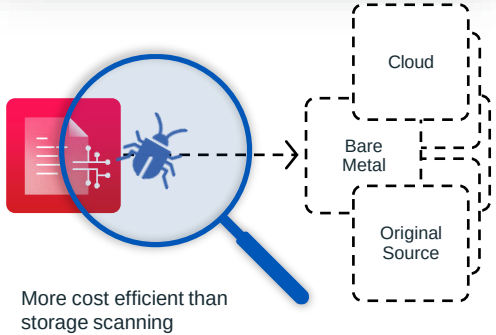
Anomaly detection in near real-time

Post Backup



Spot-checking of known high-risk areas

Before Restore



Scanning before restore to ensure clean data

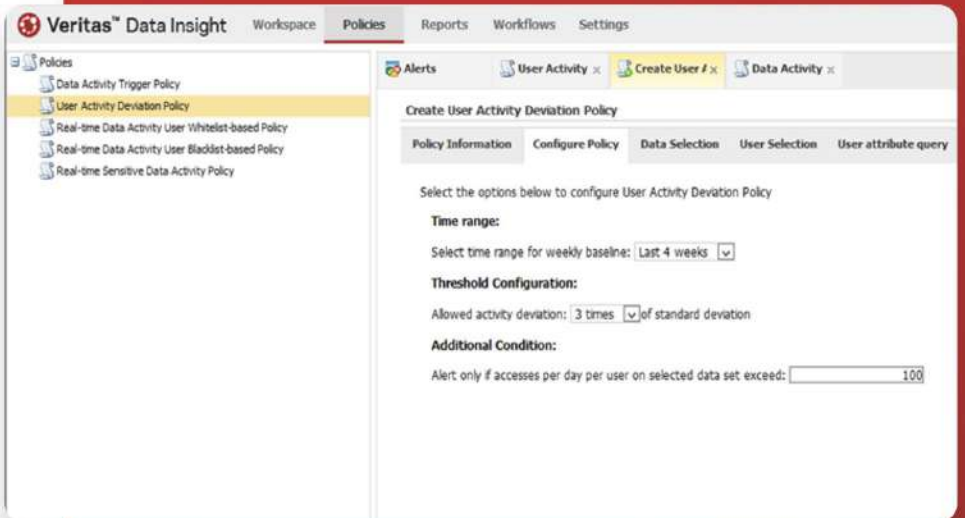
VERITAS

Advance Your Risk Intelligence with Machine Learning

alhambra
leave IT in our hands

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

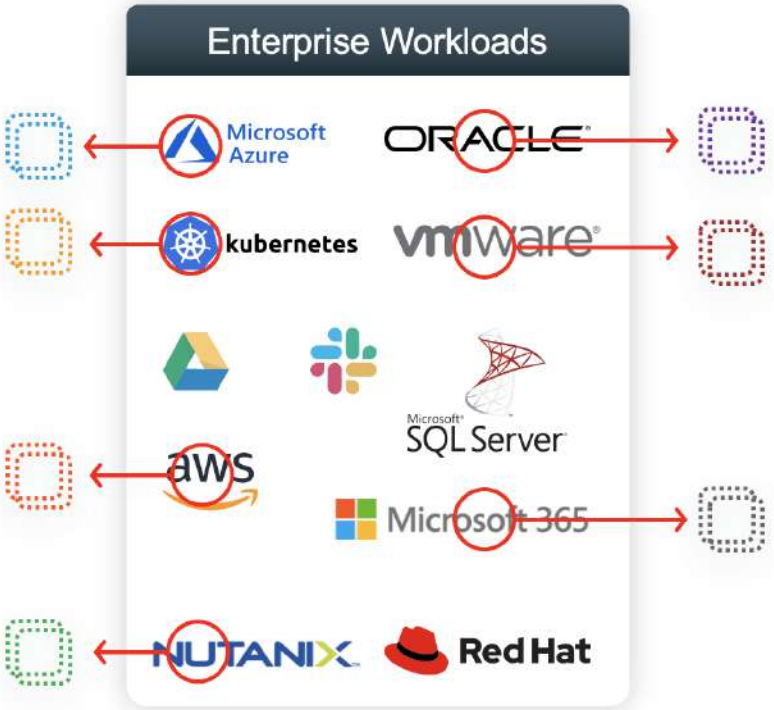


VERITAS

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.

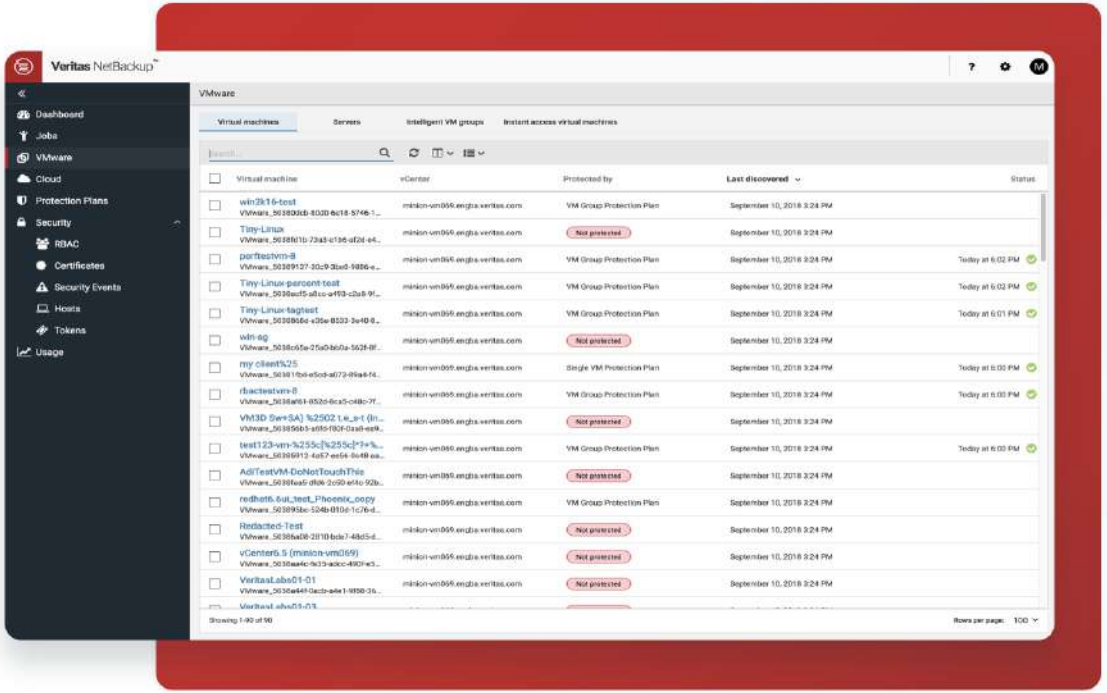
Additional considerations:

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

Support for RPO & RTO Requirements

alhambra
leave IT in our hands

- 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



VERITAS

Your Plan is Only as Good as Your Last Test!

alhambra
leave IT in our hands

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 disruptived 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

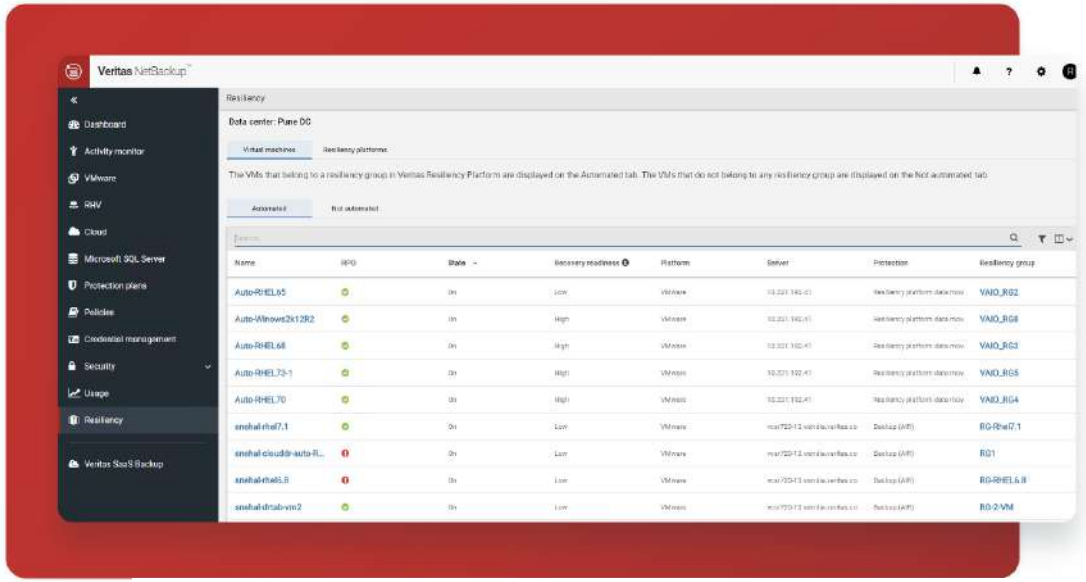
Veritas had a 100% recovery success rate for customers that were hit by a ransomware attack in 2020.

Tracking toward a repeat in 2021!

Automated Recovery Orchestration

VERITAS

Resiliency



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:

How do I know I am recovering from clean data?

Best practices to ensure desired outcomes:

- ***UR*** — *Don* ... ***AND*** — *y.*
- ***AD*** — *Kee* ... *age.*
- ***AC*** — *App* ... *access.*
- ***OR*** — *Limi* ... ***EST*** — *often.*
- ***UN*** — *Detect anomalies and malware across data and infrastructure.*

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

alhambra
leave IT in our hands

Servicios Productos Clientes ¿Hablamos? IT Blog

Hemos unido dos mundos desde la BASE

alhambra
leave IT in our hands

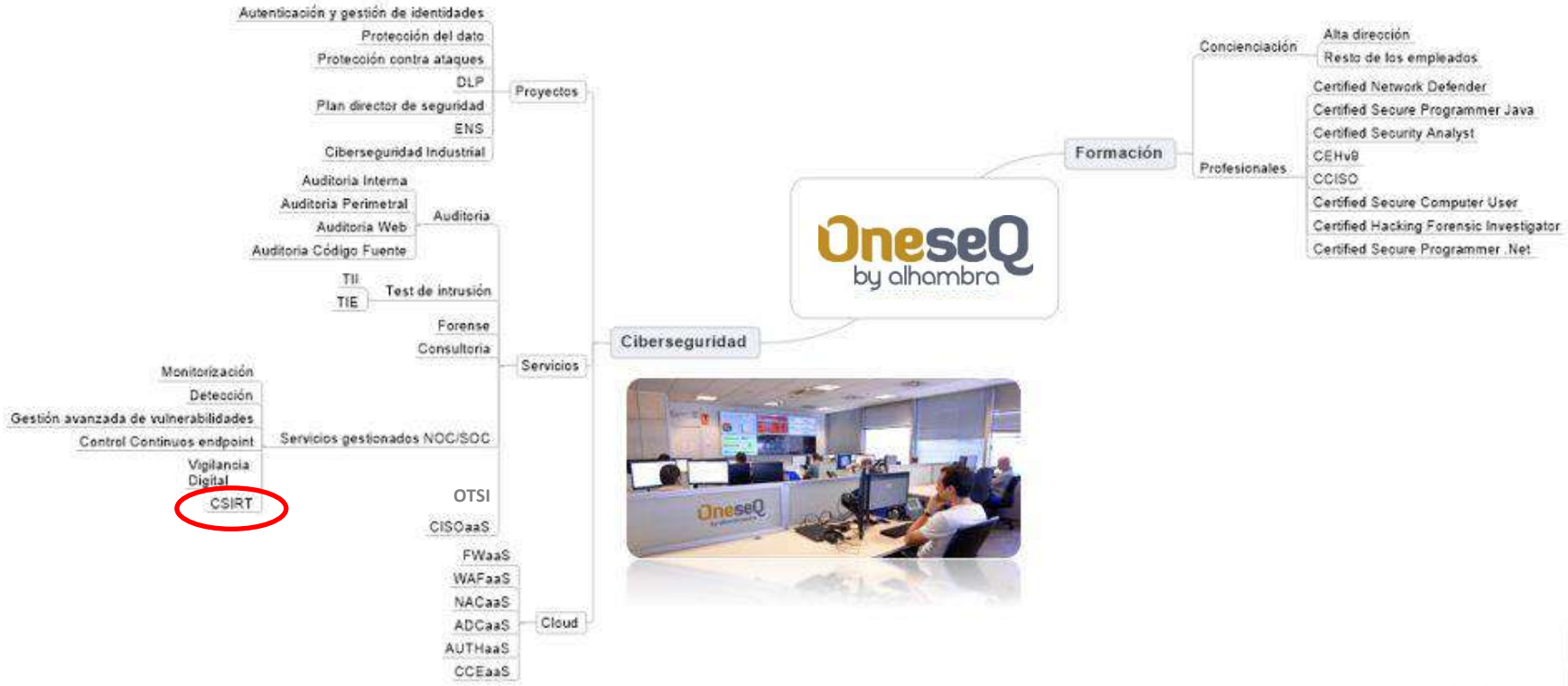
Especialista en IT
Integración de sistemas, comunicaciones, desarrollo, formación, etc …
Más de 30 años

Ciberseguridad

OneseQ
by alhambra

VERITAS

Hemos puesto el SOC en el centro de los servicios



Para un IR hay dos conceptos CLAVE

alhambra
leave IT in our hands

Incident Response (IR)
CSIRT

Threat Hunting

VERITAS

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

alhambra
leave IT in our hands

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 Triaje: 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.

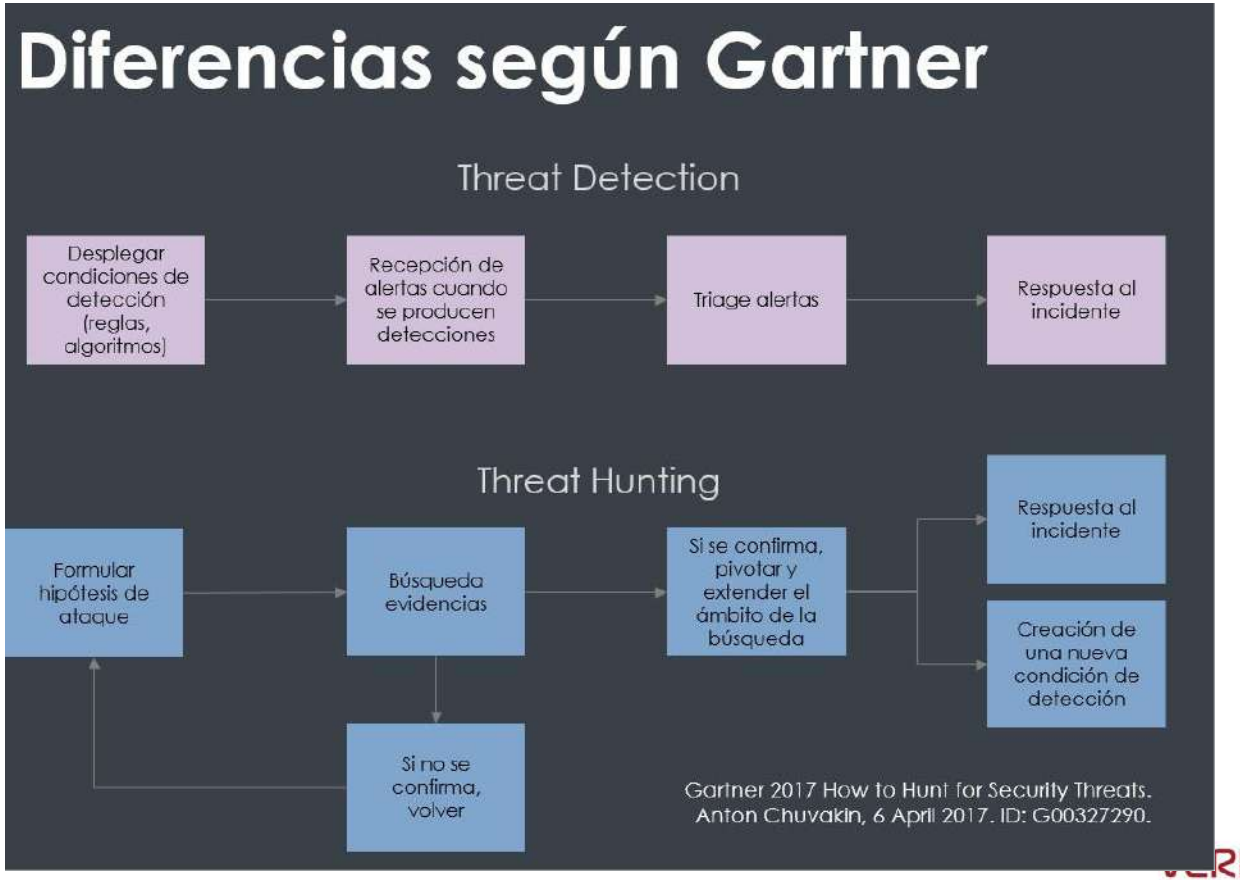
VERITAS

El otro concepto importantísimo

alhambra
leave IT in our hands

Alerta Temprana

Threat Hunting



VERITAS

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

alhambra
leave IT in our hands

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 SOCs 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

ISO 9001 ISO 14001

VERITAS

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

> Multiples SOCs en distintas zonas geográficas (**implantación internacional**)

> Nuestros SOCs además operan y **colaboran compartiendo información con otros SOCs**

> 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

www.alhambraIT.com | www.veritas.com

alhambra
leave IT in our hands

VERITAS

Alhambra IT y Veritas

Julio Saíz
Business Developer Manager | Alhambra IT

Alhambra IT como partner de Veritas

alhambra
leave IT in our hands

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

VERITAS Partner Force
Gold Partner

En proceso

VERITAS Partner Force
Platinum Partner

NETBACKUP guru

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

VERITAS

Alhambra IT como cliente de Veritas

alhambra
leave IT in our hands

alhambra
cloud

CO_2 cero

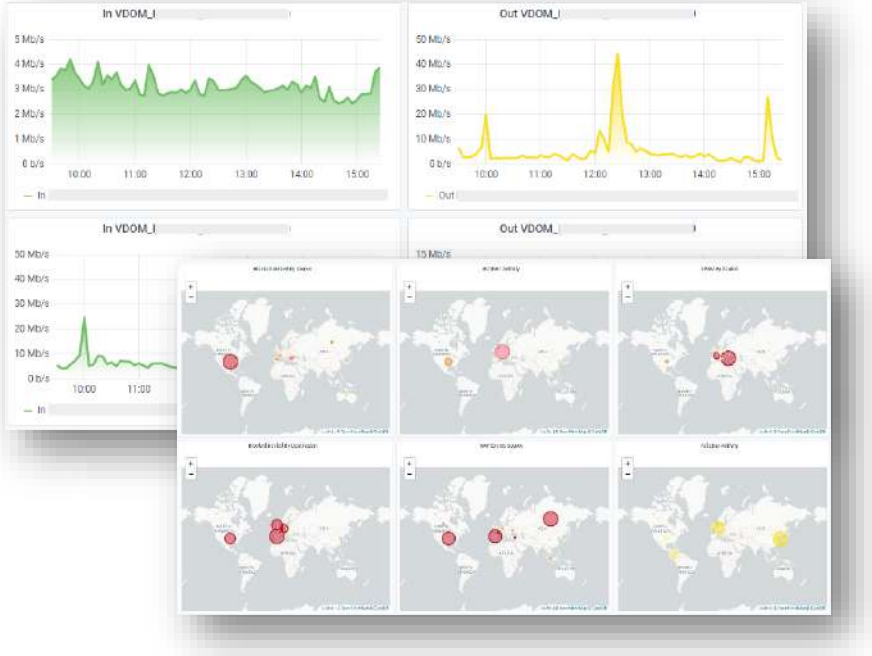
Madrid-1 | Madrid-2 | París | Miami

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

alhambra
leave IT in our hands

Servicio de Backup

Servicio de Repositorio Offsite

Servicio de Replicación

Servicio de Disaster Recovery

Servicios MultiCloud

VERITAS

www.alhambraIT.com | www.veritas.com

alhambra

VERITAS