

Anatomy of an Attack



The New Ransomware Reality

Ionuț Roșca

Security and Resilience Platforms Specialist

 Dell Technologies

It's not IF.... but **When**

Events once seen as extreme and unusual are now commonplace.

AI, accelerating vulnerability exploitation to hours, not weeks

The impact is already real



Frontier AI models compress attack velocity

Models such as Anthropic's Mythos shrink the gap between vulnerability discovery and exploitation from weeks or months into hours.



Adversaries are more convincing and at scale

AI-enabled attackers increase the speed, scale and sophistication of attacks — including AI-assisted voice social engineering.

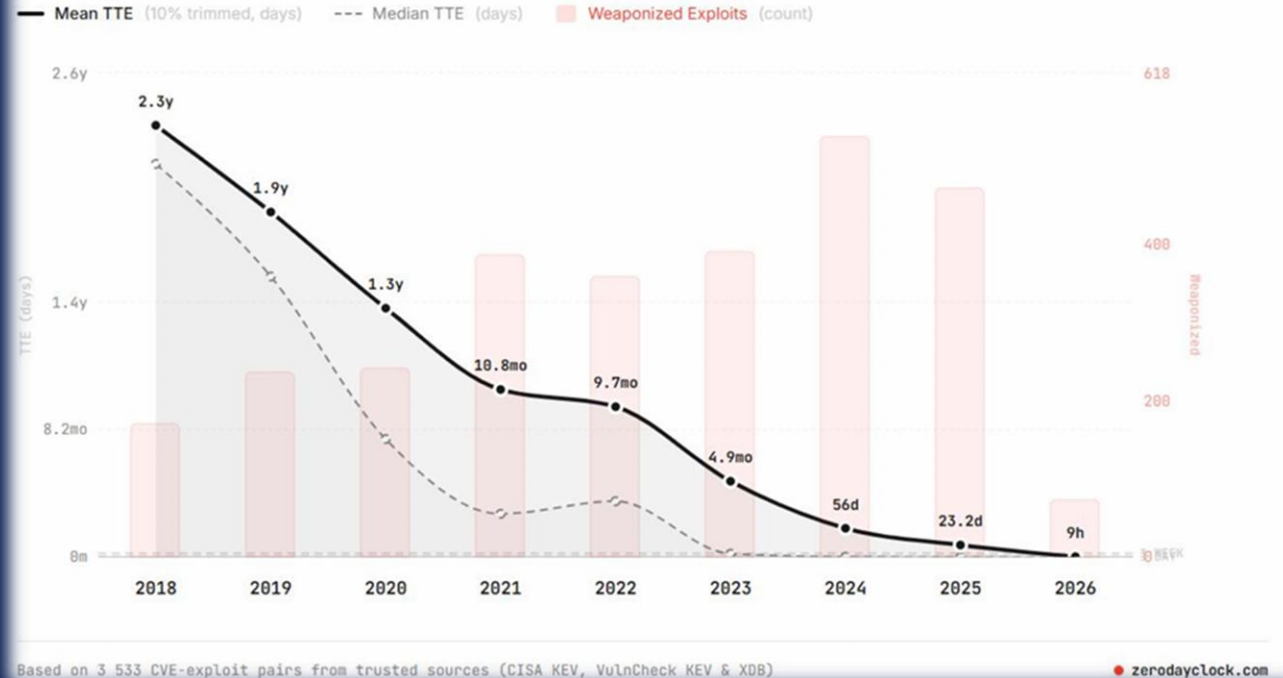


Non-human identities are the new target

Attackers increasingly pursue tokens, service accounts and other non-human identities that can unlock broad administrative access.

From Vulnerability to Exploitation

TTE (Time-to-Exploit) measures the gap between CVE disclosure and confirmed exploitation



Resilience is not an option, it's **Existential** to your business

Customer Challenges



24 days

Average downtime after a Ransomware attack¹

79%

Attacks did not deploy malware - relying instead on “hands-on-keyboard” techniques²

73%

Of organizations say data privacy and security is a risk they are concerned about when using GenAI³

94%

Of ransomware attacks included attempts to compromise the backup (57% success rate)⁴



STORMY CLOUD

Google accidentally deleted a \$125 billion pension fund's account

About half a million customers of the Australian fund UniSuper were locked out of their accounts for a week

By **Laura Bratton** Published Monday 12:07PM



While UniSuper normally has duplication in place in two geographies, to ensure that if one service goes down or is lost then it can be easily restored, because the fund's cloud subscription was deleted, it caused the deletion across both geographies.

UniSuper was able to eventually restore services because the fund had backups in place with another provider.

"These backups have minimised data loss, and significantly improved the ability of UniSuper and Google Cloud to complete the restoration," the pair said.

COMUNICAT DE PRESĂ: Atac cu ransomware împotriva companiei AAylex (Cocorico)

2025/03/13 Popularitate 1000 Tweet

București, 13 martie 2025

Directoratul Național de Securitate Cibernetică (DNSC) a fost notificat duminică, 9 martie 2025, referitor la atacul cibernetic desfășurat asupra **AAylex ONE**, grupul integrat din industria alimentară, care include fluxul complet de producție, distribuție și comercializare a produselor din carne de pui, cunoscute sub marca **Cocorico**.

În cel mai scurt timp, specialiștii DNSC s-au deplasat la fața locului pentru a oferi suport în remedierea incidentului. În acest moment, o investigație amplă este în desfășurare, informațiile preliminare indicând că este vorba despre un atac informatic de tip ransomware lansat de un grup infracțional internațional.



Foto: DNSC

Home

News

Sport

Business

Innovation

Culture

Arts

Travel

Earth

Audio

Video

Live

JLR to restart production on Wednesday after cyber-attack

22 hours ago

Theo Leqqett business correspondent and Josh Martin business reporter

Based on those numbers, a month-long shutdown could cost billions of dollars and seriously strain the company's profit margin; without insurance, the company could be on the hook for all of those losses.

[One analyst estimate](#)d that JLR has lost more than £1 billion (\$1.36 billion in revenue) since the attack.

Atacurile cibernetice s-au intensificat în 2024: ce domenii au fost vizate și ce arată datele oficiale DNSC

În 2024, România s-a confruntat cu o **creștere semnificativă a atacurilor cibernetice**, reflectând tendințele globale. DNSC a detectat peste **27 de milioane de evenimente de securitate**, față de 21,5 milioane în 2023. Deși numărul incidentelor efective raportate a scăzut ușor (8.852 față de 9.881), complexitatea și ingeniozitatea atacurilor a crescut.

Sectoarele cele mai afectate:

- Energie, bănci, telecomunicații, transport, administrație publică – vizate de atacuri DDoS.
- Instituții publice și private – afectate de ransomware, brute-force, defacement.

Tipuri de atacuri predominante:

- Phishing (22.05% din totalul incidentelor)



Hello everyone today we hacked into orange and stole all information related to orange.com and orange.ro from romania

The stolen information is very detailed (around 4.5 Terabytes - unique email addresses along with source code, internal documents, invoices, contracts, projects, plans. Then,

a little bit of detail:
Customer Records, Source Code, Internal Credit Cards, PII, Call Logs

and there is still a lot more that we stole,

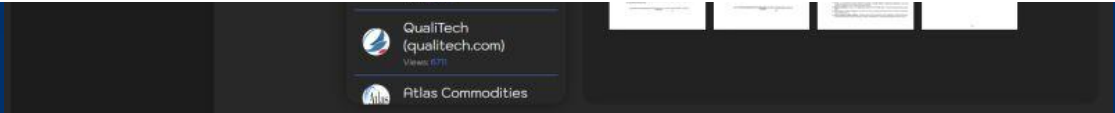


Agencia Națională de Cadastru, ținta unui atac informatic

Agencia Națională de Cadastru și Publicitate Imobiliară (ANCP) a anunțat că a fost vizată de un atac informatic, însă **datele instituției nu au fost compromise**. Potrivit reprezentanților ANCP, măsurile de securitate implementate au permis limitarea impactului, iar specialiștii lucrează pentru restabilirea completă a funcționării serviciilor afectate.

Instituția precizează că bazele de date sunt în siguranță și colaborează cu autoritățile competente pentru investigarea incidentului și consolidarea măsurilor de protecție.

A venit Ana, al carei prieten lucreaza la o firma de contabilitate. Le-a spart baza de date, a cerut 4500\$ ransom, a negociat la 2500 \$ in cripto. Le-a lasat doar adresa de mail a tipului ca sa il contacteze, deci mare grija cu serverul nostru.



When basic security fails, everything falls

No matter what advanced security mechanisms your organization has in place, everything falls if basic security measures fail. In the **KNP attack**, Akira targeted the company's internet-facing systems, found an employee credential without **multi-factor authentication**, and guessed the password. Once inside, they deployed their ransomware payload across the company's entire digital infrastructure.

But the hackers didn't stop at encrypting critical business data. They also destroyed KNP's backups and disaster recovery systems, ensuring that the company had no path to recovery without paying their ransom. The criminals demanded an estimated £5 million - money the transport company didn't have.

KNP had industry-standard IT compliance and cyber-attack insurance, but none of these protections were enough to keep the organization going. Operations came to a standstill. Every truck was sidelined. All business data remained locked away. The cyber crisis team brought in by insurers described it as "the worst-case scenario" for any organization. Within weeks, KNP entered administration, and **700 employees** lost their jobs.

Worst Case Scenario

Imagine a severe but plausible scenario where:

Data is destroyed,
locked up, or
corrupted



Impacting both
primary systems
and the backup
system



Command, control
and processing are
unavailable or
unreliable



Customers are
disconnected from
their services and
assets



Business continuity
and disaster recovery
efforts are unable to
reconnect



1. How would the business recover without a backup system?
2. Can you prove that you can recover the business?
3. What would the total cost and time be for recovery?

Dell Technologies Cyber Resilience

Through the lens of the threat funnel



Secure

Reduce the Attack Surface:

Minimize the vulnerabilities and entry points that can be exploited to compromise the environment.



Detect

Detect and Respond to Threats:

Actively identify and address potential security incidents and malicious activities.



Recover

Recover from Cyberattacks:

Restore the organization as quickly as possible while minimizing disruption.



PowerProtect Data Domain

The foundation of Cyber Resilience

2700+

Cyber Recovery
Vault customers*



Zero Trust Alignment

Hardware Root of Trust | Secure Boot | RBAC | Secure Period



Immutability

Retention Lock Compliance Mode | SEC 17a-4(f) Compliance | FDA 21 CFR Part II



End-to-End Encryption

Data in Flight TLS 1.2 256 Bit | Data at Rest FIPS 140-2 Crypto Libraries



Multi-factor Authentication (MFA)

Web UI, CLI, Security Officer, and iDRAC



Secure System Clock | NTP Clock | Tamper Controls

Clock Change | Drift | Synchronization



File System - DDFS

Hashed Containers – not recognized by malware



Transport Protocol – DD Boost

Encrypted, Secure, Authorized, Not Open

PowerProtect Data Domain

The Foundation for Cyber Resilience



Security to ensure data is not
tampered with or corrupted

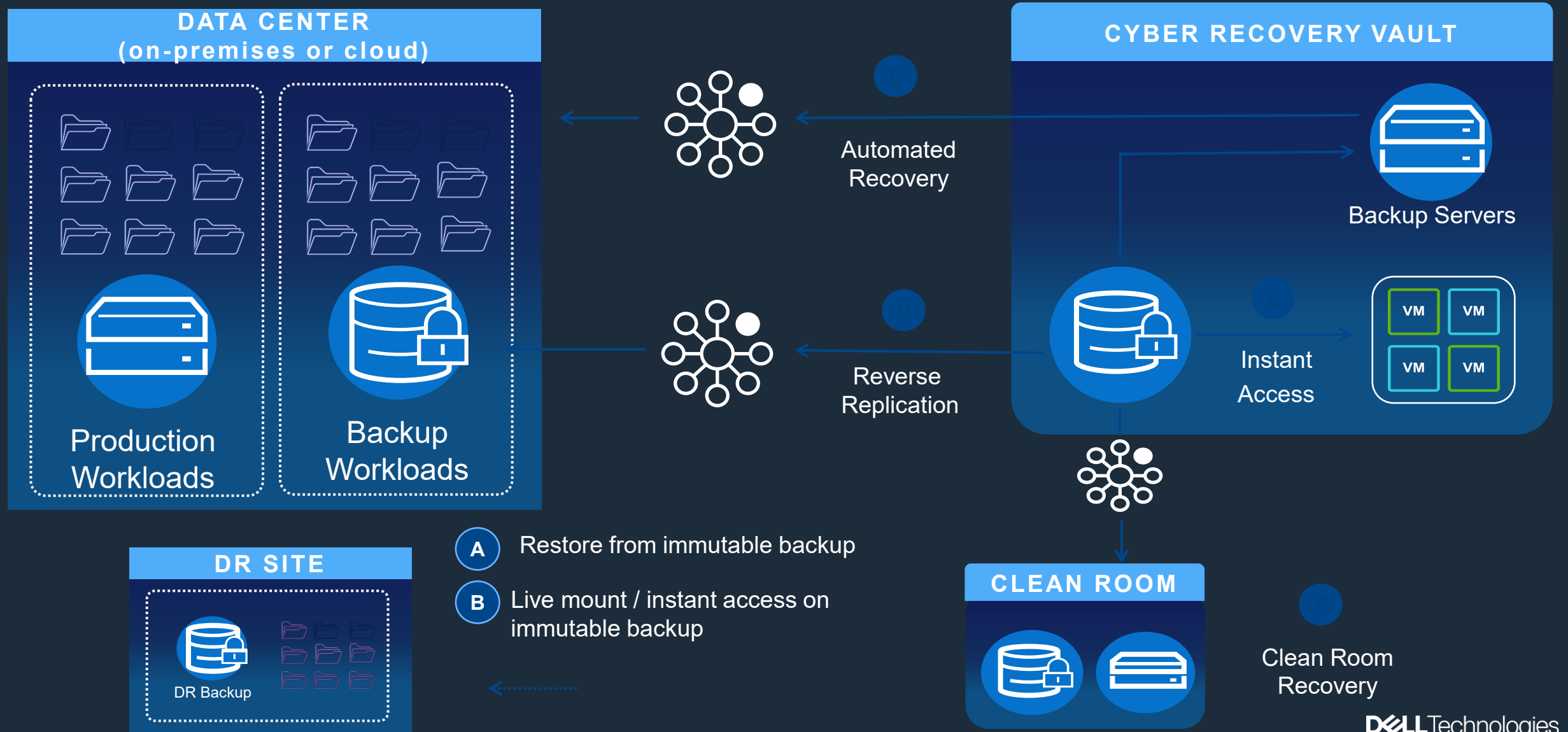


PowerProtect Cyber Recovery & CyberSense

Protect, isolate and validate critical data to recover
from cyber threats

Recovery Options To Meet Your Cyber Resilience SLAs

Flexible Recovery options to fit your needs



PowerProtect Cyber Recovery Deployment

Modern protection and recovery for critical rebuild data from ransomware and cyber threats to **enable cyber resiliency and ensure business continuity.**

ON-PREMISES



Optional Managed Services

PUBLIC CLOUD



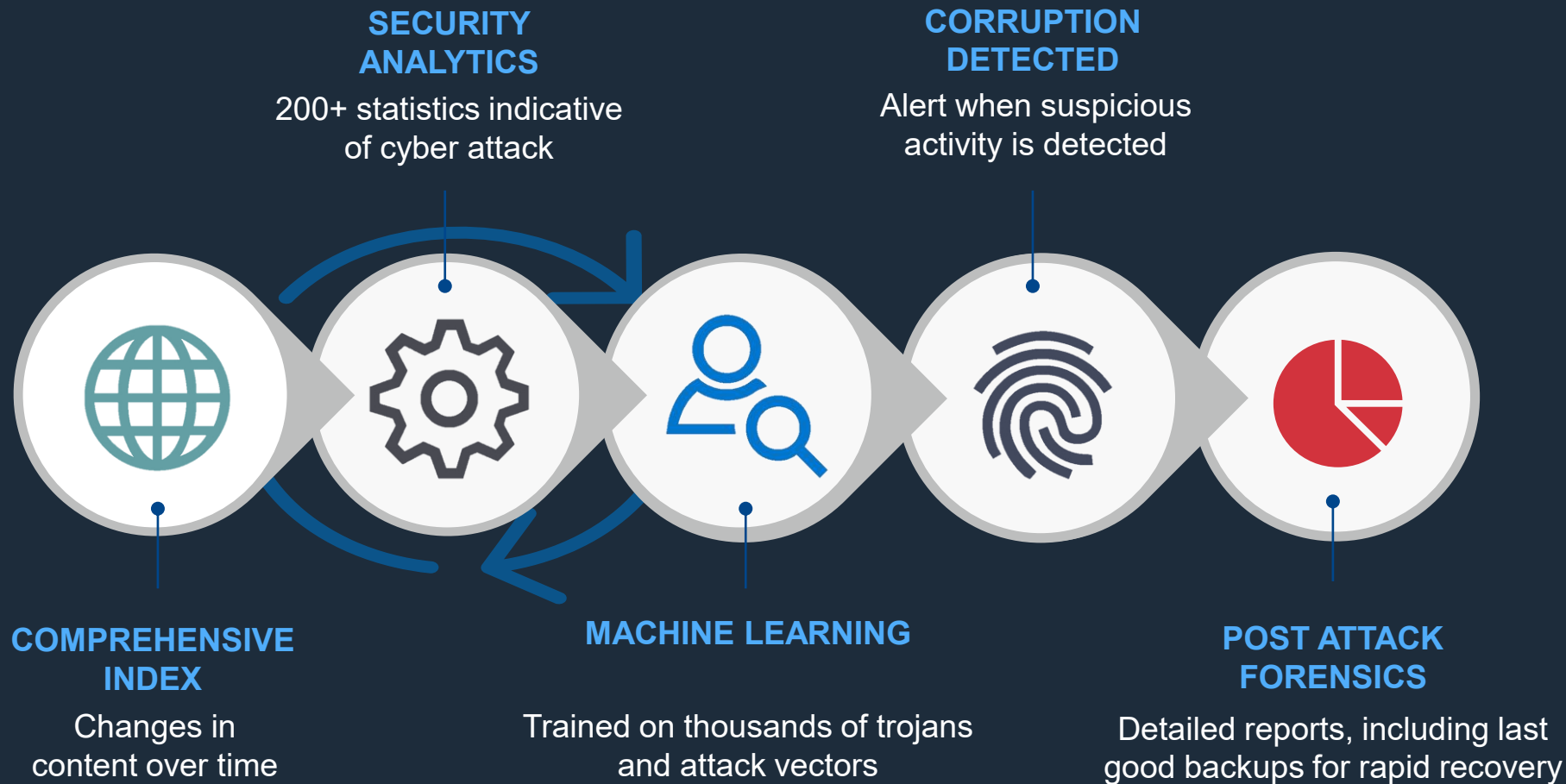


Intelligence with CyberSense

AI-based Machine Learning Analytics To Verify Data
Integrity for Resilience

How CyberSense Works

Analytics, Machine Learning and Forensic Tools to Detect & Recover from Cyber Attacks



CyberSense Provides

- Attack type notification
- Ransomware detection
- Corrupted file details
- Data changes / deletions
- Breached user accounts
- Breached executables
- Last good backup copy

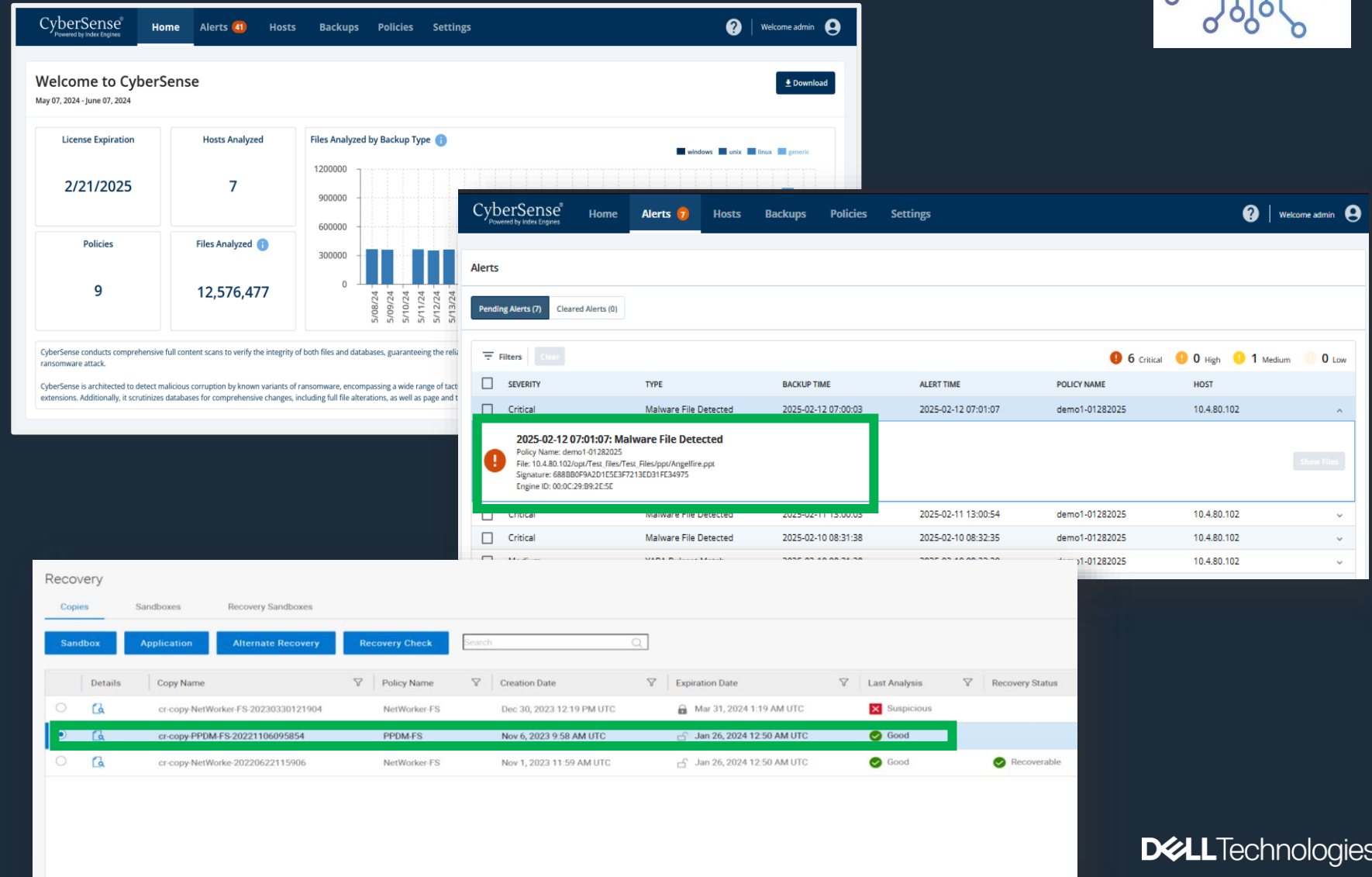
Recover Smarter with CyberSense

Simplified Dashboard for Analytics and Reporting



Dashboard View

- Simple Health view of analytics environment
- Detect corruption within a backup cycle
- Investigate the Who, What, Where and When of the attack
- Quickly identify last Clean backup for recovery



Cyber Resilience Services

Dell Security and Resiliency Services



Advisory Services

Evaluate your strategies continuously to reduce risk, align with compliance needs and improve processes and procedures:

- Vulnerability Management
- Ransomware Readiness Assessment
- Business Continuity and Disaster Recovery



Managed Detection and Response

Strengthen your security posture
Secure your devices across endpoint, network, and cloud.

- Industry-leading tools and expertise
- Around-the-clock access to security experts
- End-to-end visibility and protection from endpoint to cloud



Incident Response and Recovery

Backed by the scale of Dell's global network, we can react quickly, with experts standing by to help assess your situation and determine the best course of action.

- Fast response from cybersecurity experts
- Complete recovery and improved security to prevent future cyberattacks and incidents
- Vast expertise for any need



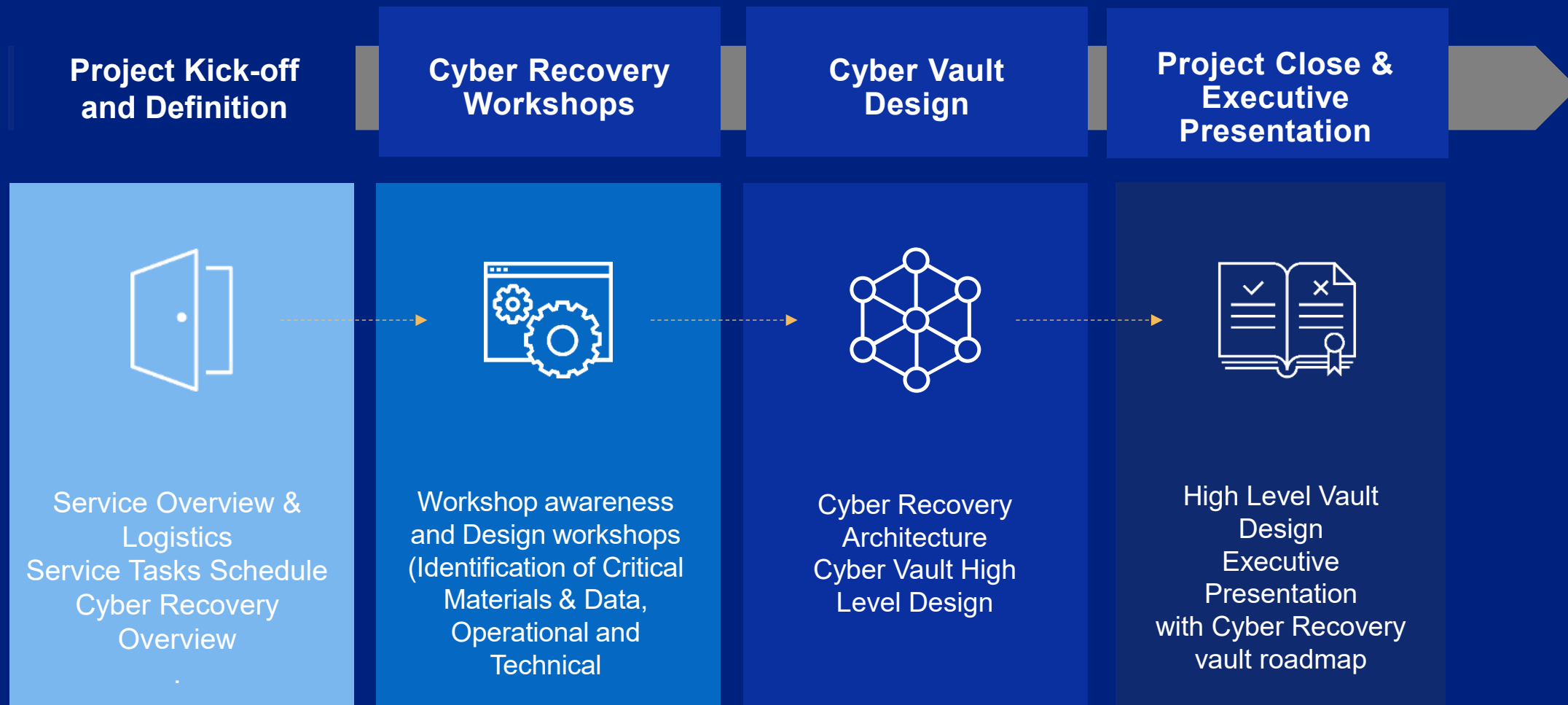
Cyber Recovery Services

Develop your strategy for a last line of defense from attacks such as ransomware. It's crucial to take a holistic approach which integrates three key components:

- Purpose-built, isolated recovery vault
- A business process focused recovery strategy
- A team prepared to continually test and improve processes

Advisory

Enhanced data resilience and robust cyber recovery architecture design



Design & Implementation Services

Providing a proven, tested, Cyber Recovery solution in your environment, delivered with a proven methodology.

Project Kick-off and Definition



Identify and collect
Cyber Security and
BCDR
background/collateral on
potential applications.

Technical Workshop



Discuss cyber vault
architecture and operation
to create cyber vault
architecture, metrics,
location and operation
considerations

Critical Materials & Data Workshop



Identification of Critical
Materials to target for initial
implementation of Cyber
Vault. Preliminary estimate
on application data to be
protected.

Deployment & Configuration



Configure Cyber Recovery
Vault Infrastructure,
Hardening and Deploy air-
gap copy, data immutability
and optional analytics
capability

Recovery Testing



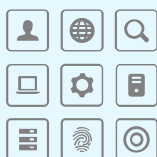
Develop recovery runbook
and test plan and conduct
knowledge transfer of vault
operations, security
analytics and restore
processes

Runbook and Testing Services

Operational Support (PowerProtect Data Domain, Block Data Storage, Unstructured Data Storage and Cloud)

Gather recovery requirements

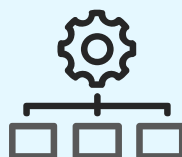
What



**Critical Rebuild
Materials**



OS Images



**Business
Processes**



Applications

How

Restore

Restore data from known Point in Time

Repair

Restore data and apply known fixes

Rebuild

Assume nothing, rebuild new environment,
restore transactional configs and data

Create tailored documentation

Cyber Recovery Solution Runbook

Table of Contents:

Cyber Recovery Vault Runbook overview	4
Section 1: Plan Activation and Criteria	8
Section 2: Perform Forensics	12
Section 3: Invoke Cyber Recovery Plan	14
Section 4: Prepare for Recovery/ Restore Operations	16
Section 5: Recovery Procedures.....	17
Section 6: Backup Recovery.....	20
Section 7: Event Recording Log.....	24

<Customer Name>
CR Vault Recovery Runbook
CONFIDENTIAL



Best Practices

Key Data to Protect by Industry



Healthcare

Electronic Medical Records, scheduling, payment and billing systems



Financial Services

Payments, Core Banking, Trading, Treasury, Sheltered Harbor data



Life Sciences

Research and development, drug discovery & Clinical trial data



Retail

Point of sale, inventory, shipping



Legal

Document management, conflicts checking, billing, email



Oil & Gas

Seismic & geographical exploration data



Government

Property records and taxes, justice systems, payment collection, licenses



Manufacturing

Plant manufacturing and scheduling, ordering systems, inventory

What to protect in a cyber vault

Best practice guidance to select your most important data and applications to protect

Applications



Intellectual Property

- Source code
- Proprietary algorithms
- Developer libraries



Host and Build Tools

- Physical/Virtual platform builds
- Dev Ops tools & automation scripts
- Firmware / microcode / patches
- Vendor software



Documentation

- CMDB / asset D/R and Cyber Recovery
- Run-books & checklists
- Management extracts
- HR resources & contacts lists

Supporting infrastructure



Authentication, Identity & Security

- Active Directory / LDAP
- DNS dumps
- Certificates
- Event logs (including SIEM data)



Networking

- Switch / router configuration
- Firewall / load-balancer settings
- IP Services design
- Access Control configuration
- Firmware / microcode / patches



Storage

- Backup hardware configuration
- SAN / array configurations
- Storage abstraction settings
- Firmware / microcode / patches

