DELL Technologies

Enhancing Your Cyber Resilience:

Protect, Detect, Respond, Recover

Enhancing your Cyber Resilience:

Protect, Detect, Respond, Recover

Jason Proctor
Advisory Systems Engineer, Cyber Resilience & Compliance
Data Protection Solutions, Global Technology Office

DELL Technologies


CYBER
is the new
DISASTER

Cyber Attack

Cyber Attack

A cyber attack is an attempt by cybercriminals, hackers or other digital adversaries to access a computer network or system, usually for the purpose of altering, stealing, destroying or exposing information

Malware

- Ransomware
- Fileless Malware
- Spyware
- Adware
- Trojan
- Worms
- Rootkits
- Mobile Malware
- Exploits
- Scareware
- Keylogger
- Botnet
- MALSPAM
- Wiper Attack

Code Injection Attacks

- SQL Injection
- Cross-Site Scripting (XSS)
- Malvertising
- Data Poisoning

Phishing

- Spear Phishing
- Whaling
- SMiShing
- Vishing

DNS Tunneling

Supply Chain Attacks

Spoofing

- Domain Spoofing
- Email Spoofing
- ARP Spoofing

Social Engineering

- Pretexting
- Business Email Compromise (BEC)
- Disinformation Campaign
- Quid Pro Quo
- Honeytrap
- Tailgating/ Piggybacking

Identity-Based Attacks

- Kerberoasting
- Man-in-the-Middle (MITM) Attack
- Pash-the-Hash Attack
- Golden Ticket Attack
- Silver Ticket Attack
- Credential Harvesting
- Credential Stuffing
- Password Spraying
- Brute Force Attacks
- Downgrade Attacks

Denial-of-Service (DoS) Attacks

IoT-Based Attacks

Insider Threats

AI-powered attacks

- Adversarial AI/ML
- Dark AI
- Deepfake
- AI-Generated Social Engineering

12 Most Common Types of Cyberattacks Today – CrowdStrike (updated July, 2024)

What is Cyber Resilience?

"The ability to anticipate, withstand, recover from & adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment."

SP800-160 V2 R1

- Developing Cyber-Resilient Systems: A Systems Security Engineering Approach


COMPLEX PROBLEMS
require
COMPLETE
SOLUTIONS
DELL Technologies

Project Fort Zero

The US DOD developed, engineered, and invested over five years, to architect an **Advanced Zero Trust** system using their best engineers.

This is the foundation of our solution.

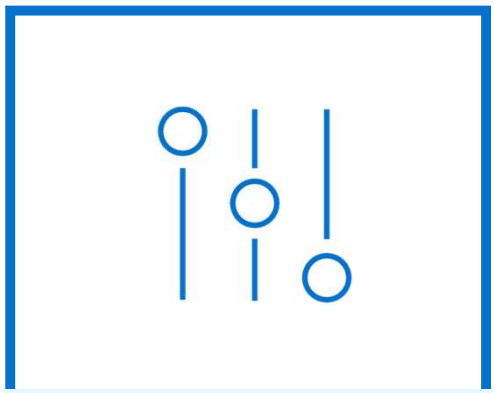
Dell will deliver…

- Capabilities integration & orchestration completed by Dell
- Repeatable ZTA blueprint
- Executive order compliance for **federally validated** solution

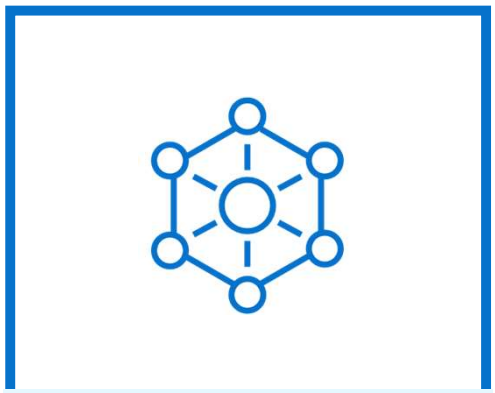
Dell brings…

- Dedicated investment
- Leading partner ecosystem
- Advanced maturity ZT
- Hybrid configurations
- Available to all industries
- Center of Excellence
- Ongoing engagement

Understanding Cyber Resilience Maturity:
Assessment & Planning



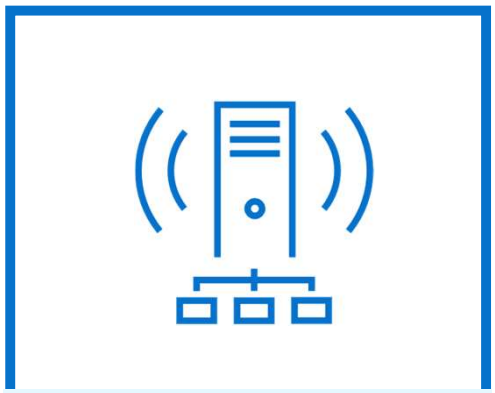
Business Controls & Governance



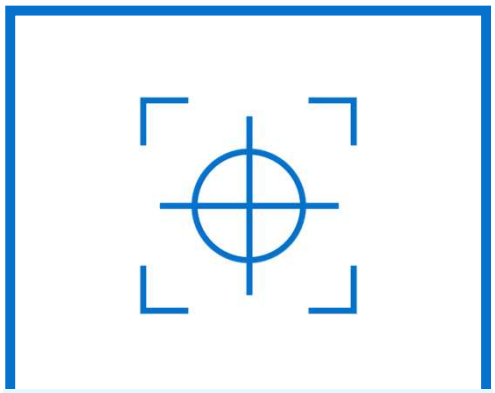
Frameworks

Education & Awareness

Understanding Cyber Resilience Maturity:
Layered Defense



Reduce the Attack Surface

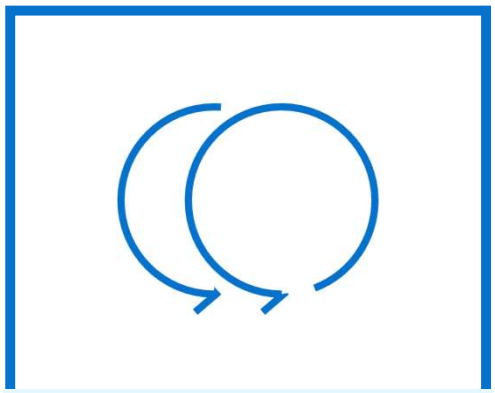


Detect & Respond to Threats

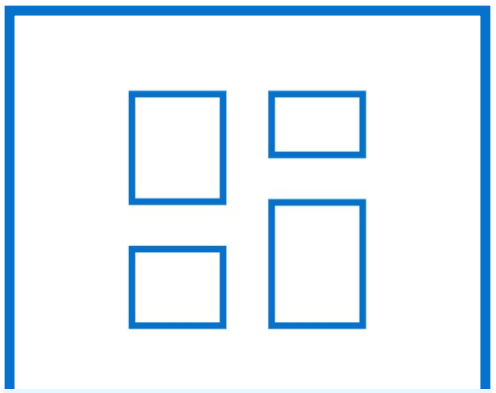
Recover from a Cyberattack

Understanding Cyber Resilience Maturity:
Visibility & Continuous Improvement

Testing & Validation



Incident Response & Recovery



Security Dashboard & Reporting

Capabilities that Support Zero Trust Principles

Dell Data Protection

Data Isolation | Immutability | Encryption | Dual Role Authorization | System lockdown | Drift detection | Secure enterprise key management | TLS 1.3 | IPv6 | Multi-factor authentication | Single sign-on | Role based access | STIG Hardening | DDBoost

Dell Server Platforms

Software bill of materials | Secure component verification | Silicon Root of Trust | System lockdown | Drift detection | Secure enterprise key management | TLS 1.3 | IPv6 | Multi-factor authentication | Single sign-on | Role based access

Dell Services

Zero Trust Advisory | Zero Trust Networking | Zero Trust Identity | Zero Trust with Microsoft

Dell HCI / CI

Hardware root of trust | Digitally signed updates | Key management | Secure logging | Distributed virtual switches | VM isolation | Authentication & authorization | Continuously validated states | Software code integrity | Electronic compatibility matrix

Dell Storage Platforms

Data isolation | Data immutability | Threat detection | Access control authentication | Data encryption | STIG hardening | HW Root of Trust | Secure boot | Digitally signed firmware | Role-based access | Extremely space efficient, secure snapshots

Dell Edge Solutions

Hardware root of trust | Secure boot chain of trust | Identity access management | Secure device onboarding | Digitally signed OS / updates | System lockdown | Secure OS/application delivery | Secure Component Verification

Dell Endpoint Solutions

BIOS/firmware security | hardware security | supply chain assurance | threat management software (EDR, XDR) | network and cloud data protection software

Dell APEX AIOps

Continuous security misconfiguration monitoring, notifications and recommendations | Common vulnerability and exposure advisories and recommendations | Storage anomaly detection for early ransomware detection and notification

Dell Network Switches

SmartFabric | SD-WAN | VLAN segmentation | Enterprise SONiC | Access control lists | RADIUS | TACACS+ | Cryptography | Secure boot | Switch hardening | Micro-segmentation | Virtual routing & forwarding | Federal certifications

Immutability ≠ Invulnerable

Good enough is not good enough

im·mu·ta·ble | \ (ˌ)i(m)-ˈmyü-tə-bəl \

Definition of *immutable*
: not capable of or susceptible to change

in·vul·ner·a·ble | \ (ˌ)in-ˈvəl-n(ə-)rə-bəl , -nər-bəl \

Definition of *invulnerable*
1: incapable of being wounded, injured, or harmed
2: immune to or proof against attack

"Immutability is used differently by vendors and varies in implementation and effectiveness. Therefore, it's important to understand what each vendor means by "immutable" and how its functionality is implemented to assess the risk that hackers can override it."

- Gartner

PowerProtect Data Domain built-in security features

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

End-to-End Encryption
Data in Flight TL2 1.2 256 Bit | Data at Rest FIPS 140-2 Crypto Libraries

Multi-factor Authentication (MFA) - RSA
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

What the Experts are Saying

Good enough is not good enough

"Offline backups (or backups that are verified as **inaccessible to attackers with full control of production IT**) must be available for all critical systems, data and infrastructure, including core IT infrastructure such as Active Directory ("AD"), with a well-defined and tested restore procedure that includes verification of ability to recover all systems to a common point-in-time."

- Conti cyber attack on the HSE: Independent Post Incident Review
  03 December 2021
  PricewaterhouseCoopers (PwC)
  Full Report

3 I's of Cyber Recovery

Modern threats require modern solutions

Isolation

Physical & logical separation of data

Protected with operational air gap either on-premises, public cloud or multi-cloud environments

Immutability

Preserve original integrity of data

Multiple layers of security and controls protect against destruction, deletion and alteration of vaulted data

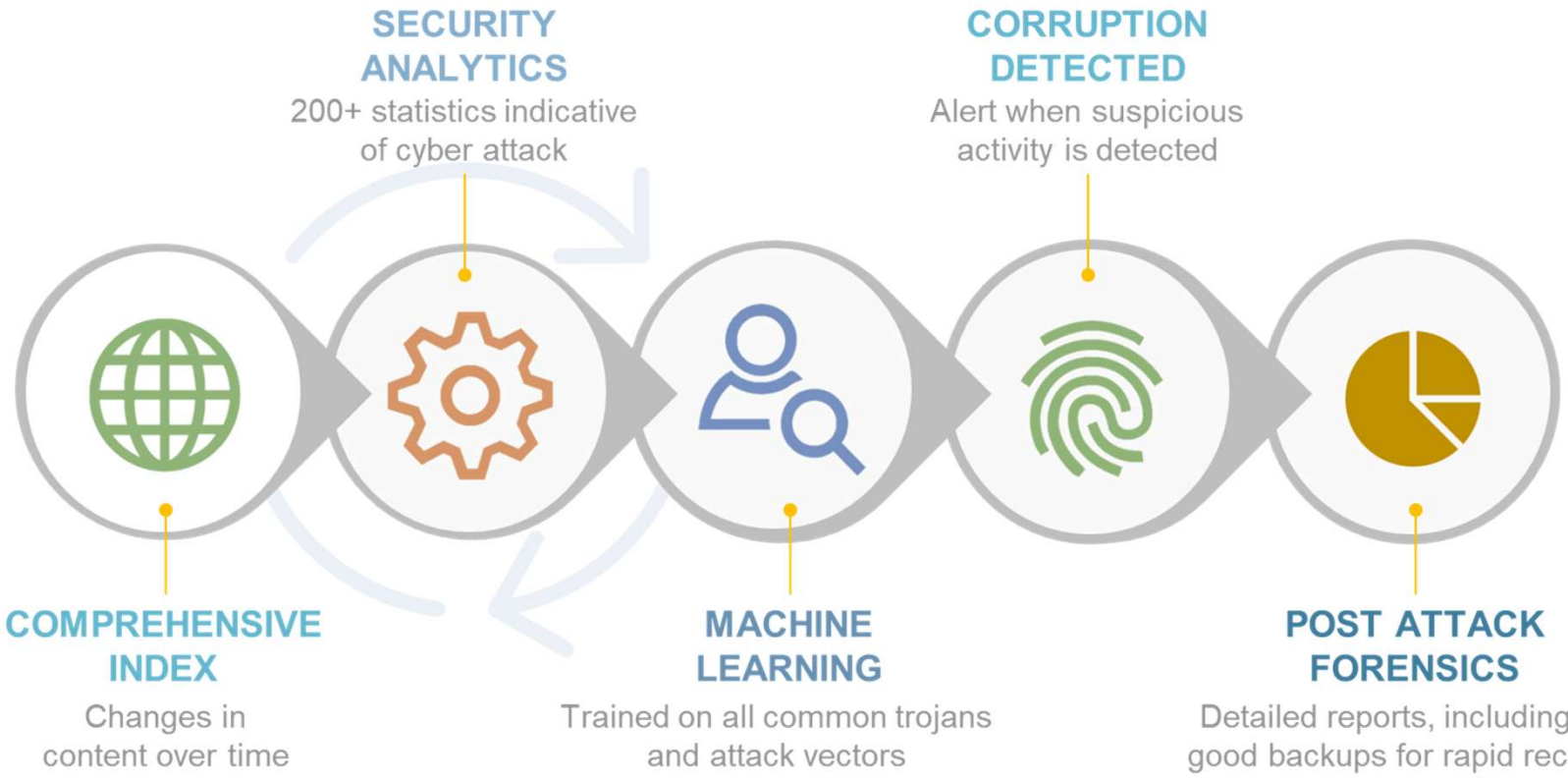
Intelligence

ML & analytics identify threats

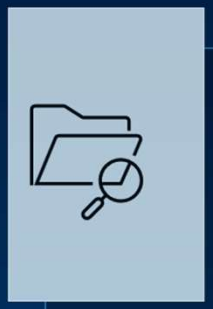
Enables assured recovery of good data and offers insight into attack vectors from within the vault

CyberSense Workflow

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



The Importance of Data Integrity



Efficient Detection

- Direct scanning of backups/snapshots, no rehydration.
- Saves time and compute resources without allowing malware to spread.

Faster Recovery

- Identifies last-known good copy of data, immediate recovery.
- Eliminates the need for mass data restores and reduces recovery time.

Minimizing Data Loss

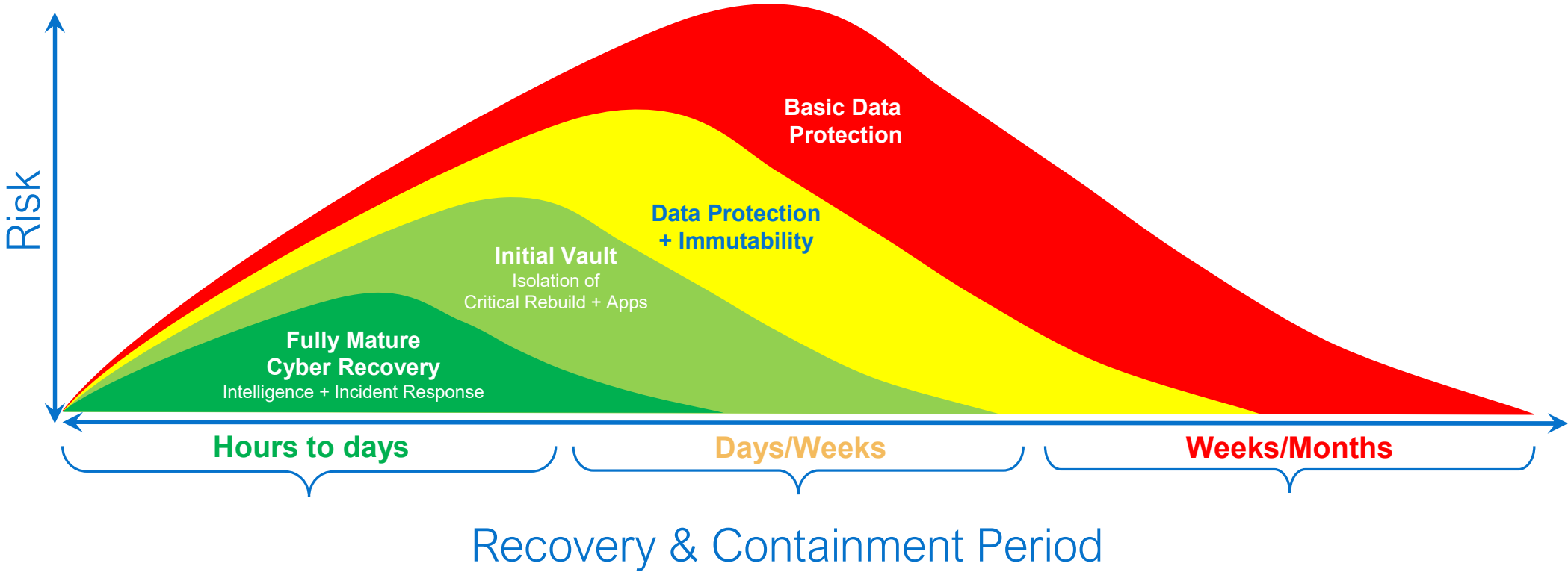
- Detailed listing of corrupted files for curated recovery.
- Avoid mass restores that overwrites clean data

Mitigating Future Risk

- Detailed forensic analysis of blast radius.
- Telemetry data points to proactively stop attacks in the future.

Stronger Resilience = Better Outcomes

Reduce Risk, Speed Recovery & Lower Costs



Incident Response & Recovery

Approach to Cyber-Incidents: Best Practices & Methodology

Phase I
Steps: 1 - 4

Phase II
Step: 5

Phase III
Steps: 6 - 8

Phase IV
Step: 9

Phase V
Step: 10

DETECTION, NOTIFICATION & PROTECTION

THREAT HUNTING & ANALYSIS

CONTAINMENT & ERADICATION

RECOVERY & STABILIZATION

MONITORING & DOCUMENTATION

5 Phase approach to Incident Response

DELL Technologies

US Department of the Air Force:
Zero Trust Strategy

- **Applications and Workloads:**
  - Application-Level Visibility and Control
- **Data:**
  - Data As The New Perimeter
- **Users:**
  - Right Access, To The Right Entity, For The Right Reason
- **Endpoint Devices:**
  - Reduce The Risk Created By Any Single Device
- **Network and Environment:**
  - Access To Protected Resources Anytime, Anywhere
- **Automation and Orchestration:**
  - Automated Security Responses Based on Security Policies
- **Visibility and Analytics:**
  - Improve Detection and Reaction Time

"The greatest risk to this strategy is institutional resistance to change.

This massive cultural shift requires all DAF communities to adapt in uncomfortable ways and participate in its collective cybersecurity mission."

Combine a holistic architecture with a proactive strategy

Where to begin …

Focus on unifying key components and ensuring gaps are identified and filled continuously

1. Begin with a strategic advisory or risk assessment to understand how to **Reduce Exposures**
2. **Protect Data and Assets** across the IT ecosystem
3. **Manage Proactively** and increase end-to-end resilience

Unified
Risk management

Proactive
SecOps

Resilient
Architecture, devices & infrastructure

DELL Technologies

Jason Proctor

Advisory Systems Engineer,
Cyber Resilience & Compliance

jason.proctor@dell.com
+1 773.217.2479

Geography: Chicago, IL (US Central Time)

Follow me on: X (Twitter) LinkedIn

DELL Technologies
Data Protection Systems
Global Technology Office

DELL Technologies

DELL Technologies

Thank you for viewing this Dell Technologies presentation! Carahsoft is the distributor for Dell Technologies public sector solutions available via GSA, ITES-SW, MHEC, and other contract vehicles.

To learn how to take the next step toward acquiring Dell Technologies' solutions, please check out the following resources and information:

For additional resources:
carah.io/DellResources

For additional Dell Technologies solutions:
carah.io/DellSolutions

To purchase, check out the contract vehicles available for procurement:
carah.io/DellContracts

For upcoming events:
carah.io/DellEvents

For additional public sector solutions:
carah.io/DellSolutions

To set up a meeting:
Dellgroup@carahsoft.com or 866-Dell-2-Go

carahsoft

For more information, contact Carahsoft or our reseller partners:
Dellgroup@carahsoft.com | 866-Dell-2-Go