VIRGINIA
IT AGENCY

APRIL ISOAG MEETING

VIRGINIA IT AGENCY

AGENDA

- DOUG POWERS & LOUCIF KHAROUNI, DELOITTE
- JUERGEN BAYER, HP
- DAVID FINLEY, DELL
- UPCOMING EVENTS
- ADJOURN

THERE ARE NO SLIDES AVAILABLE FOR THIS PRESENTATION.

LIVE DEMO

HP PC Security

The World’s Most SECURE & MANAGEABLE PC’s

Juergen Bayer

HP Inc.
Senior Security
Adviser

WORKING FROM EVERYWHERE

ENDPOINT SECURITY IS MORE RELEVANT THAN EVER

A remote workforce leads to more vulnerabilities

800%

Increase in cybercrimes post Covid

FBI Aug, '20

Endpoints are a critical component of security strategy

70%

Of successful breaches start with endpoint devices

Endpoint malware breaches start with a user click (email, web, chat...)

99%

Caused by a click from an end-user

WORLD’S MOST SECURE AND MANAGEABLE PCs

2017

PROTECTION BELOW, IN, AND ABOVE THE OS

- HP Sure View
- HP Sure Start with Runtime Intrusion Detection
- HP Multi-Factor Authenticate
- HP Sure Click

2018

HARDWARE-ENFORCED SECURITY

- HP Endpoint Security Controller
- HP Sure Run
- HP Sure Recover

2019

RESILIENCE AGAINST GROWING THREATS

- Expanded Hardware Enforced Security
- HP Sure Sense
- HP Proactive Security

2020

ADVANCING SECURITY FOR UNKNOWN THREATS

- HP Sure View Reflect
- HP Pro Security Edition
- HP Sure Click Enterprise
- HP Sure Admin
- HP Tamper Lock

HP ESSENTIAL SECURITY 2021

HARDWARE-ENFORCED PROTECTION

	DEVICE	IDENTITY/PRIVACY	DATA
ABOVE THE OS		**HP SURE VIEW** Built-in Privacy Screen **HP PRIVACY CAMERA** Built-in Camera privacy shutter	
IN THE OS	**HP SURE RUN** Protect Applications with Persistence & Kill Prevention **MICROSOFT SECURED-CORE PC** Best In Class OS Security	**HP PRESENCE AWARE** Auto Login/Logoff **WINDOWS HELLO FOR AUTHENTICATION** Secure Biometric Devices	**HP SURE CLICK** Hardware-enforce secure browsing/viewing solution **HP SURE SENSE** Protect from never-before-seen malware
BELOW THE OS	**HP BIOSPHERE** Comprehensive BIOS Management **HP SURE START** Self-Healing Endpoint Security Controller Protection **HP SURE RECOVER** Embedded Image Recovery **HP SURE ADMIN** Crypto **HP TAMPER LOCK** Tamper Protection		**HP SECURE ERASE** Permanent Data Removal on HDD/SSD **CERTIFIED SELF-ENCRYPTING DRIVES** HW Data Encryption

HP MIK
Centralized Security Management

HP IMAGE ASSISTANT
Enforcement, Monitoring and Analytics

HP CMSL
PowerShell Script Library for Client Management

HP ENDPOINT SECURITY CONTROLLER

HP ENDPOINT SECURITY CONTROLLER

UNIQUE HARDWARE ENABLES RESILIENT DEVICES

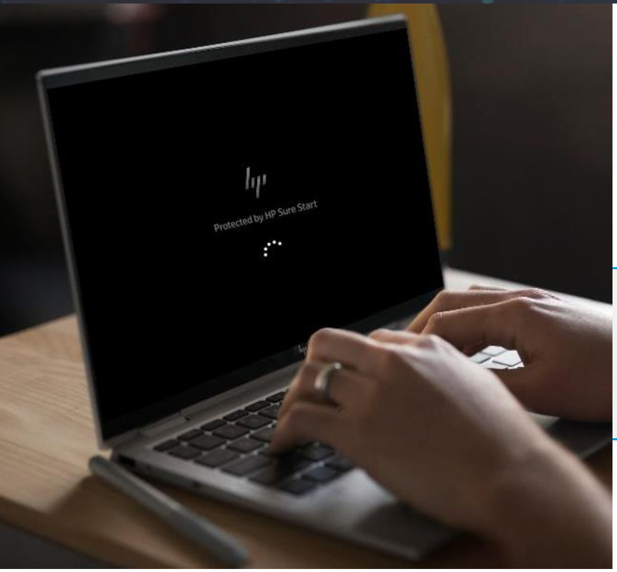
- ✓ Physically isolated
- ✓ Cryptographically secured
- ✓ Secure storage

3RD PARTY CERTIFIED

by an accredited independent test lab (Overseen by ANSSI)

HP Sure Start | HP Sure Admin | HP Sure Recover | HP Tamper Lock

HP SURE START



PROTECT WHERE ANTIVIRUS DOESN’T

Protecting your BIOS with **HP Sure Start** creates a **HARDENED ROOT OF TRUST.**

HP SURE START IS THE

WORLD’S FIRST SELF-HEALING BIOS

HP SURE RECOVER

FAST, SECURE, AUTOMATED

EMBEDDED IMAGE RECOVERY ANYTIME, ANYWHERE WITHOUT IT ENGAGEMENT

AUTOMATIC RECOVERY

if no OS is found.

SCHEDULED REIMAGING

to the corporate image.

USER EMPOWERMENT

reimage without IT.

HP SURE ADMIN

MANAGE WITHOUT PASSWORDS

Centralized protection of private keys used to authorize remote management and local access.

LOCAL ACCESS AUTHENTICATOR

Gain local access to firmware setup using One-Time-Passcodes provided by the HP Sure Admin app

REMOTE MANAGEMENT TOOLS

Remotely Manage firmware settings securely without passwords.

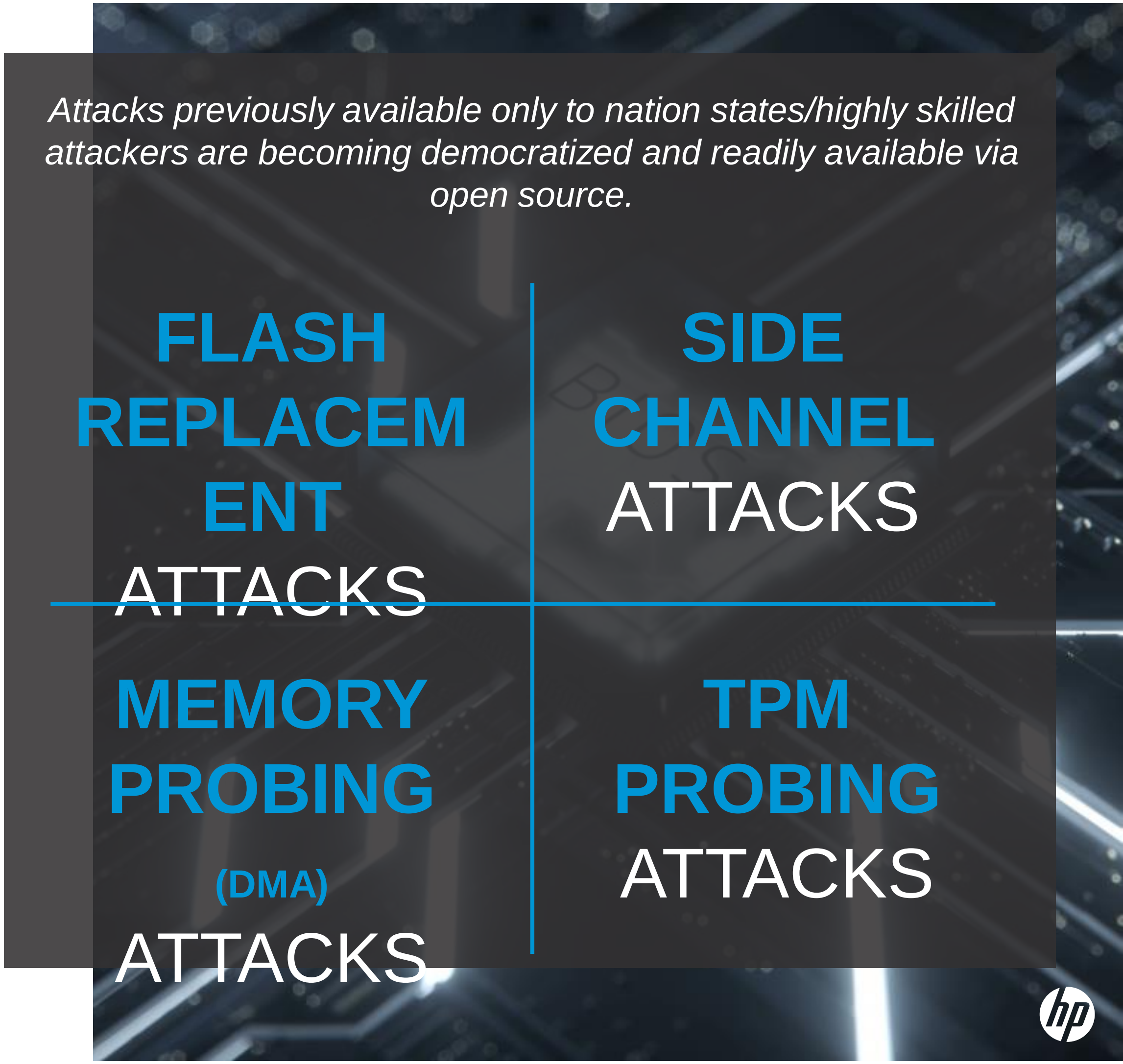
FACTORY PROVISIONING

Optional custom service to pre-install customer keys for zero-touch management of firmware settigns

HP TAMPER LOCK

Providing protection from physical attacks, which involve disassembly of the system to modify the hardware or implant attacker hardware.

- **Sensors** to detect if the case has been opened, and **rich policy controls** to configure what action is taken if this has occurred.
- Other physical attack protections, such as **DMA attack protection** and protected storage via the **HP Endpoint Controller** hardware.



Attacks previously available only to nation states/highly skilled attackers are becoming democratized and readily available via open source.

FLASH REPLACEMENT ATTACKS

SIDE CHANNEL ATTACKS

MEMORY PROBING (DMA) ATTACKS

TPM PROBING ATTACKS

HP Elite Dragonfly
with HP Sure View Reflect

HP SURE VIEW

FOUR GENERATIONS OF PRIVACY INNOVATION

GEN1

- World's first integrated privacy screen

GEN2

- Better performance in light & dark environments
- Improved privacy protection
- Flexibility for thinner designs
- One button on and off

GEN3

- Improved battery life
- Better Visuals with brighter display and higher contrast ratio

REFLECT

World's first reflective privacy experience

in an integrated solution using exclusive, proprietary optical technology.

- Exceptional visuals indoors and outdoors, in light environments as well as dark
- Luminance reducing copper, reflective technology

HP SURE CLICK

CLICK WITH CONFIDENCE

Hardware enforced, secure browsing solution

PROTECT AGAINST MALICIOUS WEBSITES

PROTECT AGAINST BAD ATTACHMENTS

HP SURE SENSE

PREVENT ATTACKS

by never-before-seen malware by harnessing the power of AI deep learning.

TRAIN THE BRAIN

Deep learning neural network trained on 100s of millions of malware samples.

CREATE THE AGENT

Brain distilled into the lightweight agent, turning TBs of learning into MBs of instinct.

PROTECT ENDPOINT

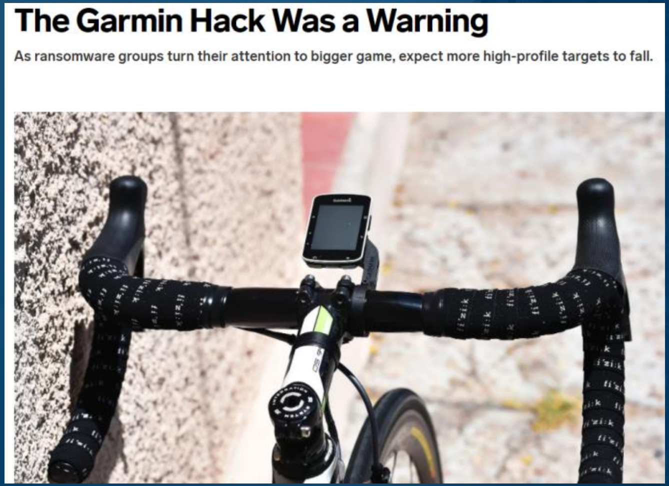
Agent scans files and quarantines likely malware.

Questions ?

Recovering Your Business from a Cyber Attack

Dell EMC PowerProtect Cyber Recovery

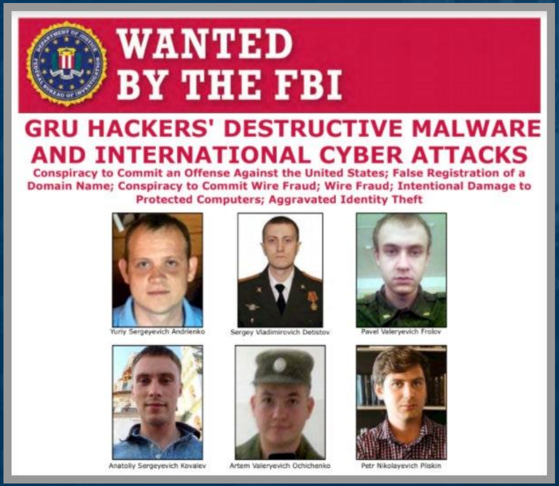
Cyber attacks are daily headlines in every market



The Garmin Hack Was a Warning

As ransomware groups turn their attention to bigger game, expect more high-profile targets to fall.

Source: Wired, Aug 2020



WANTED
BY THE FBI

GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft

Yuriy Sergeyevich Andrienko

Sergey Vladimirovich Detistov

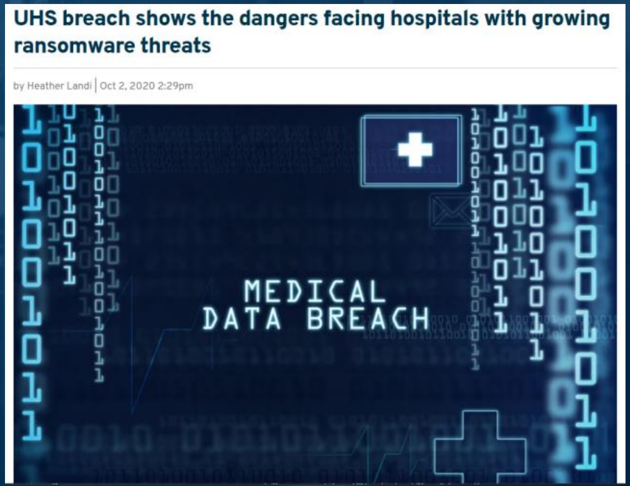
Pavel Valeryevich Frolov

Anatoliy Sergeyevich Kovalev

Artem Valeryevich Ochichenko

Petr Nikolayevich Pliskin

Source: Wired, Oct 2020

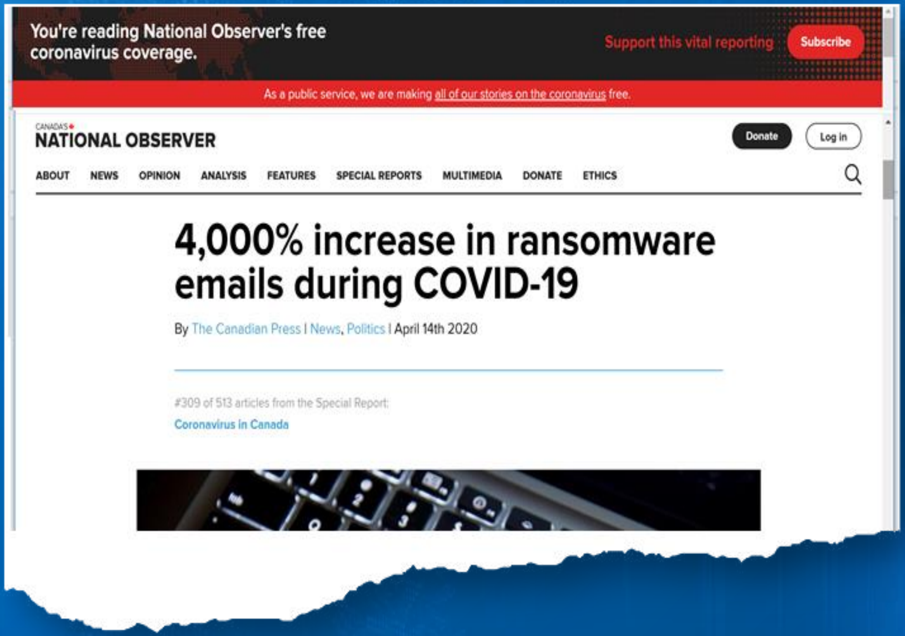


UHS breach shows the dangers facing hospitals with growing ransomware threats

by Heather Landi | Oct 2, 2020 2:29pm

Source: Fiercehealthcare.com, Oct 2020

“Cyberattacks are the fastest growing crime, and they are increasing in size, sophistication and cost…”



You're reading National Observer's free coronavirus coverage.

As a public service, we are making all of our stories on the coronavirus free.

4,000% increase in ransomware emails during COVID-19

By The Canadian Press | News, Politics | April 14th 2020

#309 of 513 articles from the Special Report:

Coronavirus in Canada

Governments, universities and private businesses have spent more than $144 million in 2020.
CRN

52% of breaches featured hacking, 28% involved malware and 32–33% included phishing or social engineering, respectively.
Verizon

Hackers attack every 39 seconds, on average 2,244 times a day.
University of Maryland

The most expensive country in terms of average total cost of a data breach is the U.S. at $8.19 million, more than twice the global average.
Ponemon Institute / IBM

What we are observing

New ransomware trend will have executives worried

According to a new report from ZDNet, some ransomware operators are no longer casting a wide net across an organization in the hopes of finding sensitive data to encrypt. Instead, they're specifically targeting computers and other devices used by managers and top executives.

www.itproportal.com/news/new-ransomware-trend-will-have-executives-worried/

They are targeting your customers Systems and Backup Admins

Where do you think all those compromised credentials go?

Large Florida school district hit by ransomware attack

The computer system of one of the nation’s largest school districts was hacked by a criminal gang that demanded $40 million in ransom or it would erase files and post students’ and employees’ personal information online

By **TERRY SPENCER and FRANK BAJAK Associated Press**
April 1, 2021, 4:14 PM
• 5 min read

FORT LAUDERDALE, Fla. -- The computer system of one of the nation's largest school districts was hacked by a criminal gang that encrypted district data and demanded $40 million in ransom or it would erase the files and post students' and employees' personal information online.

Cyber threats: the facts

A cyber attack occurs

every

39

sec

Source: Security Magazine

verizon✓

71%

of breaches are financially motivated

verizon✓

43%

of breaches involved small business

accenture

$13M

Avg cost of Cybercrime for an organization

accenture

$5.2T

of global risk over the next 5 years

Avg. cost of cyber attack

by Industry

Industry	Avg Cost
Banking	**$18.4M**
Utilities	**$17.8M**
Software	**$16M**
Automotive	**$15.8M**
Insurance	**$15.8M**
High Tech	**$14.7M**
Capital Markets	**$13.9M**
Energy	**$13.8M**
US Federal	**$13.7M**
Consumer Goods	**$11.9M**
Health	**$11.9M**
Retail	**$11.4M**
Life Sciences	**$10.9M**
Media	**$9.2M**
Travel	**$8.2M**
Public Sector	**$7.9M**

accenture

Cyber resilience: Legal and Regulatory Trends

“An air-gapped data backup architecture…”

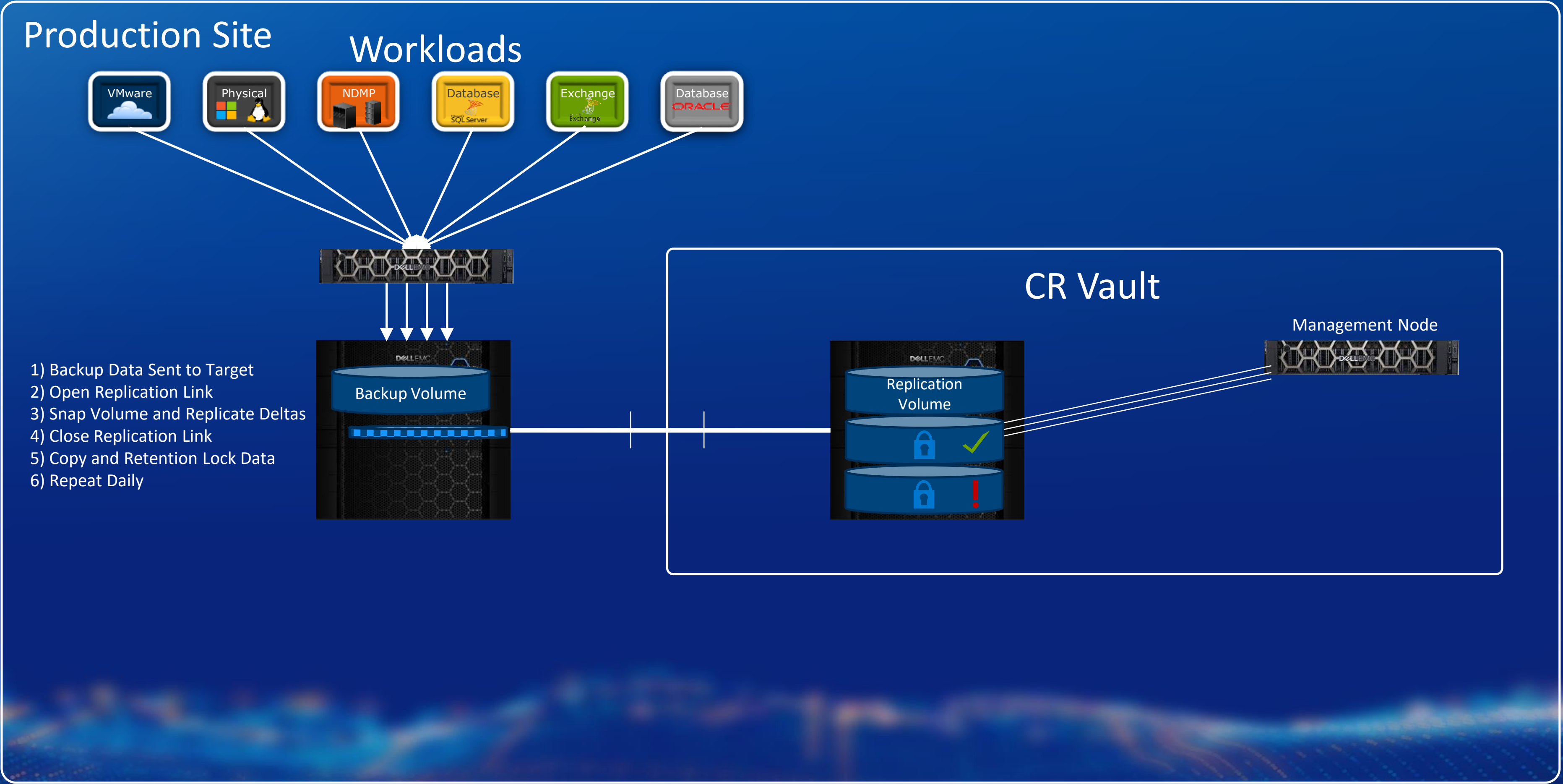
“Confidentiality, integrity, availability and resilience.”

"It is critical to maintain offline, encrypted backups of data."

"Ransomware payments may risk violating OFAC regulations."

“Ensure backups are not connected to the networks they back up.”

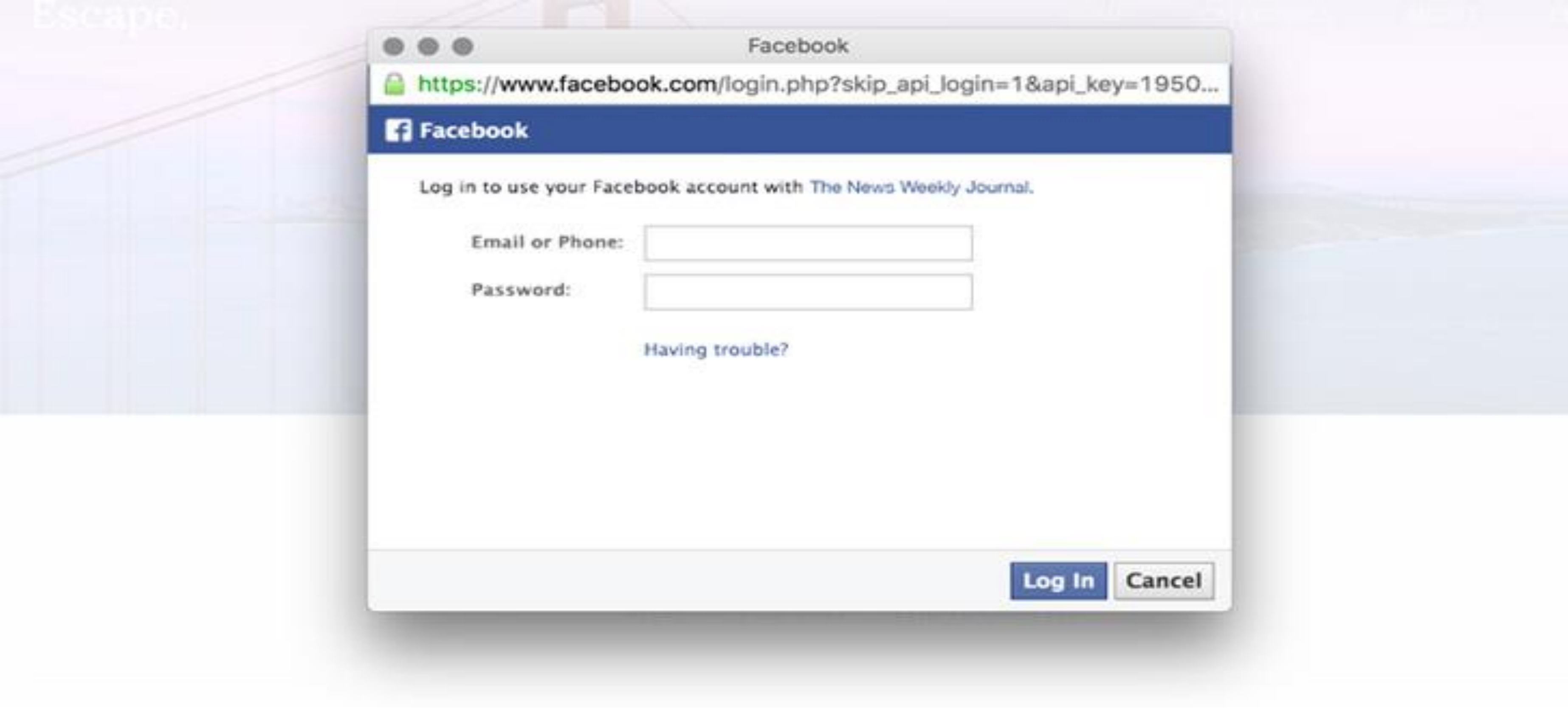
How Cyber Recovery Works



1) Backup Data Sent to Target
2) Open Replication Link
3) Snap Volume and Replicate Deltas
4) Close Replication Link
5) Copy and Retention Lock Data
6) Repeat Daily

Does this look Legit?

- How can you tell?



Facebook

https://www.facebook.com/login.php?skip_api_login=1&api_key=1950...

Facebook

Log in to use your Facebook account with The News Weekly Journal.

Email or Phone:

Password:

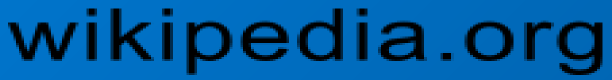
Having trouble?

Does this look Legit?

- How can you tell?

By checking if the URL is correct?
By checking if the site is using HTTPS?
Or using software or browser extensions that detect phishing domains?
By checking if the website address is not a homograph?

Credential based attacks are growing exponentially
Does this look Legit?



wikipedia.org

Is this a valid Website? https://**Terracon.com**

Nope:

It is a Homograph

An example of an IDN homograph attack; the Latin letters "e" and "a" are replaced with the Cyrillic letters "e" and "a". Computers see this address using the Cyrillic letters- You won’t get to the real Wikipedia site with this

https://www.Terracon.com

https://www.Terracon.com

You will get this (often you will go to a Bad Actor page)

This site can’t be reached
Check if there is a typo in xn--rracn-ywe1e0a.com.
If spelling is correct, try running Windows Network Diagnostics.
DNS_PROBE_FINISHED_NXDOMAIN

What if You:

Had a copy of critical data that has proven over 5 years to be 100% accessible/restorable after any Cyber Attack?

Could store the third copy securely within an Air-Gapped Cyber Vault

Could via a secure Cyber Recovery Vault, support compliance processes and detailed reporting to help meet requirements for NERC CIP 003-7, NEI 08-09, NIST 800-53, PCI DSS, GDPR, the Bulk Power Executive Order 13920, and a wide range of other global regulations.

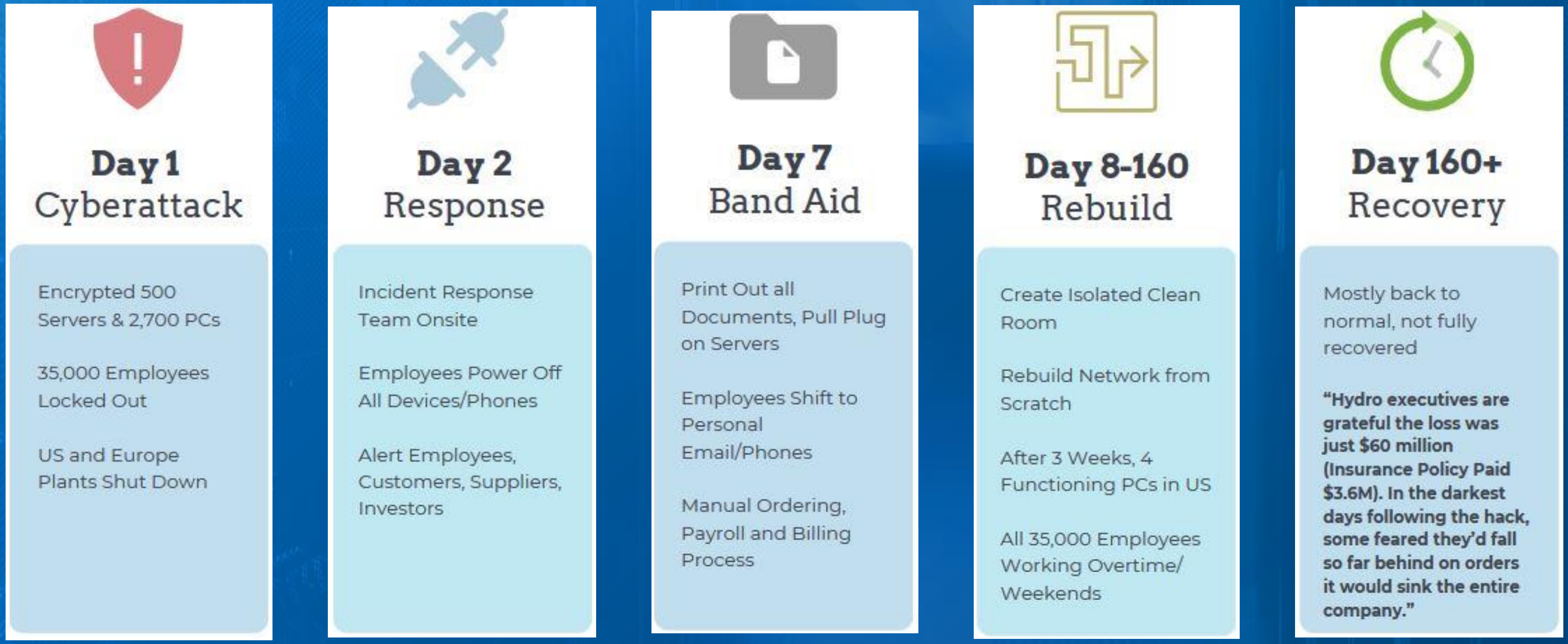
Could restore data securely minutes after a Cyber attack?

Could reduce the Risk of not being able to quickly restore to near zero?

Talking Points for the Board

Key Metrics		
	Without CR	With CR
Ransom payment decision	Dependent on threat actors and applicable laws	Not needed
Amount of ransom	Potentially millions	Not needed
Possibility of recovery	Not assured	Assured
Time to recover	A week or possibly months in a severe attack	Day(s) depending on pre-planning and attack

Case Study: Utility Company Cyber Attack



Day 1
Cyberattack

Encrypted 500 Servers & 2,700 PCs

35,000 Employees Locked Out

US and Europe Plants Shut Down

Day 2
Response

Incident Response Team Onsite

Employees Power Off All Devices/Phones

Alert Employees, Customers, Suppliers, Investors

Day 7
Band Aid

Print Out all Documents, Pull Plug on Servers

Employees Shift to Personal Email/Phones

Manual Ordering, Payroll and Billing Process

Day 8-160
Rebuild

Create Isolated Clean Room

Rebuild Network from Scratch

After 3 Weeks, 4 Functioning PCs in US

All 35,000 Employees Working Overtime/ Weekends

Day 160+
Recovery

Mostly back to normal, not fully recovered

"Hydro executives are grateful the loss was just $60 million (Insurance Policy Paid $3.6M). In the darkest days following the hack, some feared they'd fall so far behind on orders it would sink the entire company."

***Source**: Bloomberg Businessweek: How to Survive a Ransomware Attack Without Paying the Ransom July 23, 2020*

Authentication, Identity & Security

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

Networking

- Switch / router configuration
- Firewall / load-balancer settings
- IP Services design
- Access Control configuration
- Firmware / Microcode / Patches

Storage

- SAN / Array configurations
- Storage Abstraction settings
- Backup Hardware configuration
- Firmware / Microcode / Patches

Intellectual Property

- Source code
- Proprietary algorithms
- Developer libraries

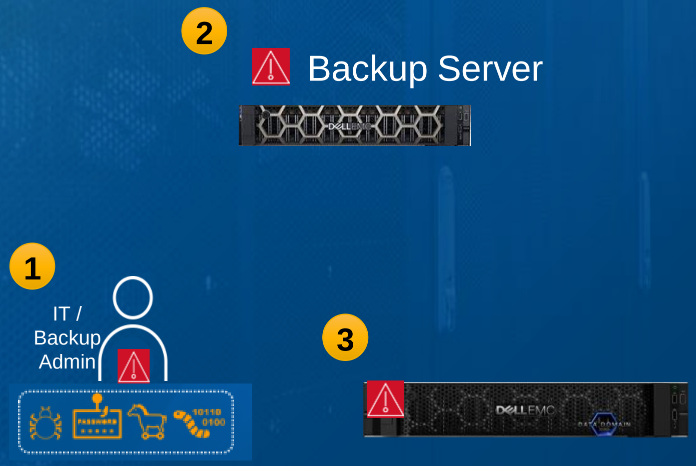
Host and Build Tools

- Physical/Virtual Platform Builds
- Dev Ops tools & automation scripts
- Firmware / Microcode / Patches
- Vendor software
  - Binaries (golden images)
  - Configurations & settings

Documentation

- CMDB / asset management extracts
- D/R and Cyber Recovery Run-books & Checklists
- HR Resources & Contacts Lists

Ransomware Increasingly Targeting Primary Backups



1 **IT & Backup Admins are main targets for compromise through a variety of attack vectors because their access is trusted and can easily and rapidly become the effective change agent to carry out an attack**

2 **Backup Software (Backup Catalog):** Backup master server is targeted and infected resulting in encrypted/wiped backup catalog, or pre-mature policy expiration

3 **Backup Target:**

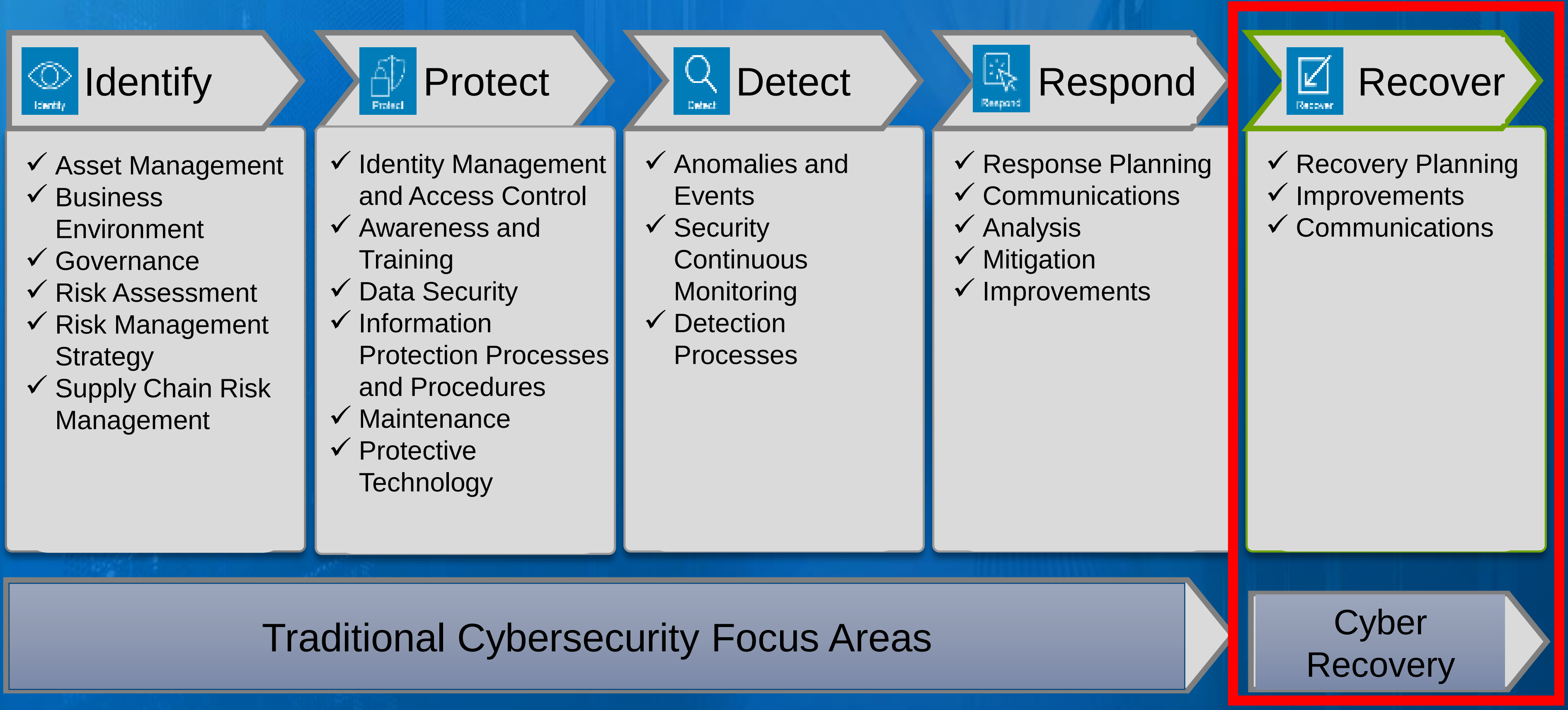
Filesystems on the media server are targeted and encrypted/wiped. Backup repositories can become encrypted/wiped from ransomware crawling network file shares

Disaster Recovery is not Cyber Recovery

Disaster Recovery / Business Continuity is Not Enough to Address Modern Cyber Threats

Category	Disaster Recovery	Cyber Resilience
Recovery Time	Close to Instant	Reliable & Fast
Recovery Point	Ideally Continuous	1 Day Average
Nature of Disaster	Flood, Power Outage, Weather	Cyber Attack, Targeted
Impact of Disaster	Regional; typically contained	Global; spreads quickly
Topology	Connected, multiple targets	Isolated, in addition to DR
Data Volume	Comprehensive, All Data	Selective, Includes foundational services
Recovery	Standard DR (e.g. failback)	Iterative, selective recovery; part of CR

NIST Framework



Identify

- ✓ Asset Management
- ✓ Business Environment
- ✓ Governance
- ✓ Risk Assessment
- ✓ Risk Management Strategy
- ✓ Supply Chain Risk Management

Protect

- ✓ Identity Management and Access Control
- ✓ Awareness and Training
- ✓ Data Security
- ✓ Information Protection Processes and Procedures
- ✓ Maintenance
- ✓ Protective Technology

Detect

- ✓ Anomalies and Events
- ✓ Security Continuous Monitoring
- ✓ Detection Processes

Respond

- ✓ Response Planning
- ✓ Communications
- ✓ Analysis
- ✓ Mitigation
- ✓ Improvements

Recover

- ✓ Recovery Planning
- ✓ Improvements
- ✓ Communications

Traditional Cybersecurity Focus Areas

Cyber Recovery

Analytics SW on Vaulted Data

Machine Learning AI for Cyber Analytics

- Software that runs on Server(s) Isolated in the Cyber recovery Vault
- Taught how to recognized compromised data (IOC) by introducing over 1700 Variants
- Both Meta Data and Deep Content Data Analysis
- Use of Similarity Mining techniques and distance measures along with Entropy of blocks/chunks of examined files to create similarity matrix between observations
- Examines Data behavior patterns and intrinsic data characteristics of multiple observations of the data leading to 99.5% accuracy in finding Malware IOC's

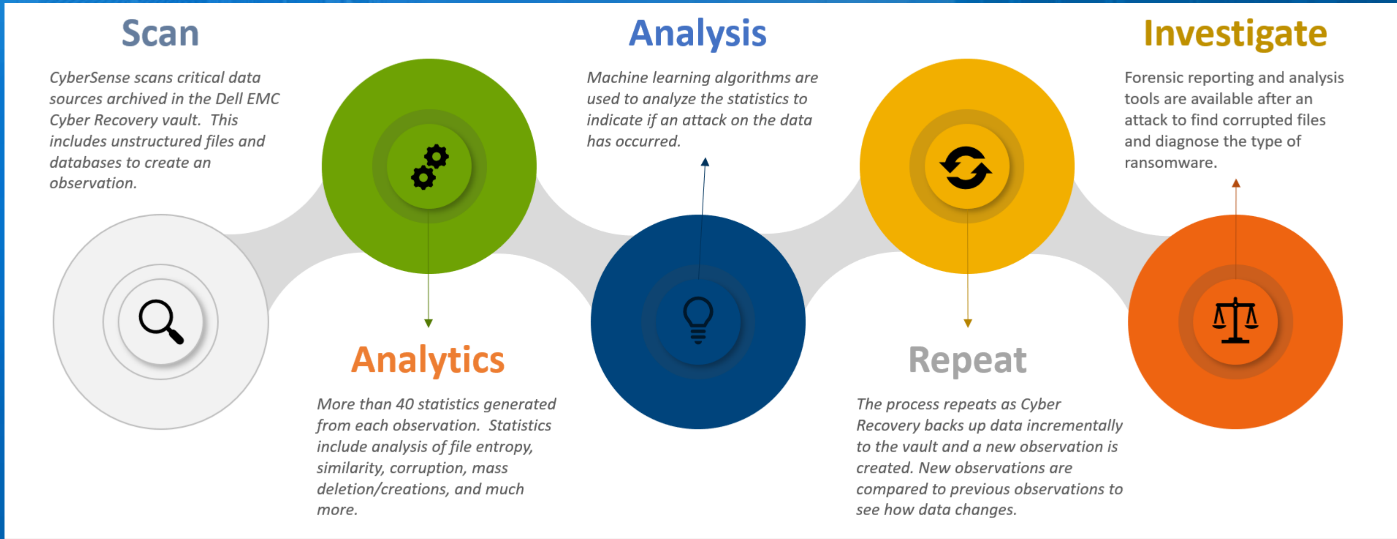
Characteristics of a Zero Day(the future of finding Zero day Malware)

- Unknown variants of existing malware that obfuscate their behaviour to evade from detection. These malware are called zero-day malware (new malware) as there are zero-days between the unknown malware's first attack and the time it is discovered. Such attacks are also called zero-day attacks.

- Malware writers make use of metamorphic and polymorphic engines to generate new dissimilar malware variants for zero-day attacks. A "similarity analysis" can quantify the level of similarity and the difference between two binary executables.

- Example: Register reassignment transformation→Replaces code between registers=Zero Day

Daily Workflow
Finding Indicators of Compromise inside the Vault



Scan

CyberSense scans critical data sources archived in the Dell EMC Cyber Recovery vault. This includes unstructured files and databases to create an observation.

Analytics

More than 40 statistics generated from each observation. Statistics include analysis of file entropy, similarity, corruption, mass deletion/creations, and much more.

Analysis

Machine learning algorithms are used to analyze the statistics to indicate if an attack on the data has occurred.

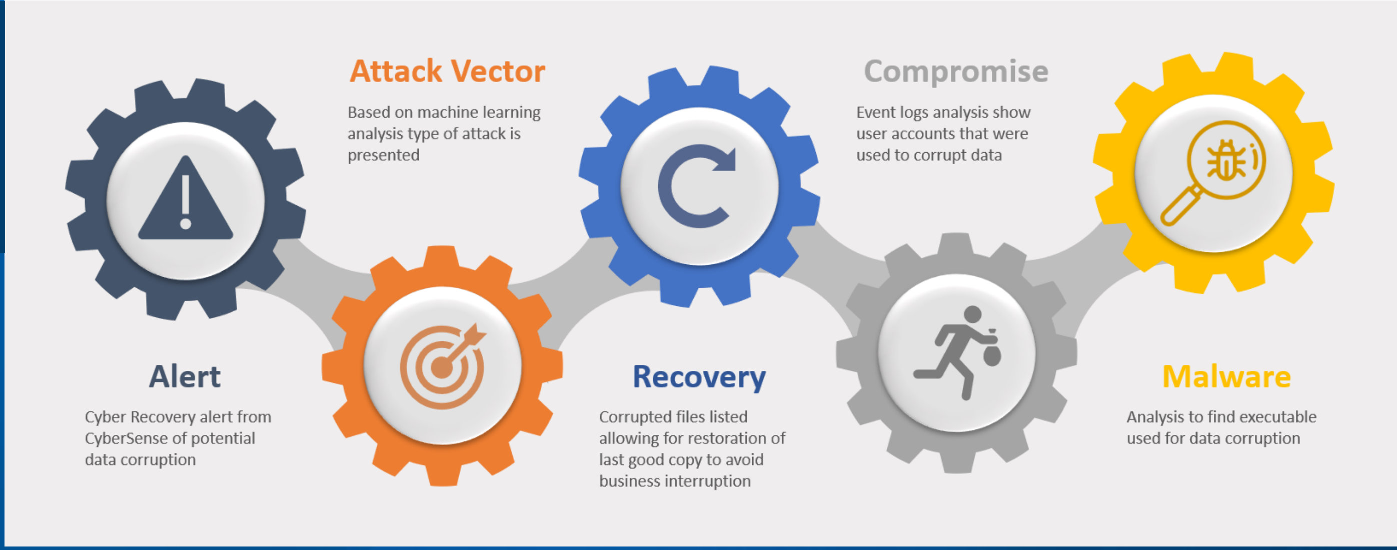
Repeat

The process repeats as Cyber Recovery backs up data incrementally to the vault and a new observation is created. New observations are compared to previous observations to see how data changes.

Investigate

Forensic reporting and analysis tools are available after an attack to find corrupted files and diagnose the type of ransomware.

Post Attack Recovery and Diagnosis
Replace Corrupted Files and Clean Up Malware



Alert

Cyber Recovery alert from CyberSense of potential data corruption

Attack Vector

Based on machine learning analysis type of attack is presented

Recovery

Corrupted files listed allowing for restoration of last good copy to avoid business interruption

Compromise

Event logs analysis show user accounts that were used to corrupt data

Malware

Analysis to find executable used for data corruption

DELL Technologies

UPCOMING EVENTS

2021 Virtual Commonwealth of Virginia Information Security Conference

Registration is now open! The theme of the conference is “2021 Cybersecurity Reboot: Tools for building cyber resilience.” In addition to break-out presentations, the conference program will feature two keynote addresses.

Date: June 24
Location: Virtual! Event will be hosted by the College of William & Mary.
Registration cost: $25 for conference, which covers access to top-notch speakers and presentations, as well as a conference swag bag (mailed to participants).
Conference website: https://www.vita.virginia.gov/information-security/security-conference/
Questions: covsecurityconference@vita.virginia.gov

Keynote Speakers

SUSAN ADAMS

CHIEF TECHNOLOGY OFFICER

MICROSOFT FEDERAL

LARRY WEAVER

PROFESSIONAL COMEDIAN AND

BUSINESS LEADER

Agency Security Awareness Training Form Reminder

Please complete the form in Archer by April 16. If you do not have access to Archer, you may submit your completed form to Commonwealthsecurity@vita.virginia.gov

The form is located at the link below: https://www.vita.virginia.gov/policy--governance/itrm-policies-standards/

If you questions about completing the form, contact: Tina.gaines@vita.virginia.gov

NEXT ISOAG MEETING

May 5 from 1- 4 p.m.

- Greg Williams, EY
- Ben Timms, HP
- Eric Robinson, KLDiscover

VIRGINIA
IT AGENCY

THANK YOU FOR ATTENDING