The Financial Kill Switch for Ransomware 2026

RICOH
imagine. change.

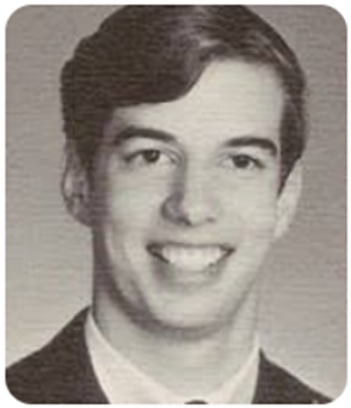
Presenters:
Richard Hyde - Strategic Solutions Consultant

Did you know…

What year was the first ransomware attack?

Bonus Questions

Who was the author, and what was the attack?



Author – Dr Joseph Popp
Year deployed -- 1989

Delivery: Distributed via floppy disks labeled *"AIDS Information – Introductory Diskettes"*.

The Trigger: After a user rebooted their computer 90 times, the malicious program hid directories and encrypted file names, rendering the data inaccessible.

The Ransom: Victims were instructed to mail a payment to PC Cyborg Corporation at a post office box in Panama.

Ransomware is no longer an IT issue.

RICOH
imagine. change.

It’s a Business interruption and financial risk problem

Average Impact Includes:

Revenue loss from downtime

Regulatory penalties (privacy, critical infrastructure laws)

Recovery costs (IR, legal, rebuild)

Reputational damage impacting valuation

Traditional defenses (EDR, backups, firewalls) are preventative not designed to stop lateral spread once breach

Ransomeware: A Shared Threat

RICOH
imagine. change.

City of Dallas

27,000 impacted and a
cost of $8.5M

MGM Grand Casino

Operations, including gaming, shut for
10+ days at a cost of $100M

London Drugs

All 79 stores closed for over a week.
Ranson demanded: 25M

City of Hamilton

80% of city systems offline; licensing, tax, transit and phone system disrupted.

Estimated cost 18.M plus 33.6M for cybersecurity modernization

SWAHN
SouthWestern Academic Health Network

Healthcare Network – 7.4M

Windsor Regional Health
Bluewater Health
Chatham-Kent Health Alliance
Erie Shores HealthCare

Indigo

Indigo Books

Locbit crippled POS systems, ecommerce, payroll and internal operations
Estimated Cost 26.5M

Why Is Ransomware Resilience Mission Critical?

RICOH
imagine. change.

Business Continuity

Ransomware can cripple core systems — from customer service to supply chains.

Regulatory & Legal Pressures

Data protection laws (like GDPR, HIPAA, NIS2, DORA) require rapid breach reporting and mitigation.

Reputation & Customer Trust

Demonstrating resilience shows clients, investors, and regulators that you're a trustworthy, secure organization.

Recovery Is Hard!

Even companies with backups often can't recover all their data (only 13% fully do)
57% Average Data Recovery – calamu.com

The Financial Impact Is Severe

Businesses lose money from downtime, fines, settlements, loss of revenue. **34%** take more than a month to recover

It's Not If You'll Be Targeted

"It's *When*
Resilience = preparation + containment + recovery + continuity."

Traditional Security Stack

RICOH
imagine. change.

Defense-in-Depth Architecture

Customer Challenge

THE PROBLEM IS …

You can't have100% protection - 100% of the time.

Prevention-Only Strategies Require That …

- ✓ You're 100% Effective100% of the Time
- ✓ On 100% of Your Attack Surfaces
- ✓ Against 100% of Threats, That Are Forever Evolving In Their Sophistication

What you require is Ransomware Resilience.

Enhanced Security Stack

RICOH
imagine. change.

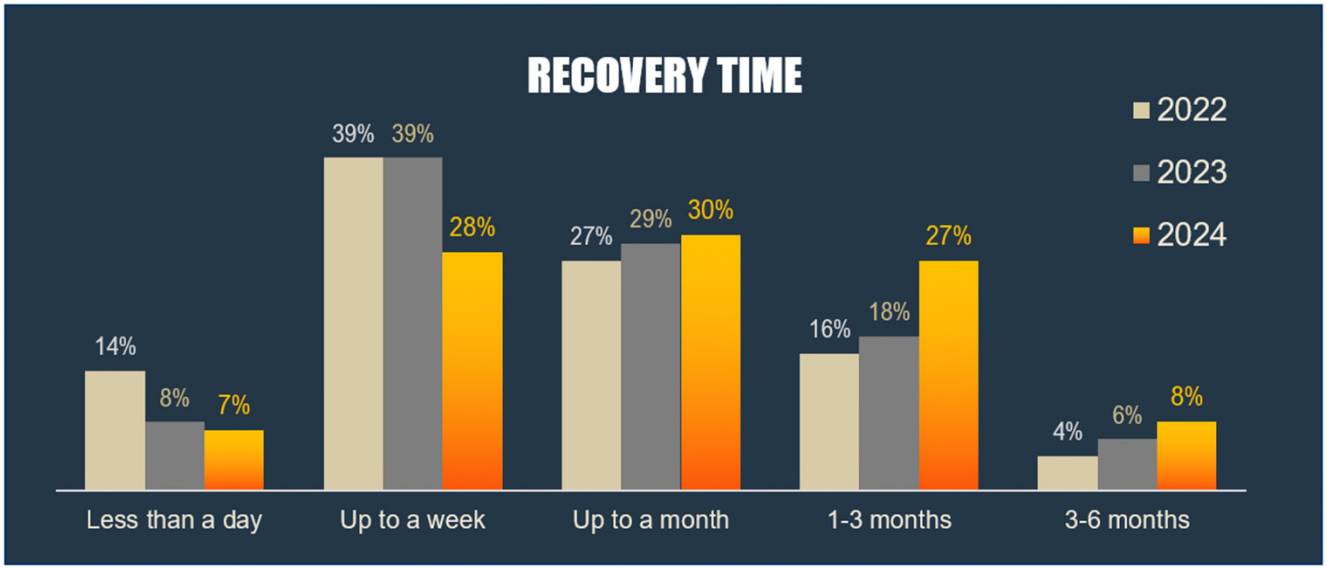
Ransomware Containment at the Core

Canada Has a Ransomware Problem

- 7,000 expected ransomware attacks by the end of 2026, up by 2,000 attacks since 2024.
- A recent survey says over 50 percent of small businesses have reported a cyber incident.
- We are the 2nd most attacked country in the world.
- We experienced 30 significant breaches in 2025 – 6.7% of significant worldwide breaches.
- IT makes up 18% of attacks. Transportation is 13%.

Operational Impact of Ransomware

2022	2023	2024
Ransomware Attacks: YOY Increase		
66%	66%	59%
Recovery Costs		
$1.4M	$1.82M	$2.73M



Constantly Evolving Attacks

Cybercriminals are rapidly evolving their attack strategies by leveraging data, AI and vulnerabilities

Recovery Cost is Increasing

The number of attacks have decreased but recovery cost increased by 50%

- Increase in cyber insurance premium
- Increase in ransomware payments

Operational Downtime

Recovery cost is directly related to an ability to rapidly recover from an attack

Source: The State of Ransomware Report 2024 by Sophos

Not another Endpoint Solution

RICOH
imagine. change.

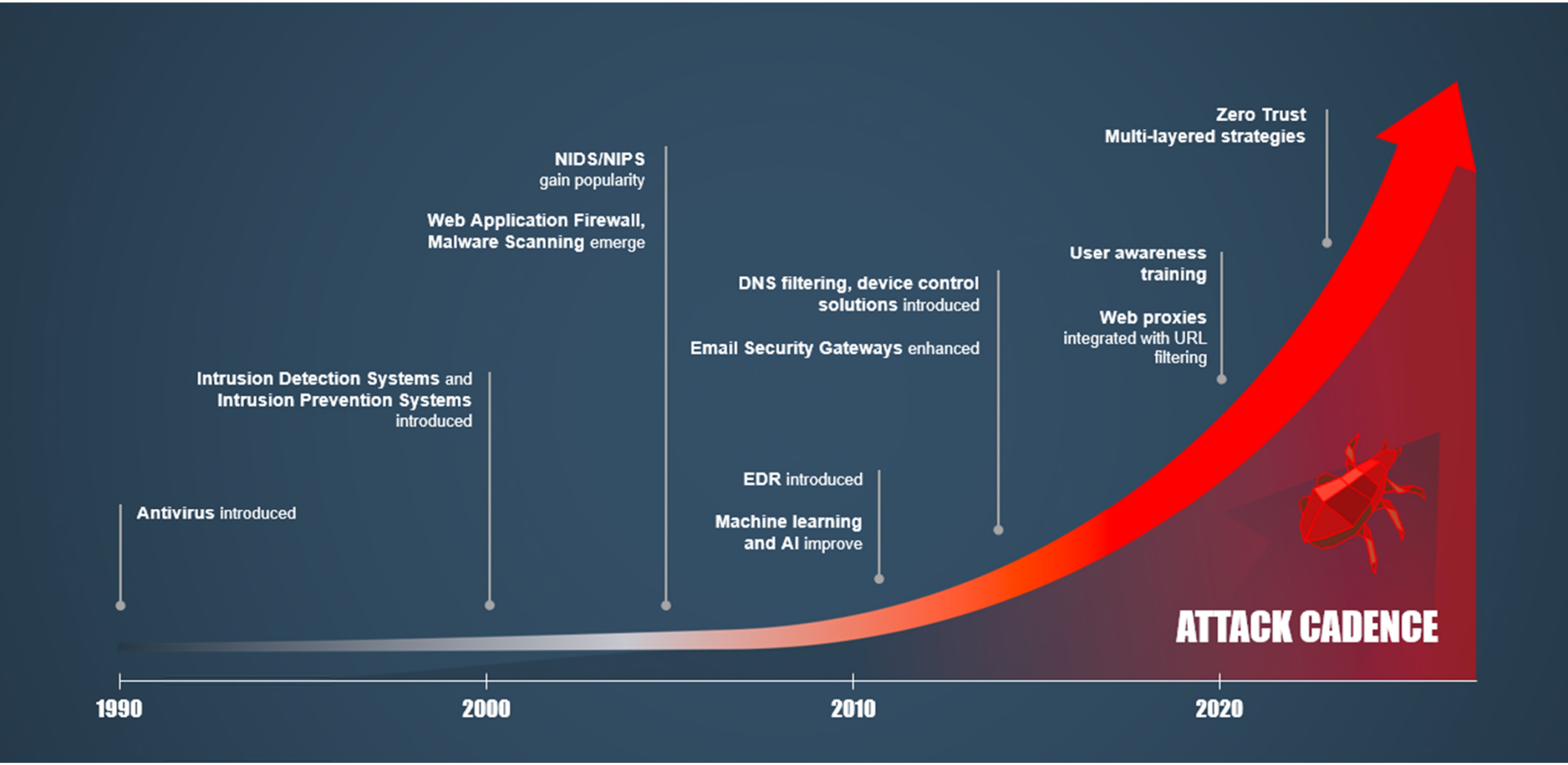
The Ultimate Companion

CROWDSTRIKE
CYLANCE
Carbon Black.
DARKTRACE
eset
Symantec

SentinelOne
TREND MICRO
McAfee
cisco AMP for Endpoints
Microsoft Defender for Endpoint
KASPERSKY lab

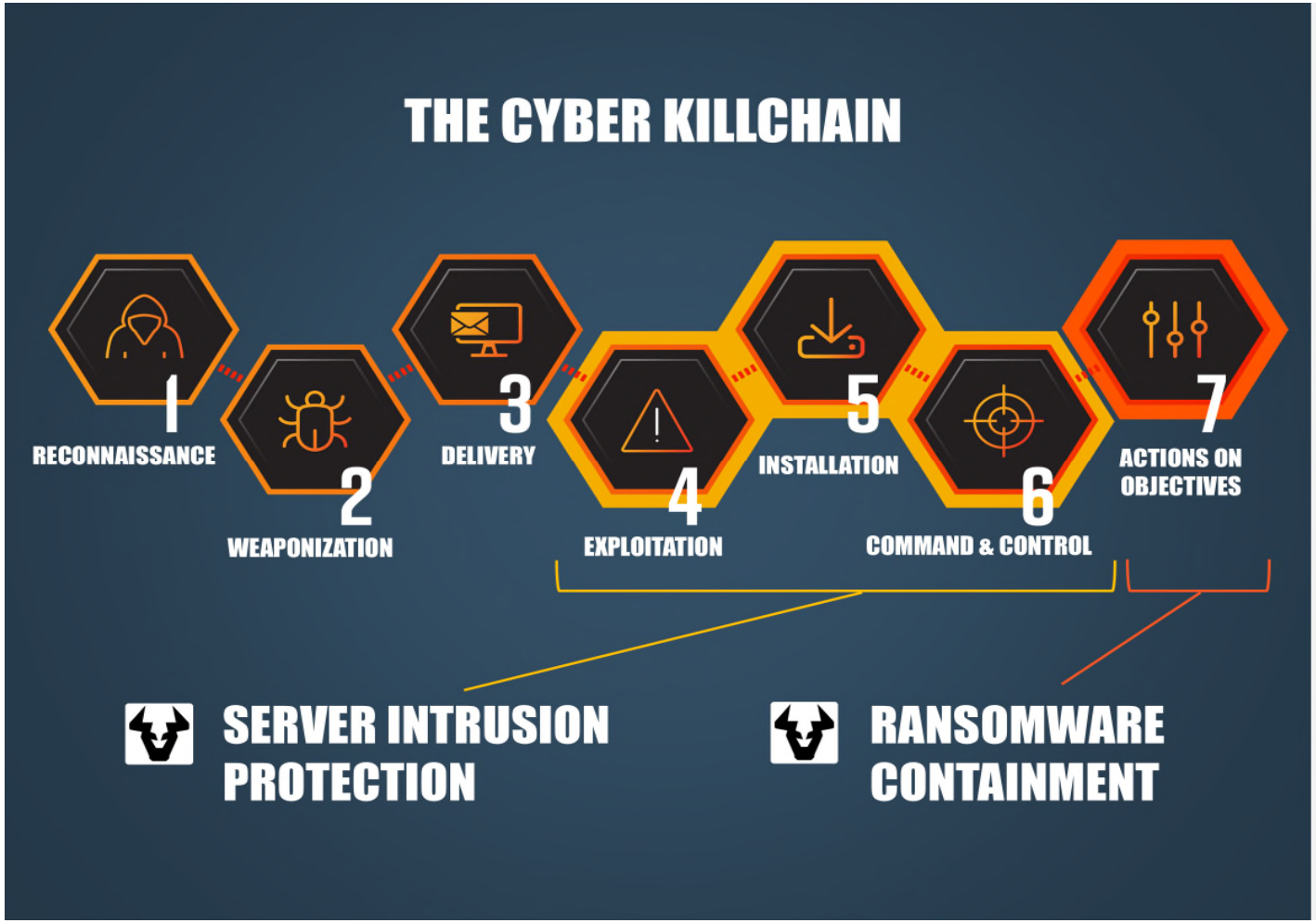
Evolution of Ransomware Prevention

RICOH
imagine. change.



The Cyber Kill Chain

RICOH
imagine. change.



BULLWALL

24x7 Automated Containment
Including Zero-Day Exploits and protection of all IT critical infrastructure

Secure Remote Access & Tasks
Intruder Entrapment, blocks malicious activities and use of compromised credentials

Cyber Insurance
Meets criteria for discounts or approval for most insurance

We’re Bullwall – Last Line of Defense

RICOH
imagine. change.

Our Mission

TO FIGHT THE IMPACT OF RANSOMWARE WORLDWIDE

BullWall is committed to helping customers address the major concern that is Ransomware

Ransomware attacks are increasing

Prevention is no longer enough

Ransomware is more than a Security issue, its Boardroom concern

The cost of recovery is increasing YoY

Businesses need to Prioritize Recovery and Resilience

RICOH
imagine. change.

PwC Global Crisis & Resilience Survey

Out of 2000 respondents 89% noted that resilience is one of their most important strategic organizational priorities. Yet many also report that their organizations have not taken the steps needed to implement an integrated enterprise resilience program or even identified the steps to move forward on that journey. Business leaders' express confidence in their ability to recover from a crisis.

Too many organizations are lacking the foundational elements of resilience needed to be successful.

McKinsey & Company

The world is experiencing a level of disruption and business risk not seen in generations. Some companies freeze and fail, while others innovate, advance, and even thrive.

The difference is resilience.

TechRadar

Today's CISOs face a perfect storm. Cyberattacks are increasing year-on-year, and new technologies such as AI are empowering attackers. Meanwhile, the amount of data CISOs are defending is growing. Last year alone, 85% of IT and security leaders in the UK reported experiencing a significant cyberattack, with 36% of those victims enduring at least one ransomware attack.

CISOs must evolve and implement a cyber strategy which centers resilience and recovery - no matter where their data is stored.

MSN

It's an uncomfortable reality that cyberattacks are increasingly unavoidable. But it is the reality. Until relatively recently, prioritizing cyber resilience fell to the wayside - however regulations are coming into play to support the prioritizing of cyber-resilience. (DORA and NIS2) That's why cybersecurity professionals must move to adopt a position of cyber resilience, ***and prepare to recover from an attack, not just defend against it.***

A cybersecurity strategy that disproportionally focuses on prevention is unsustainable and ineffective.

Containment is a key component to resilience.

Prevention

SentinelOne, CROWDSTRIKE, Microsoft, Bitdefender, CHECK POINT, eset, Trellix

Blocks Known Attacks

What could go wrong…

Misconfiguration
Agent doesn't talk to server
Misses zero days

Agentless Containment

Containment Fills the Gaps

Immediately Halts Attacks

Recovery of 10-100 Files
(not 1m+)

Backup/Recovery

veeam, rubrik, druva, COMMVAULT, COHESITY, aws Backup automation

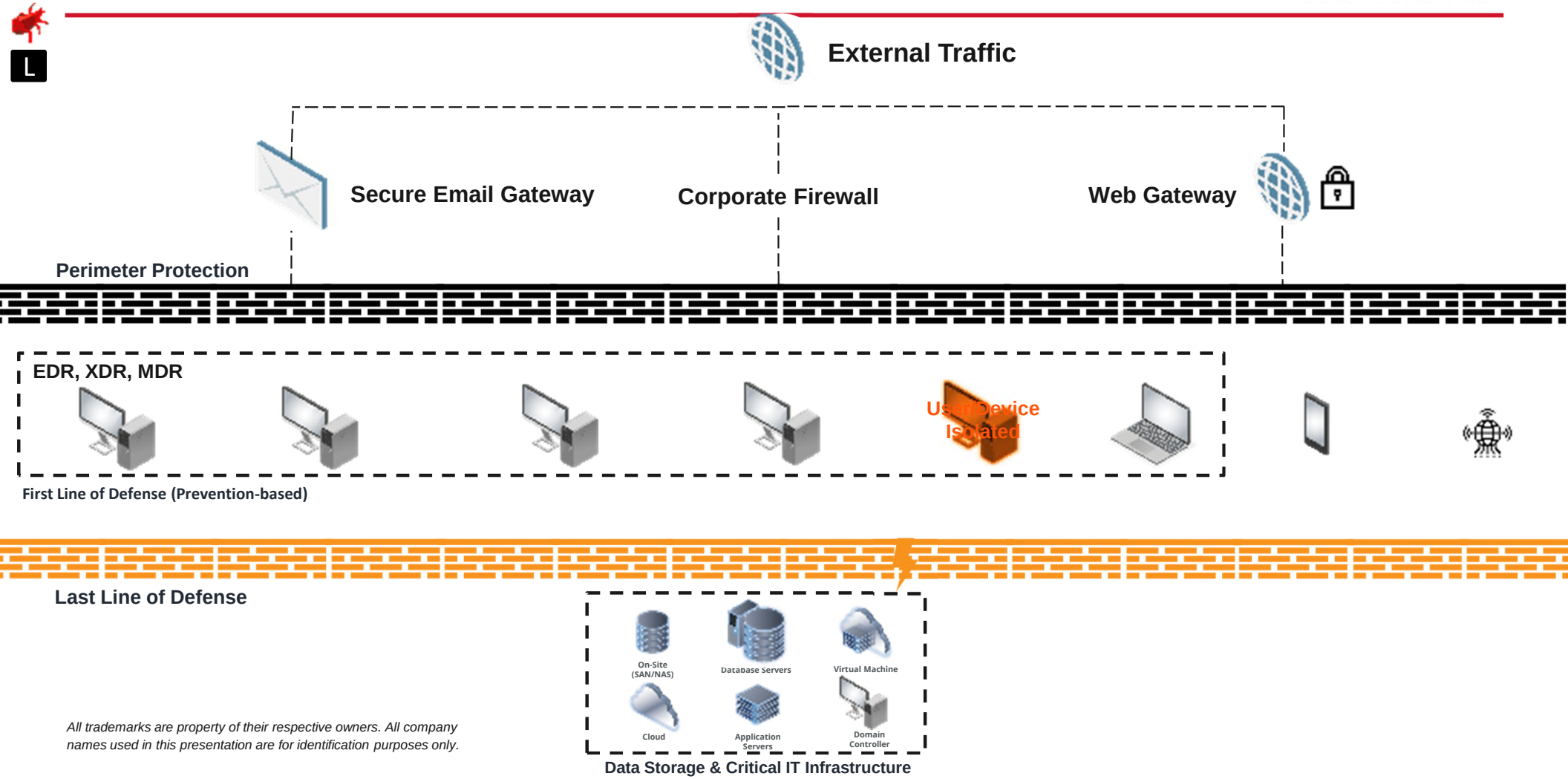
Critical to Business Continuity

What could go wrong…

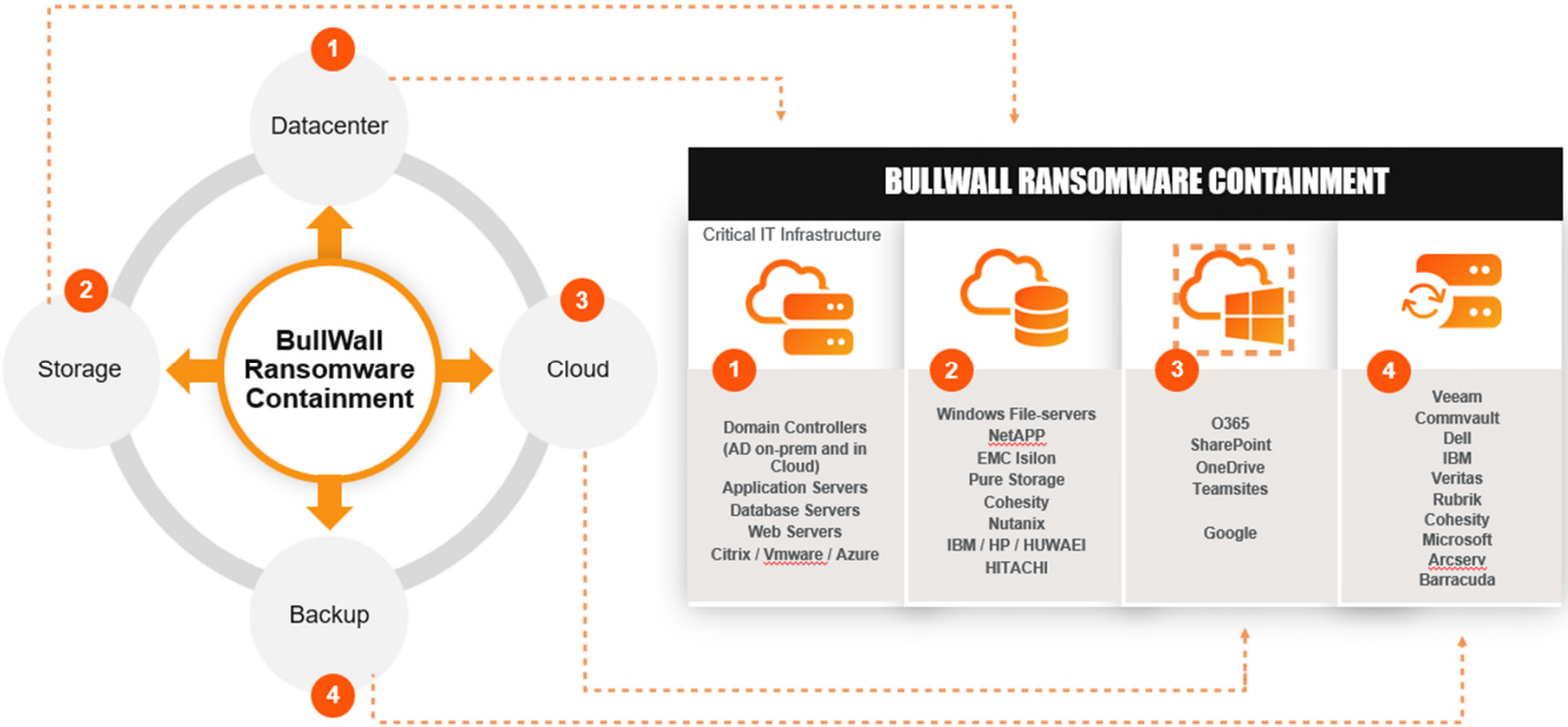
Backups Hit
Delta to Recovery

How RC Fits with your existing Security Stack

RICOH
imagine. change.



Protecting Critical IT Infrastructure



Full Organization Protection All Servers / Platforms / Cloud

Bullwall Ransomware Containment

RICOH
imagine. change.

- **Protects All Critical IT Infrastructure**
  On-Prem and In-Cloud
- **Agentless & Easy to Implement**
  No Endpoint Installation

- **24x7 Automated Detection**
  & Response
- **Automated Compliance Reporting**
  for GDPR, NIST and More

Detect

Monitors data activity in real-time

28 detection sensors and AI machine learning

Instantly detects illegitimate encryption and malicious events

Respond

Immediately isolates compromised users and devices

Integrates with SIEM, NAC, EDR, via RESTful API

Alerts via email, SMS, app, etc.

Recover

Identifies encrypted files to restore from backup

Pinpoints compromised users and devices

Understands initial attack vector for internal investigation

Report

Automates incident reporting with immediate attack log

Informs executive leadership

Provides compliance report to alert agencies

CALCULATING THE COST OF

NUMBER OF USERS ON THE NETWORK

How many users are in the Active Directory?

Users in the AD

RANSOMWARE IMPACT

What percentage of employees will be impacted by a ransomware attack?

0

Users affected

TECHNOLOGY DEPENDENT

How dependent are employees on technology to conduct normal operations?

Dependency on IT

AVERAGE EMPLOYEE COSTS

What is the average hourly cost per employee?

Include wages, pension, and indirect costs such as office rental, etc.

Total cost per employee

According to Coveware, downtime is still the costliest aspect of a ransomware attack. In Q2 of 2022, the average firm experienced 24 days of downtime, a 3-day increase from 2020.

OFFLINE SERVICES

How many hours will employees experience downtime while IT professionals restore online services following a ransomware attack?

One workday is equivalent to 8 hours.

24 days = 192 hours

FILE RESTORATION

How many hours will it take for average employee to recreate lost files that were unrecoverable from the data backup?

COST OF DOWNTIME

You might not have the budget for additional protection. However, do you have the budget to cover the cost of recovering from a potential devastating incident? The below calculator is just a tool of protection, typically only 20-35% of the entire recovery cost.

$0

Call to Action

RICOH
imagine. change.

1.Sign up for a free Ransomware Assessment ($1,000 value) for BCASBO conference attendees (must sign up at booth)

2.Register for a special invitation only webinar

3.Discover how Ricoh can help your organization work smarter, faster and more securely

Ransomware Assessment

RICOH
imagine. change.

Step 1 - Preparation

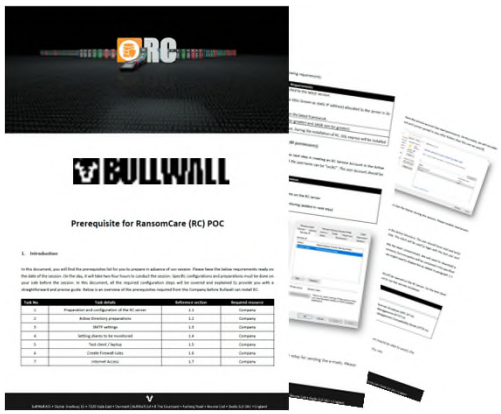
- Approx. 30 minutes
- Follow prerequisites
- Setup test share

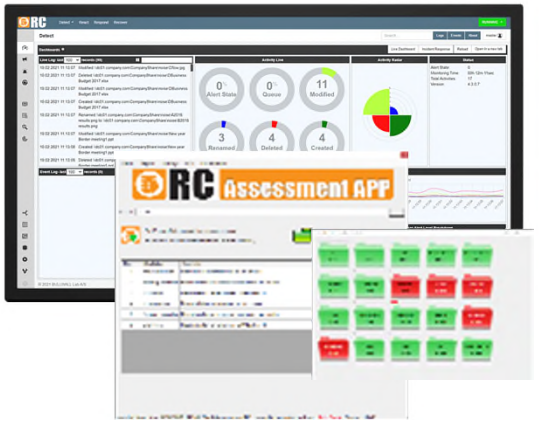
Step 2 - Simulation

- See how your network reacts
- Experience RansomCare in your environment
- Are your existing tools effective?

Step 3 - Outcomes

- 500+ assessments completed
- Reporting available
- Understand your resilience to an encryption outbreak





RICOH
imagine. change.

Questions?

RICOH
imagine. change.

Thank you.

RICOH

imagine. change.