



**Hewlett Packard  
Enterprise**



# **ZERO TRUST SECURITY, COMPLIANCE AND RANSOMWARE PROTECTION**



---

**Steve Tcherchian, CISSP, PCI-ISA  
Chief Product Officer and CISO  
XYPRO Technology**

# The State of Cyber Trends and Challenges



Average cost of Cyber Attack

**\$5 million**  
in 2023



Ransomware to cost world economy

**\$30 billion**  
in 2025



Insider Threats

Risk of malicious or accidental actions by authorized users, such as employees or contractors are a major concern.



**80% rank**  
cyber risk as a top-five concern



Ransomware is the fastest growing cybercrime  
A business will fall victim to a ransomware attack every

**11 seconds**



**75%**  
of breaches involve attack surface exposure <sup>1</sup>

1. 2023 Unit 42 Ransomware and Extortion Report



# Government Regulation and Compliance



**HIPAA**  
Health Insurance  
Portability and  
Accountability  
Act of 1996



**PCI DSS 4.0**  
Payment Card  
Industry Data  
Security  
Standard  
*Clock is Ticking!*  
*Are you Ready?*



**NERC**  
North American  
Electric  
Reliability  
Corporation



**DORA**  
Digital  
Operational  
Resilience Act



**GDPR**  
General  
Data  
Protection  
Regulation

New

## US Executive Order 14028:

“Within 60 days of the date of this order, the head of each agency shall...develop a plan to implement Zero Trust Architecture” – Effective January 2023

# What is Ransomware?

## The Criminal Supply Chain



Ransomware was once just a nuisance strain of malware used by criminals to encrypt files and data. It has evolved into a massive, financially lucrative attack method using data theft, harassment and other threats.

In 2022 – Ransom demands ranged from **\$3,000 to \$50 Million**  
The median request was \$650,000, with an average payment of \$350,000

# Who Is Being Attacked?

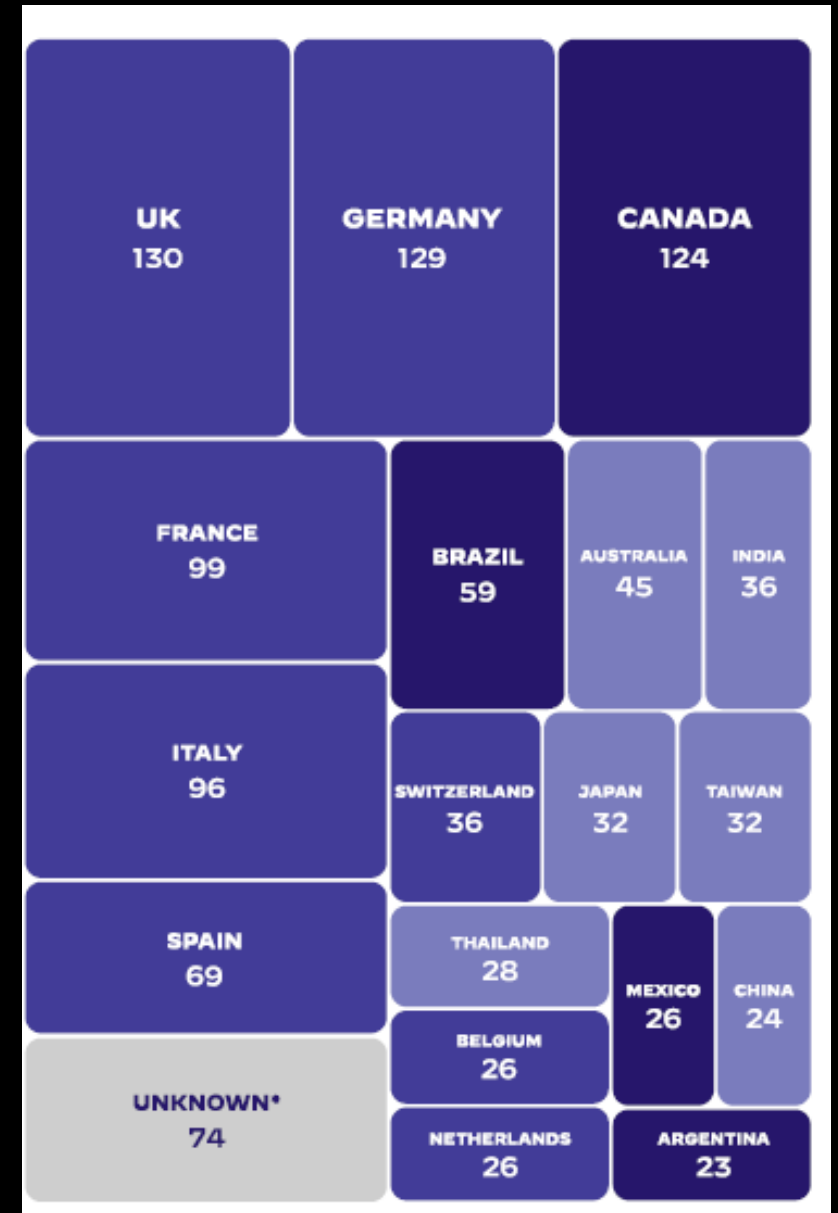
## EVERYONE IS A TARGET!

Large, multi-national organizations – “big game hunting”  
At least 30 organizations on the Forbes Top 2000 list were publicly impacted in 2022

Regulated Industries contain PII, PHI and other valuable assets

Industries where its critical for businesses to provide products and services in a timely manner

Manufacturing, retail, technology at the top of the list



Unit42 and Palo Alto Networks Report on Ransomware 2023

# Backups Are No Longer Good Enough

Traditional strategy is to keep up to date backups,  
stored offline and test them often

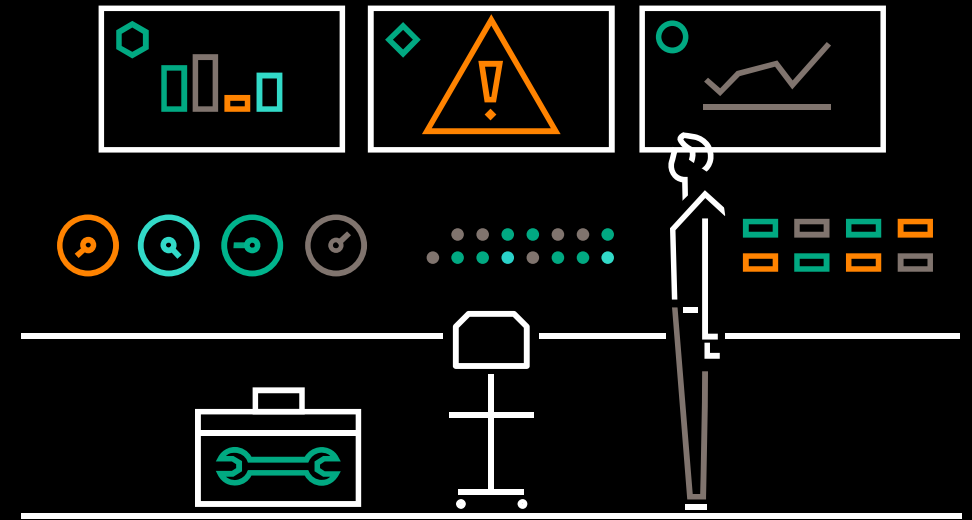
Still valid – but reactive and unreliable

*Damage is already done*

New attack methods involve disclosure of sensitive  
data to coerce organizations to pay ransom

Causes reputational damage, loss of confidence,  
employee turnover

Fines and sanctions exceed the cost of ransom  
demand



# How Does This Happen? We Make It Too Easy!



# The Result – Attack Completed!

>> What happened?

Important files on your network was ENCRYPTED and now they have “[REDACTED]” extension.  
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your network was DOWNLOADED.  
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:

- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: citizens data, courts data, bills, budgets, annual reports, bank statements, etc

Samples are available on your personal web page linked below.

>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.  
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.  
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next?

- 1) Download and install Tor Browser from: <https://torproject.org/>
- 2) Navigate to: [REDACTED]

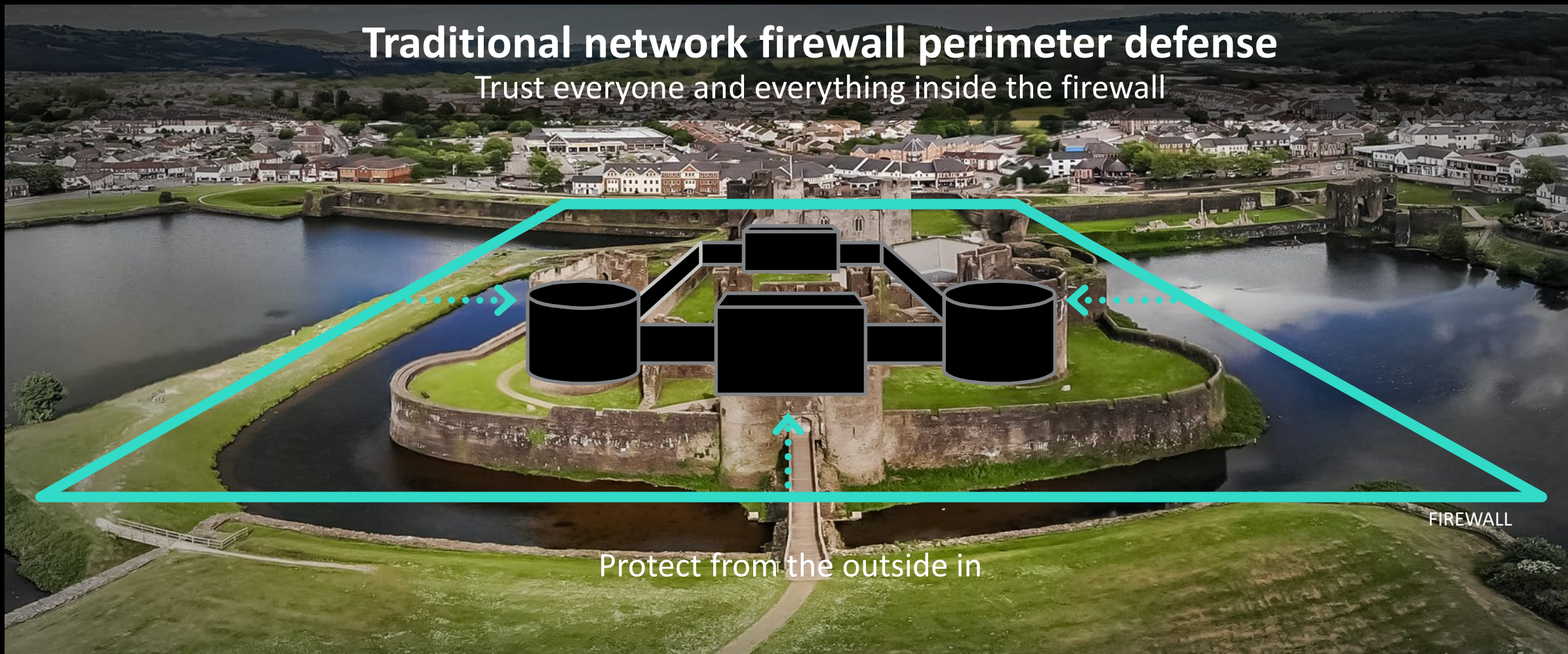


# THE ZERO TRUST MODEL

# What Does Zero Trust Mean?

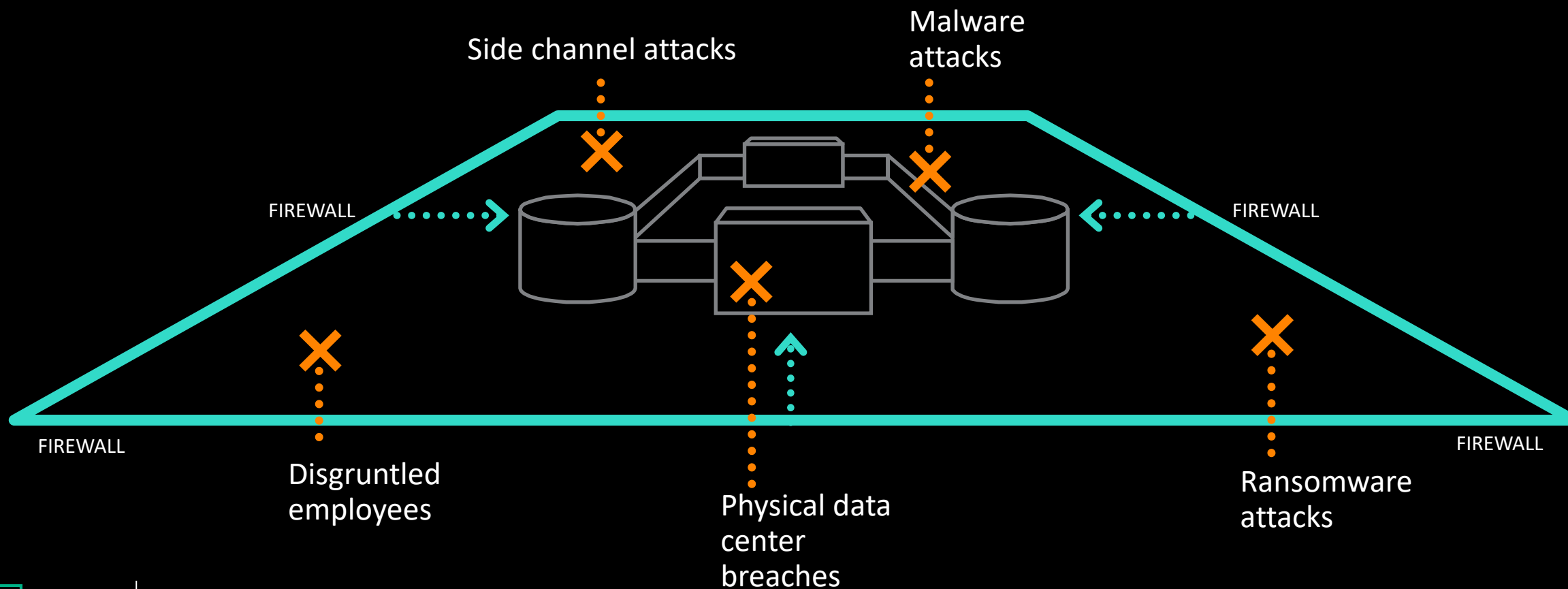
## Traditional network firewall perimeter defense

Trust everyone and everything inside the firewall

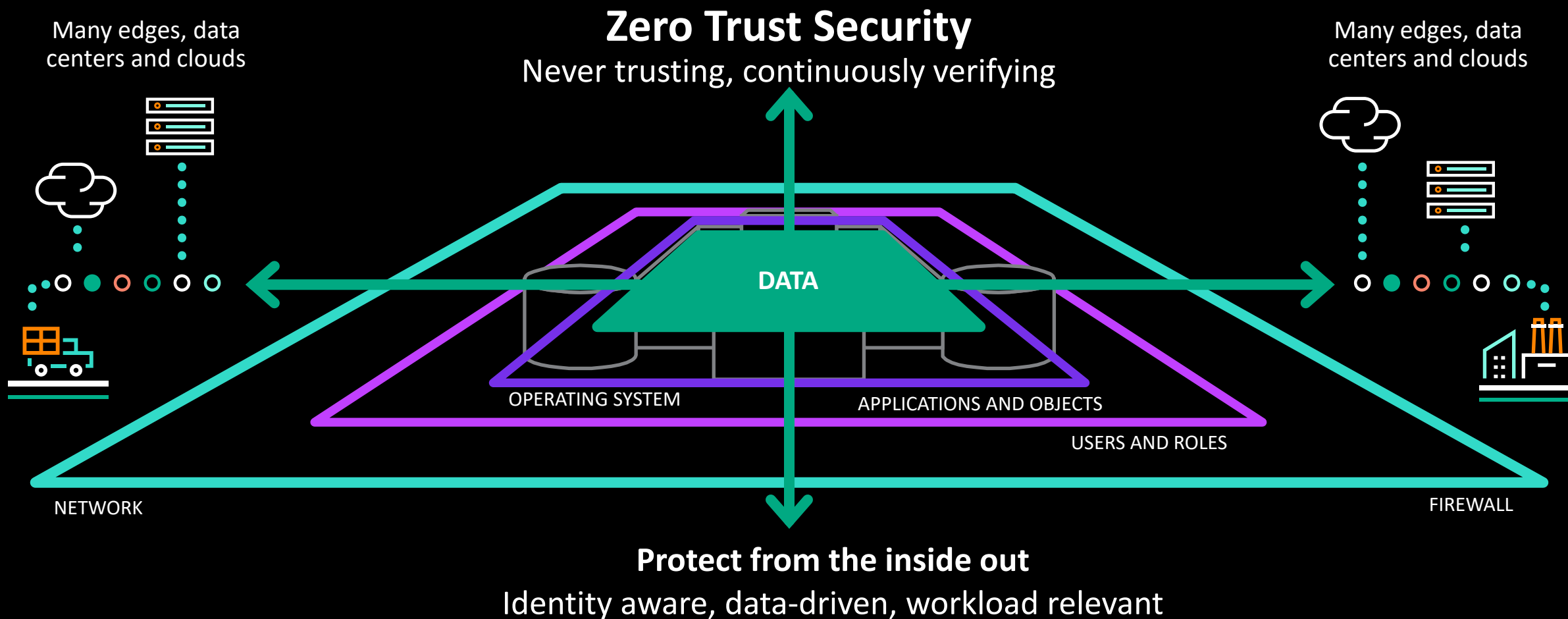


# What Does Zero Trust Mean?

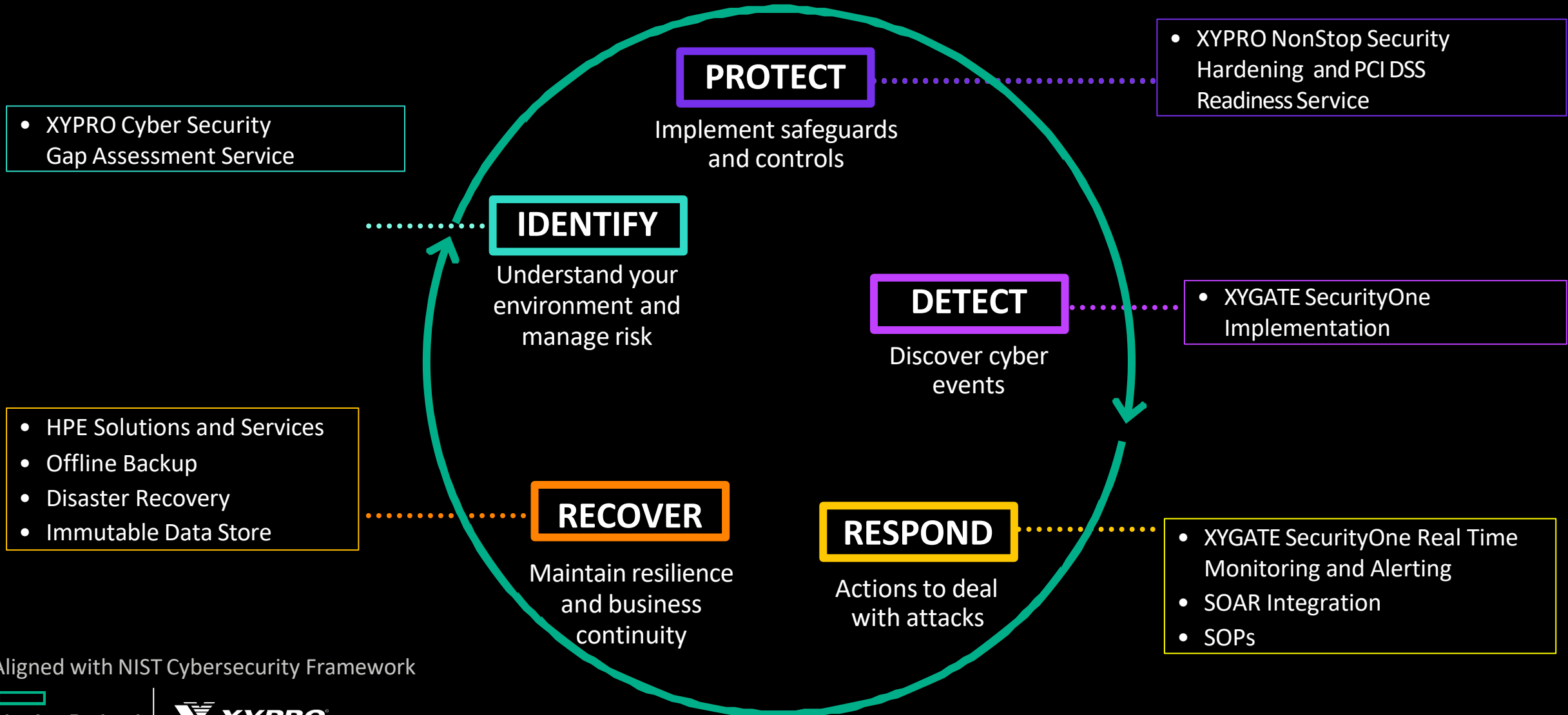
## Traditional network firewall perimeter defense



# What Does Zero Trust Mean?



# Data Resiliency Strategy



Aligned with NIST Cybersecurity Framework



# **SOLUTIONS FROM HPE AND XYPRO**

# IDENTIFY – XYPRO CYBER SECURITY GAP ASSESSMENT

- Cyber Resiliency begins with asset identification, inventory, and categorization.
- XYPRO's Security Gap Assessment identifies critical assets and security risks.
- This assessment scans, identifies and assesses security misconfiguration, compliance status, and other ransomware attack vectors.
- Builds a roadmap for subsequent phases.



# PROTECT – XYPRO SECURITY HARDENING AND SERVICE

- Based on findings from the Security Assessment, security controls are implemented to reduce the identified attack surface.
- This includes
  - Safeguard Configuration
  - XYGATE User Authentication for Auth Controls, Multi-Factor Authentication and AD Integration
  - Hardened password controls
  - User and Identity Management
  - Priveledged Session Management and Monitoring
  - Secure critical files, objects and assets
  - Implement additional security controls based on Security Assessment findings.



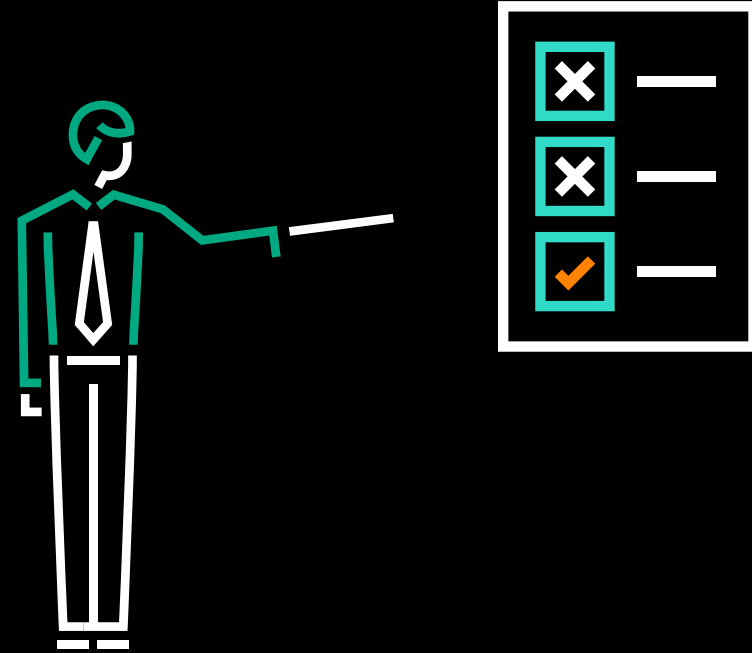
# PCI DSS 4.0

## The New Requirements

- 64 New Requirements
- 13 new requirements are effective immediately\*
- 51 are best practices until March 2025
- Biggest Impacts are to Requirements 8, 10, 11 and 12

### Important Dates

- **2023** is a transition period
- PCI 3.2.1 officially retired **March 2024**
- Best practices become effective in **March 2025**



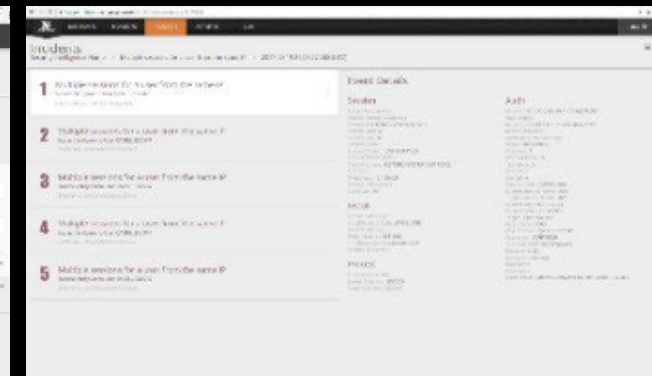
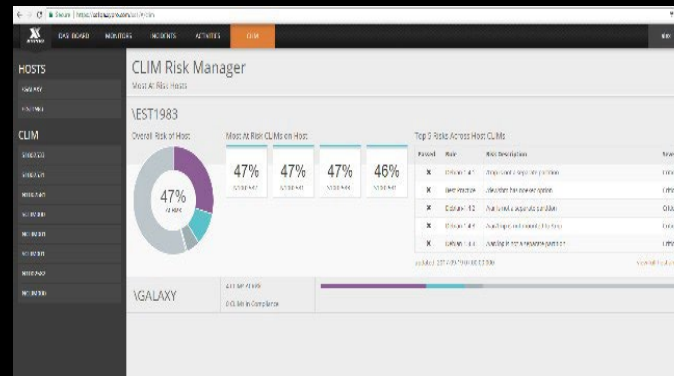
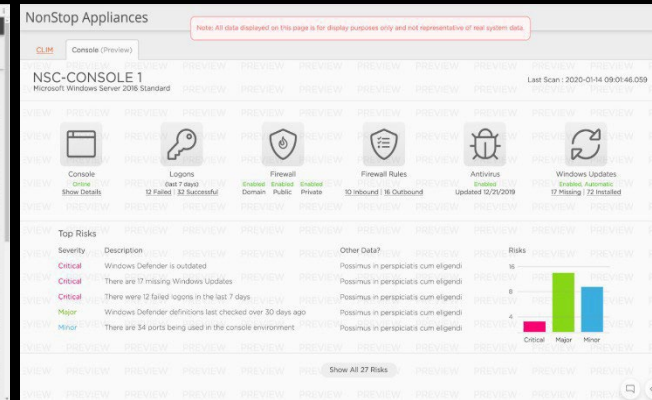
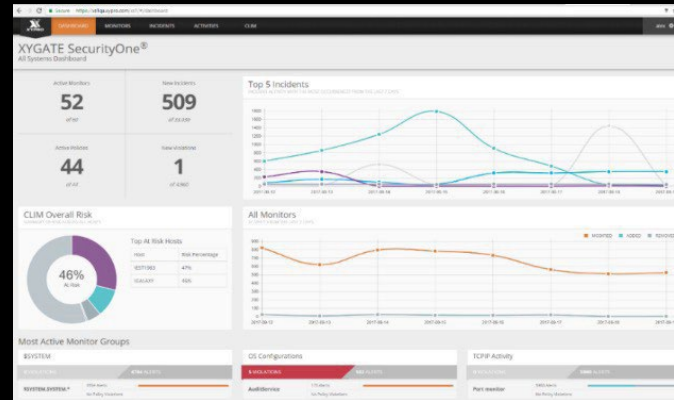
# DETECT - XYGATE SECURITYONE

## Zero Trust Security and Ransomware Protection

- Ransomware, Virus and Malware Protection
- PCI DSS 4.0, GDPR and HPE Hardening Guide
- Intelligent File and System Integrity Monitoring
- Real-Time Threat Detection and Vulnerability Management
- Monitor NonStop CLIMs and Windows Console
- Privileged Session Management
- Keystroke Logging
- Object Level Security
- User Behavior Profiling

## Business Value

- Reduce cost of security incidents. **Prevention is KEY!**
- Simplify compliance reporting
- Improve staff productivity
- Reduce business risk





# CONTEXT IS KEY

XYPRO Patented Technology

Correlation is not context

Context allows separation of noise from data

XS1 applies HPE NonStop specific knowledge to contextualize events and assess impact

Reduce false positives

Provide actionable information



CONTEXT TRANSFORMS DATA INTO INFORMATION



# FILE AND SYSTEM INTEGRITY IS CRITICAL

## Detect Malicious Activity

- Detecting unauthorized changes to objects and files is the best defense against malware and ransomware

## Identify Human Error

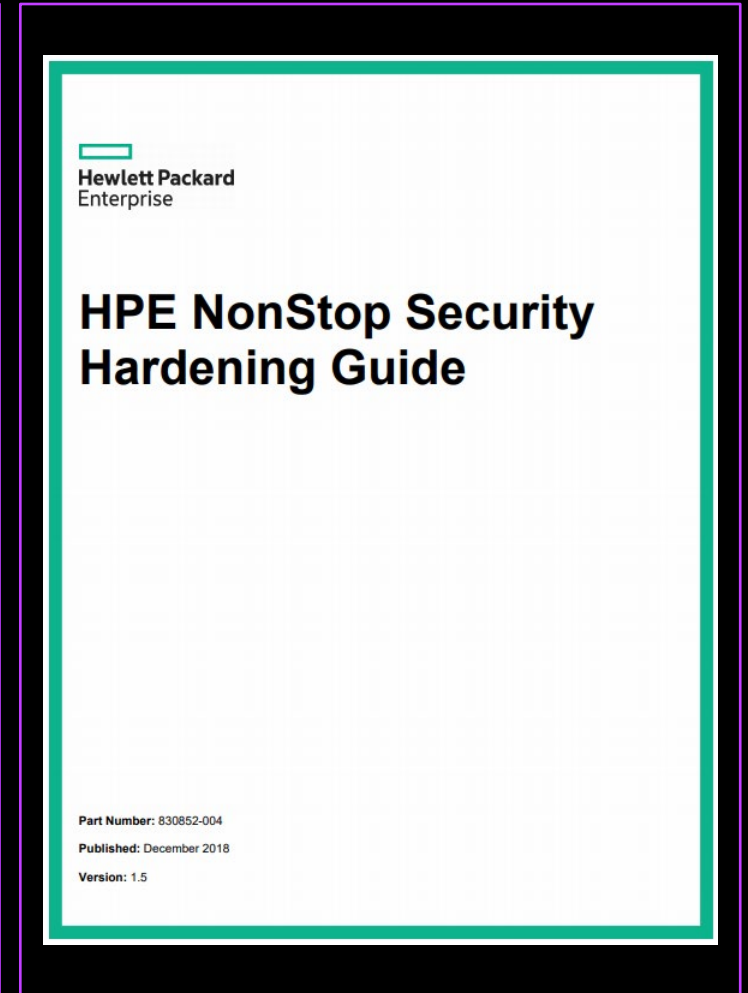
- Detect mistakes before they cause irreparable damage

## Necessary for Compliance

- PCI, GDPR, SOX, HIPAA, DORA, FISMA, NIST and other frameworks

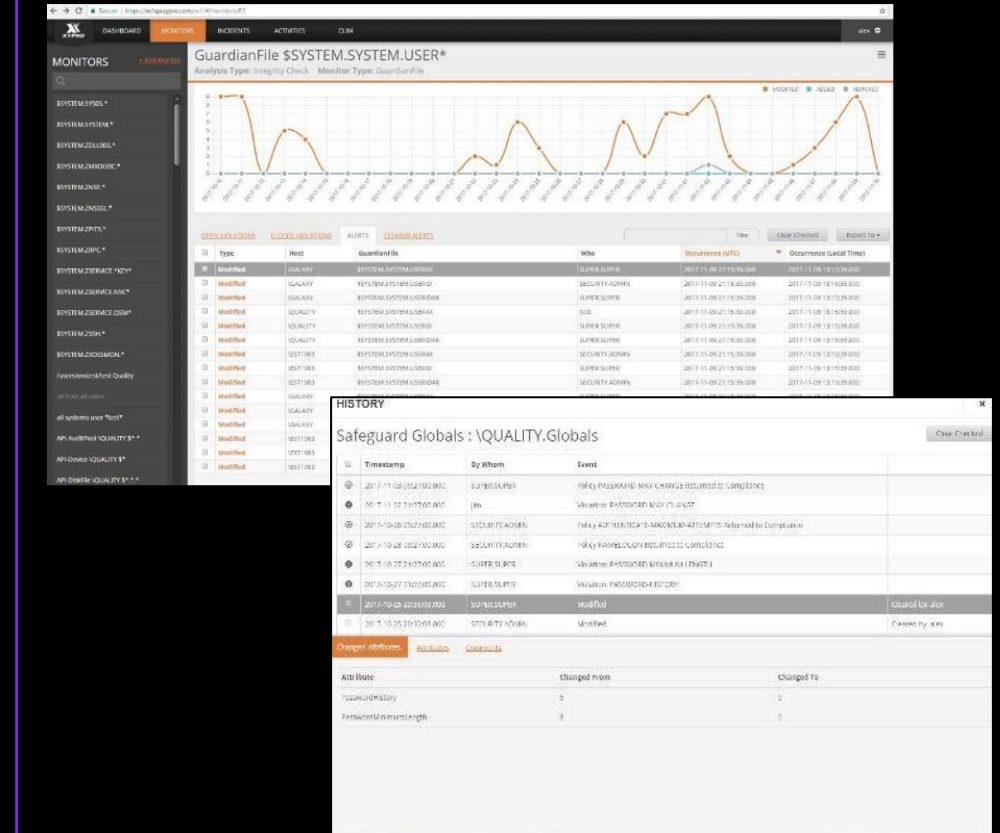
## Recommended by HPE NonStop Hardening Guide

- “Ensuring the integrity of critical operating system files and settings is an important part of your security strategy.”
- “Centralized monitoring and reporting and file integrity checking both assist you in demonstrating compliance to security regulations such as PCI DSS, SOX and HIPAA.”



# FILE INTEGRITY IS REQUIRED FOR PCI DSS 4.0 COMPLIANCE

- Real Time Monitoring
- Guardian and OSS Support
- Allow/Deny lists
- File Hashing/Fingerprinting
- Policy Management and Enforcement
- Integration with SIEM/SOAR and Analytics
- Real-time file, user, process, config monitoring
  - Network port monitor detects newly added ports
  - Process monitor detects new process creation
  - Prevent configuration drift
- Dashboards, details and context
  - Alert on who did what when
  - Entire history lifecycle of object
  - Context for changes that violate policy frameworks
  - Data trending



# RESPOND - XYGATE SECURITYONE FOR INCIDENT RESPONSE

The screenshot displays the XyGate SecurityOne interface. At the top, there are navigation tabs: DASHBOARD, MONITORS, INCIDENTS (selected), and ACTIVITIES. Below the navigation, there's a search bar with the text "Select Multiple Failed Login Incidents Where Target Login = QA.CGORST". The main content area shows a list of six "Multiple Failed Login" events, each with a timestamp and a description: "Wrong-password Verifyuser to User QA.CGORST 232.110". To the right of the list, there's a detailed view for the first event, titled "#ID 1234 - Multiple Failed Login". This view includes "Event Details" such as "SESSION", "INSTALL", and "PROCESS" information. A "Monitor Triggered" notification is visible in the top right corner, indicating a policy violation: "User Password should not be expired...".

Real-time alerting and data contextualization ensures CSIRT is not flooded with benign or false positive alerts.

Alerts are triggered based on

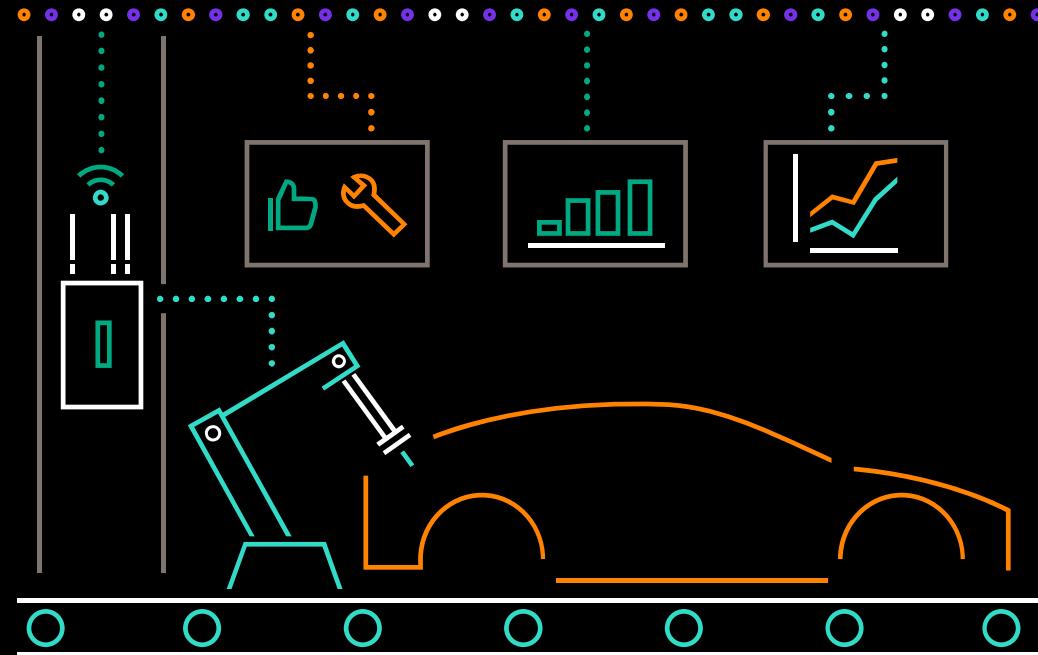
- Out of the box library
- Easy to use, visual Rule manager for create new rule patters
- ML algorithms for baselining and detecting unusual activity

Alerts can be integrated with enterprise SIEM and/or SOAR, or addressed within the XS1 Application Intelligent summary/detail dashboards highlight what is critical and what can be safely ignored for immediate response

# XYGATE SECURITYONE BUNDLE

## What's Included

- Real Time Security Threat Detection
- User Authentication (XUA)
- Merged Audit (XMA)
- Access Control (XAC)
- Object Security (XOS)
- CompliancePRO (XSW)
- File and System Integrity Monitor
- Compliance Module
- Appliance Sentry Monitor
- Onboarding Services





# RESOURCES

---

Visit [www.xypro.com](http://www.xypro.com)

- PCI Auditors Guide
- PCI DSS Summary of Change for HPE NonStop
- PCI DSS 4.0 Webinar – Not To Miss!
- Articles, Videos and more on simplifying compliance
- **PCI DSS Assessment and Readiness Services**

## Payment Card Industry Data Security Standard

PCI DSS Version 3.2.1 to 4.0  
Summary of Changes for HPE NonStop™ Servers

---

# BUSINESS VALUE AND ROI

# #1 – XYPRO REDUCES THE COST OF SECURITY INCIDENTS BY 80%

- Reduces cost of security incidents
- Improved threat detection and response
- Reduces SIEM costs



**34%**

Probability that an organization will experience a material breach in the next 24 months



**270+ Days**

Current mean time to identify and contain a breach



**\$2 Million**

Amount organizations save when using a ZERO-Trust Strategy

# #2 – XYPRO COMPLIANCE REPORTING CAN SAVE THOUSANDS OF HOURS

## Reduce manual effort, automate compliance monitoring and reporting


Audit reports generally require “pulling” data from multiple systems and consolidating into audit reports. This process is typically manual and can take months.

VS

XYPRO compliance monitoring and audit reporting are automated. Reports are generated in real time in summary/detail views.



**PCI DSS**  
Payment Card  
Industry Data  
Security Standard



**HPE**  
HPE NonStop  
Hardening Guide



**DORA**  
Digital  
Operational  
Resilience Act



**GDPR**  
General Data  
Protection  
Regulation

# #3 – XYPRO SOLUTIONS INCREASE STAFF PRODUCTIVITY

Most organizations cannot allocate enough resources to proactively monitor their environment



Security staff must devote time investigating potential incidents - a very manual and time-consuming process of collecting, correlating, and searching through disparate logs.



XYPRO solutions automate incident identification by correlating data in real-time and highlighting actionable incidents that need immediate attention – using patented technology.



Automation of investigation activities frees up nearly 80% of your staff's time, allowing them to focus on proactive monitoring



## #4 – XYPRO SOLUTIONS MODERNIZE SECURITY RESOURCES

Manage NonStop the same way you manage other IT assets

Data volume, velocity and variety is increasing

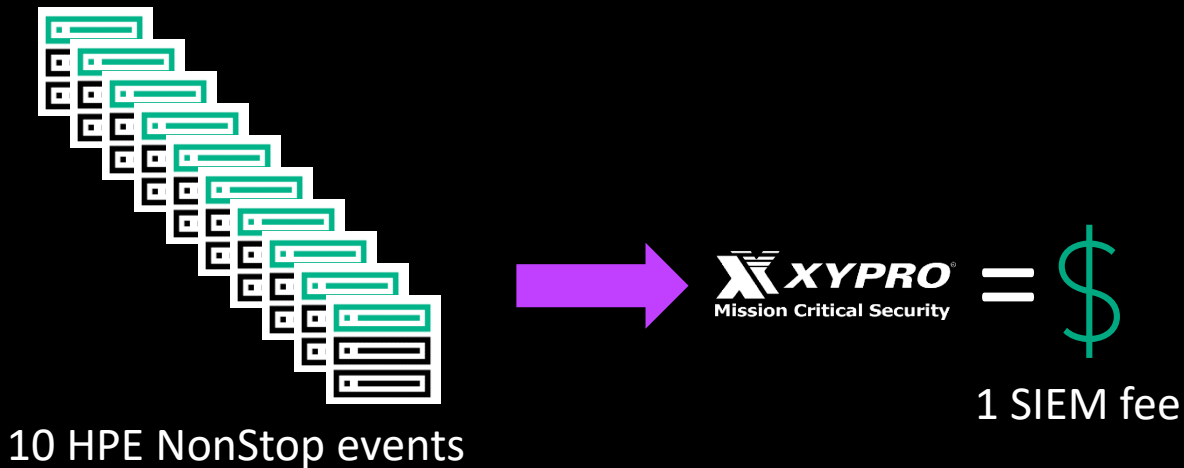
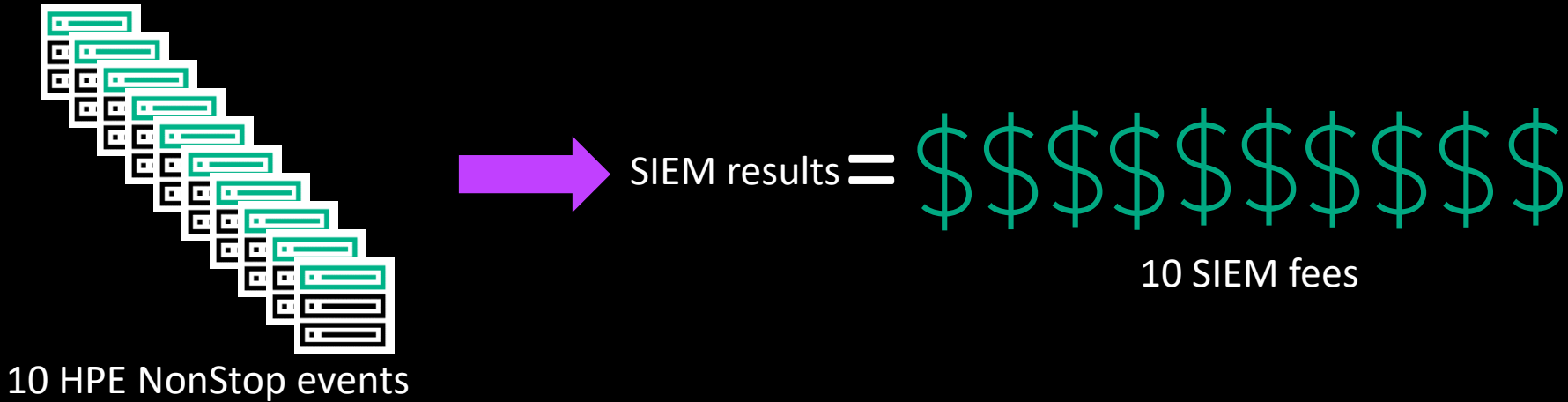
Not having the right resources to secure the HPE NonStop is a risk

NonStop-dedicated resources are shrinking

Having only a few staff members familiar with NonStop security management heightens the risk of insider abuse

Anyone with security management experience can use XYPRO solutions to manage HPE NonStop security without needing in-depth NonStop knowledge, greatly reducing the risks from resource attrition and insider abuse.

# #5 – XYPRO ENHANCES YOUR ENTERPRISE SIEM



## Cost savings

- XYPRO is licensed per connected server rather than on event volume
- XYPRO can reduce SIEM license fees

Can result to 90% cost saving on SIEM license fees associated with NonStop events



**Q: What % of breaches involve attack surface exposure?**



# CUSTOMER CASE STUDY – DISCOVER FINANCIAL SERVICES

- **3rd-largest debit/ATM network in USA**
  - 2.1 million ATMs and cardholder access locations
  - Large NonStop environment
- **Challenges**
  - Inadequate real-time monitoring of suspicious activity
  - Limited visibility and lots of noise
  - Difficult to extract value and context from data
- **Solution: XYGATE SecurityOne**
  - Unified security views, advanced analytics and threat detection, file integrity monitoring and contextualization
- **Benefits**
  - Faster detection and response to security events
  - Dramatic reduction in audit and compliance time and effort
  - Easy uptake for NonStop novices



Tanya Jones, Sr. Manager of Cybersecurity for Discover Financial Services and PULSE, presenting at 2019 NonStop Technical Boot Camp

“Summary view represents data we need to see without inundating us with details we don’t need”

“PCI audit time went from one week to 30 minutes”

“I’m actually looking forward to our next PCI audit”

# CUSTOMER CASE STUDY - HDFC BANK

- **Challenges**

- Manual effort to benchmark baseline and standards
- Applications spanning multiple systems
- Limited resources
- Too much data (volume, velocity, variety)

- **Solution: XYGATE SecurityOne**

- Immediate visibility into application health and security
- Summary results for executives
- Actionable events for security operations

- **Benefits**

- Achieved PCI DSS Compliance
- NonStop data integrated with the rest of the enterprise
- Simplified reporting
- Reduced time spent on false positive alerts
- Augmented security staff



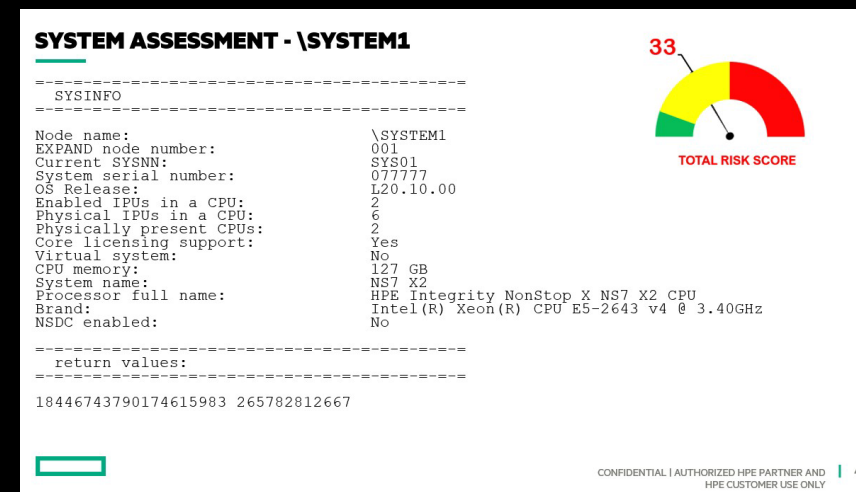
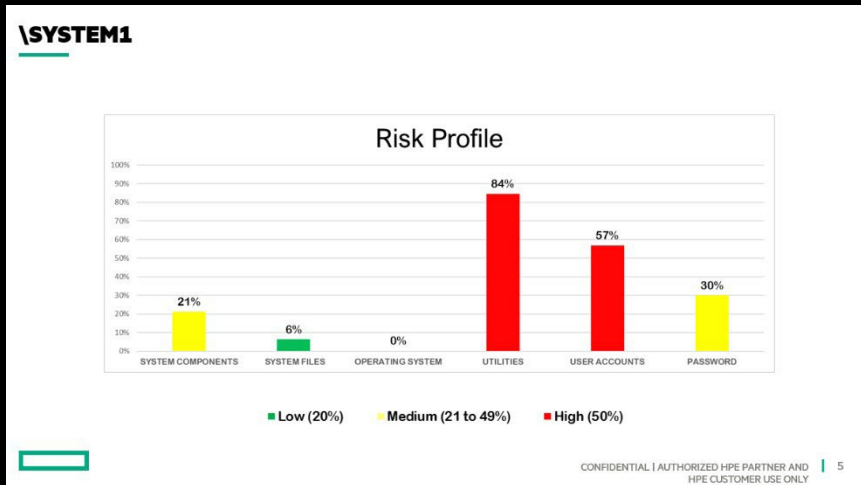
# RAPID SECURITY ASSESSMENT

## The LAST SLIDE – I PROMISE!!

- 120+ different security vectors evaluated in 6 key categories
- Single executable, nothing to install, easy to run
- No sensitive data
- Report generated and recommendation provided
- **Completely FREE!**



[xypro.com/free](http://xypro.com/free)



# THANK YOU

## TAKE ACTION

- Sign up for our free security assessment: [www.xypro.com/free](http://www.xypro.com/free)
- Visit HPE NonStop: [www.hpe.com/us/en/servers/nonstop.html](http://www.hpe.com/us/en/servers/nonstop.html)
- Visit XYPRO: [www.xypro.com](http://www.xypro.com)
  
- YouTube [youtube.com/xyprotechnology](https://youtube.com/xyprotechnology)
- X [@XYPROTechnology](https://twitter.com/XYPROTechnology)  
[@SteveTcherchian](https://twitter.com/SteveTcherchian)
  
- LinkedIn [linkedin.com/xyprotechnology](https://linkedin.com/xyprotechnology)  
[linkedin.com/stevetcherchian](https://linkedin.com/stevetcherchian)