PCI Security Standards Council

Cybersecurity Strategies for Ransomware Protection, Compliance and Digital Resilience

Steve Tcherchian – CISSP, PCI-ISA, PCI-P
XYPRO Technology

PCI Security Standards Council

Steve Tcherchian

Chief Product Officer & CISO
XYPRO Technology
CISSP, PCI-ISA, PCI-P

XYPRO®
Mission Critical Security

The State of Cyber – Trends and Challenges

Average cost of Cyber Attack

$5 million

in 2023

96%

backup repos targeted in cyberattacks

Insider Threats

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

21 Days

Average downtime after ransomware attack

40%

of IT assets are unmonitored

75%

of breaches involve attack surface exposure [1]

1. 2023 Unit 42 Ransomware and Extortion Report

PCI Security Standards Council®

Government Regulation and Compliance

HIPAA
Health Insurance Portability and Accountability Act of 1996

PCI DSS 4.0
Payment Card Industry Data Security Standard

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

PCI Security Standards Council

What is Ransomware? The Criminal Supply Chain

- Ransomware is a type of malicious software that encrypts files on a victim's computer or network, demanding payment, usually in cryptocurrency, for their decryption. It effectively holds data hostage until the ransom is paid.

- In 2023, the median ransom demand surged by 20% from the previous year to $600,000. Finance, legal, government, retail, and energy experienced even higher median demands, reaching $1 million or more.

- Average ransom paid almost doubled compared to 2022, reaching $1.54 million

PCI Security Standards Council®

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

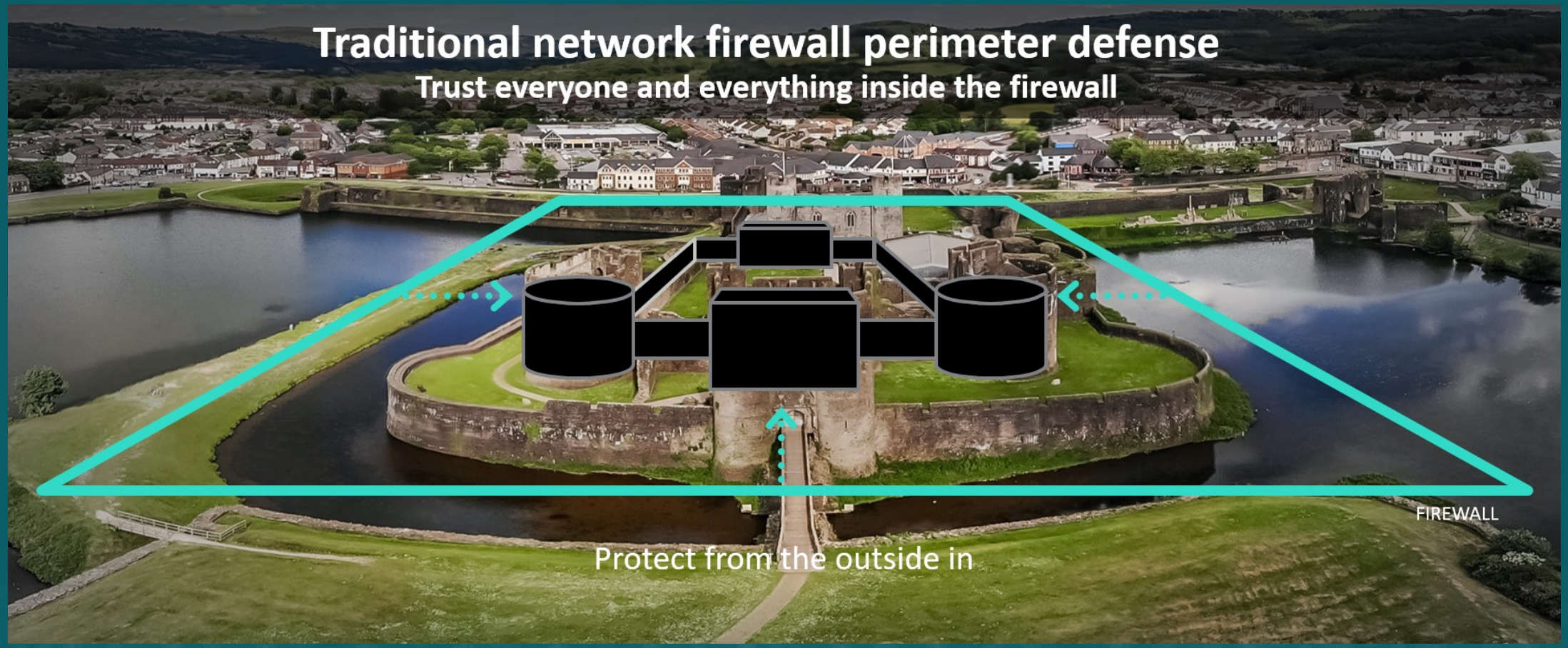
Causes reputational damage, loss of confidence, employee turnover

Fines and sanctions exceed the cost of ransom demand

PCI Security Standards Council


The Zero Trust Model

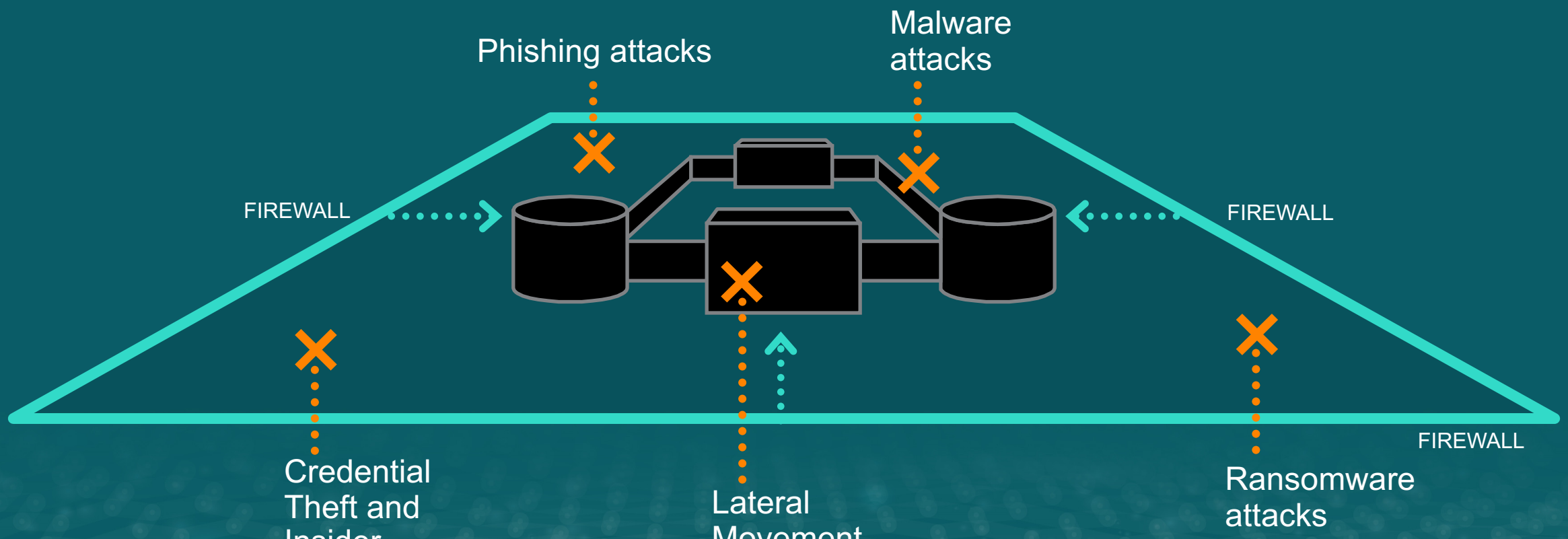
What Does Zero Trust Mean?



PCI Security Standards Council®

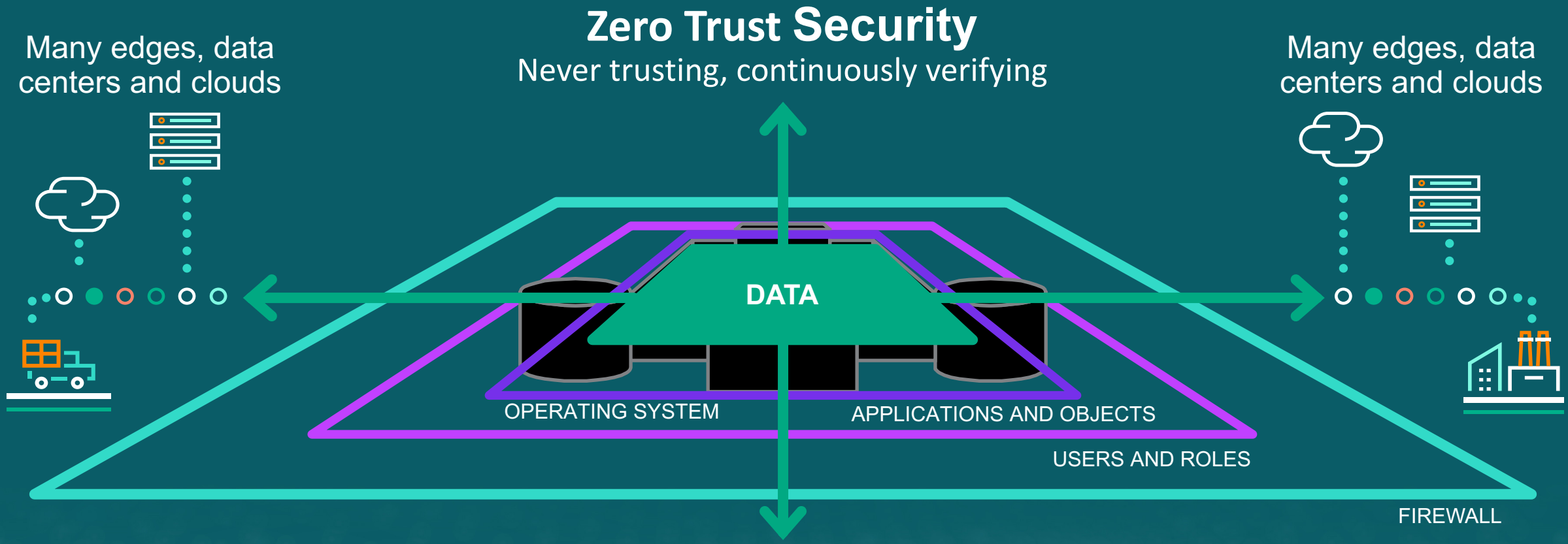
What Does Zero Trust Mean?

Traditional network firewall **perimeter** defense



PCI Security Standards Council®

PCI DSS v4.0 Was Designed With Zero Trust In Mind



Protect from the inside out

Identity aware, data-driven, workload relevant

PCI Security Standards Council®

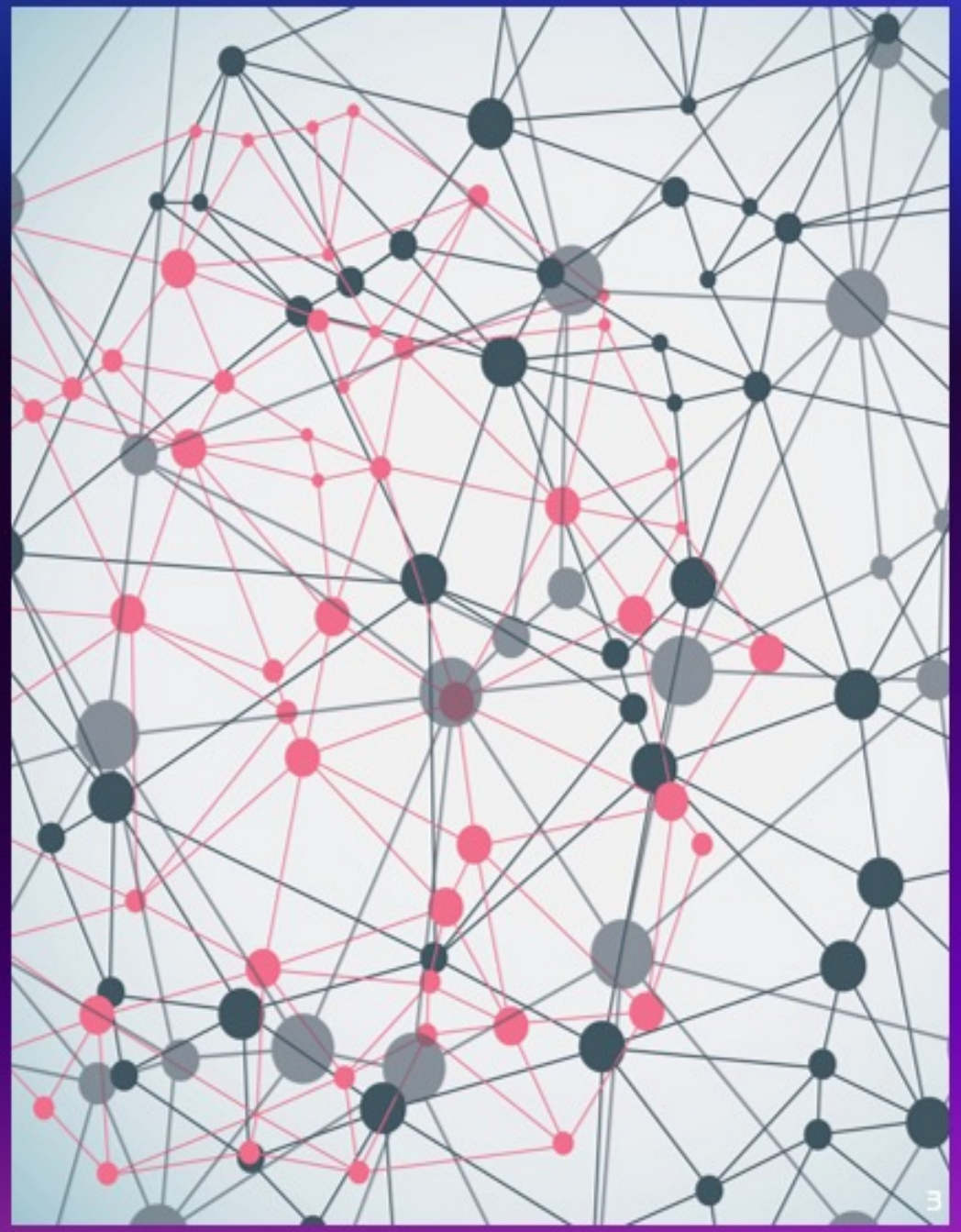
Digital resiliency is an organization's ability to maintain its core functions and recover quickly from any form of cyber disruption.

- Reducing the attack surface and minimizing vulnerabilities and potential entry points for attackers decreases the likelihood of cyber threats.

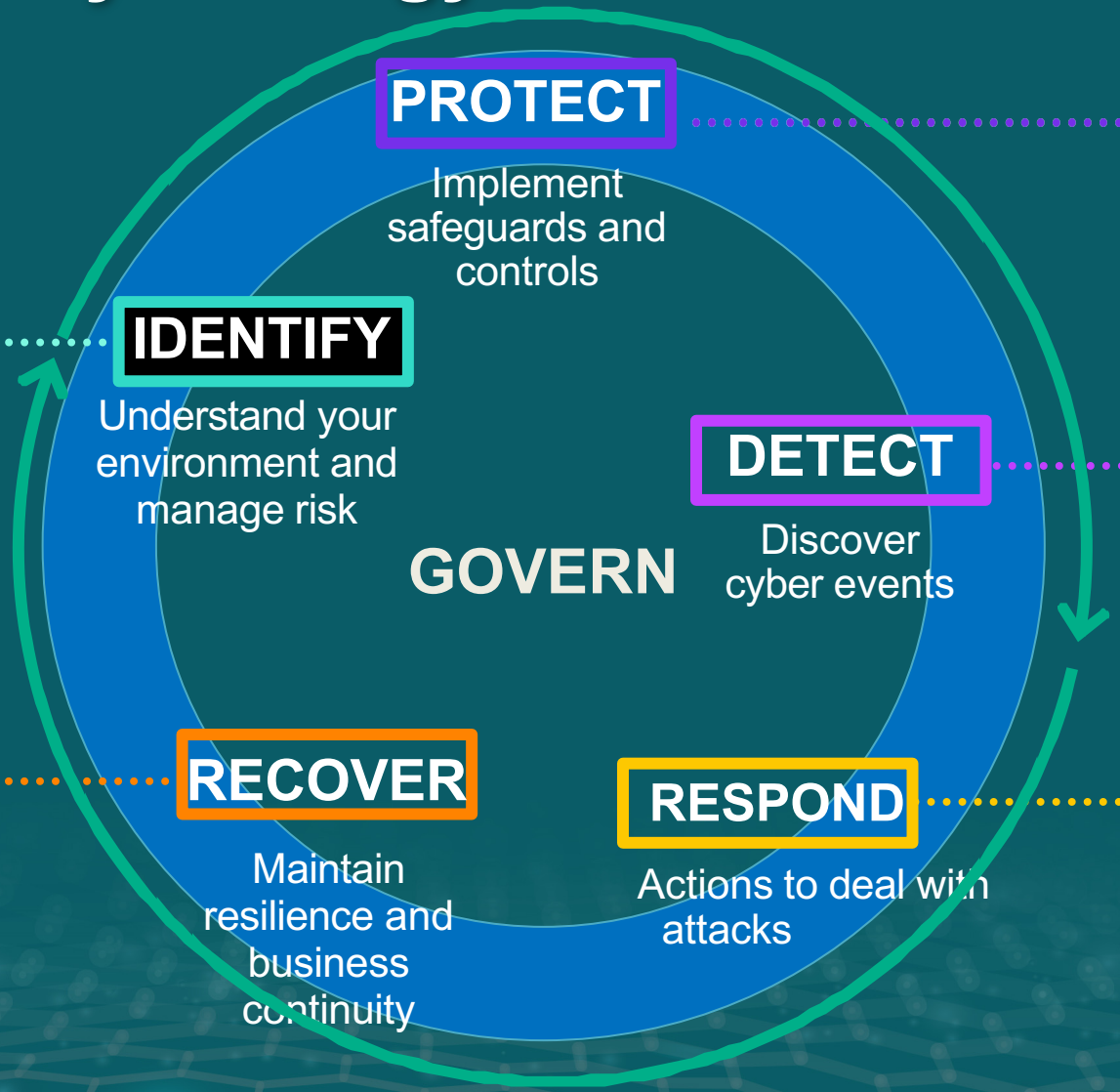
- This is fundamental towards achieving digital resiliency. It ensures that an organization can withstand and recover from cyber incidents with minimal damage

What is Digital Resiliency?

PCI Security Standards Council



Digital Resiliency Strategy



- Security Hardening and PCI DSS Readiness Service

- Cyber Security Gap Assessment Service

- File Integrity
- Threat Detection
- Logging and auditing

- Offline Backup
- Disaster Recovery
- Immutable Data Store

- Real Time Monitoring and Alerting
- SOAR Integration
- SOPs

Aligned with NIST Cybersecurity Framework

PCI Security Standards Council

Identify – Cybersecurity Gap Assessment

- Cyber Resiliency begins with asset identification, inventory, and categorization.
- Security Gap Assessment identifies critical assets and security risks.
- Scan, identify and assess for security misconfiguration, compliance status, and other ransomware attack vectors.
- Used to build a roadmap for subsequent phases.
- Required for PCI DSS v4.0.1

PCI Security Standards Council®

Protect – Security Hardening & PCI Readiness

- Security controls are implemented to reduce the identified attack surface based on gap assessment
- This includes
  - OS Configuration
  - Authentication Controls, Multi-Factor Auth and AD Integration
  - Hardened password controls
  - User and Identity Management
  - Privileged Session Management and Monitoring, Access Controls
  - Secure critical files, objects and assets
  - Implement additional security controls based on Security Assessment findings.

Detect - File and System Integrity Monitoring

Detect Malicious Activity and Ransomware

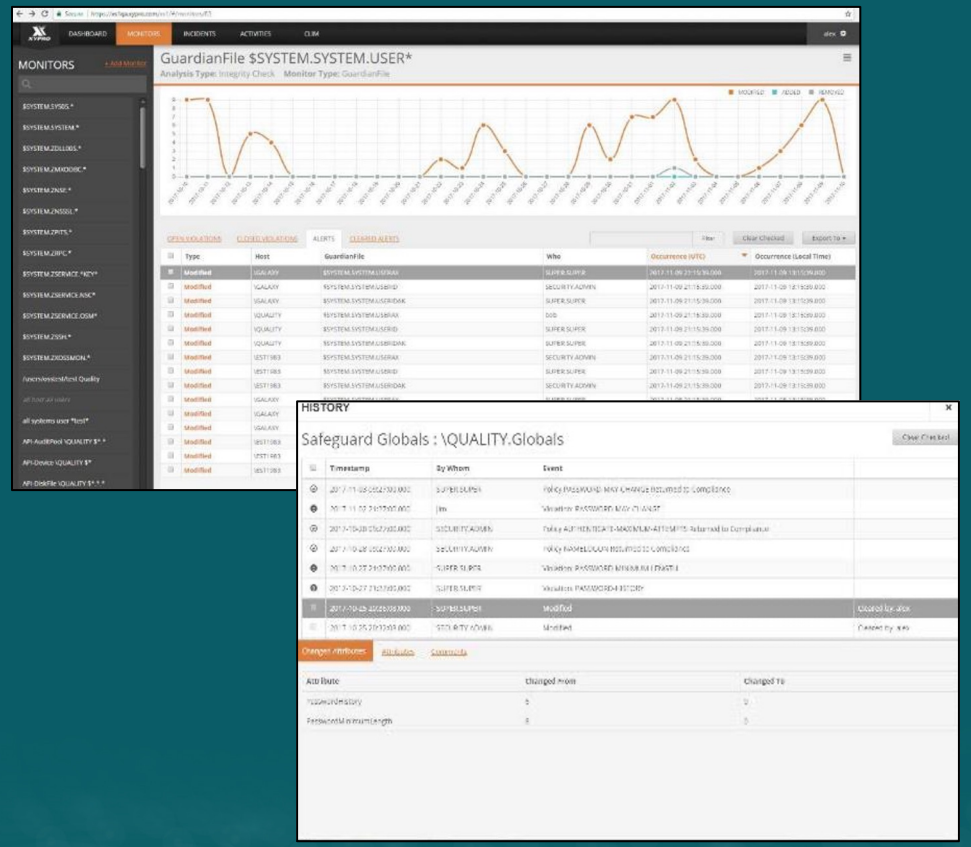
- Detecting unauthorized changes to objects and files is the best defense against malware and ransomware
- FIM triggers alerts early, allowing for swift response
- Implementing FIM as part of a broader cybersecurity strategy to enhances an organization's ability to detect, respond to, and recover from ransomware attacks by maintaining an audit trail of changes.

Identify Human Error

- Detect mistakes before they cause irreparable damage

Necessary for Compliance

- PCI, GDPR, SOX, HIPAA, DORA, FISMA, NIST, HPE NonStop Hardening Guide and other frameworks



PCI Security Standards Council

Detect - File and System Integrity Monitoring

Requirement 10: Track and monitor all access to network resources and cardholder data

- 10.3.4 Use file-integrity monitoring or change-detection mechanisms on logs to ensure that existing log data cannot be changed without generating alerts

Requirement 11: Regularly test security systems and processes

- 11.5.2 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

Requirement 12: Maintain a policy that addresses information security for all personnel

- 12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion- detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.

Best Practices for Implementing PCI DSS into Business-as-Usual Processes

- “Monitoring of security controls—such as firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), file-integrity monitoring (FIM), anti-virus, access controls, etc.— to ensure they are operating effectively and as intended.”

PCI Security Standards Council

Context is Key

XYPRO Patented Technology

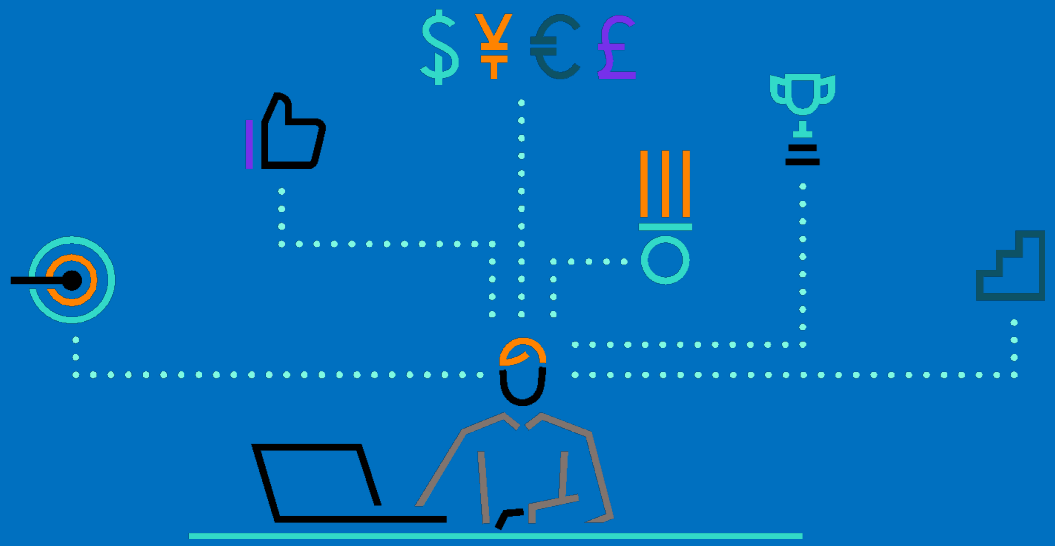
Correlation is not context

Context allows separation of noise from data

XYPRO applies specific knowledge to contextualize events and assess impact

Reduce false positives

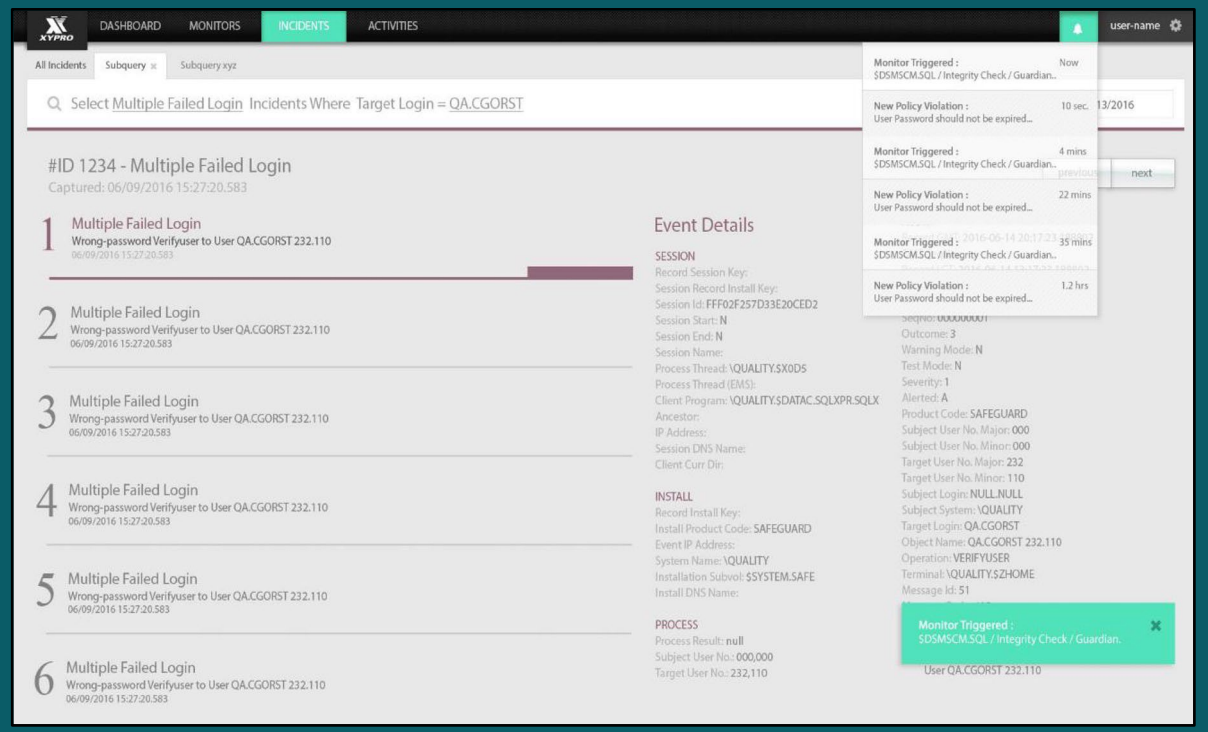
Provide actionable information



CONTEXT TRANSFORMS DATA INTO INFORMATION

PCI Security Standards Council®

Respond - Real Time Alerting For Incident Response



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

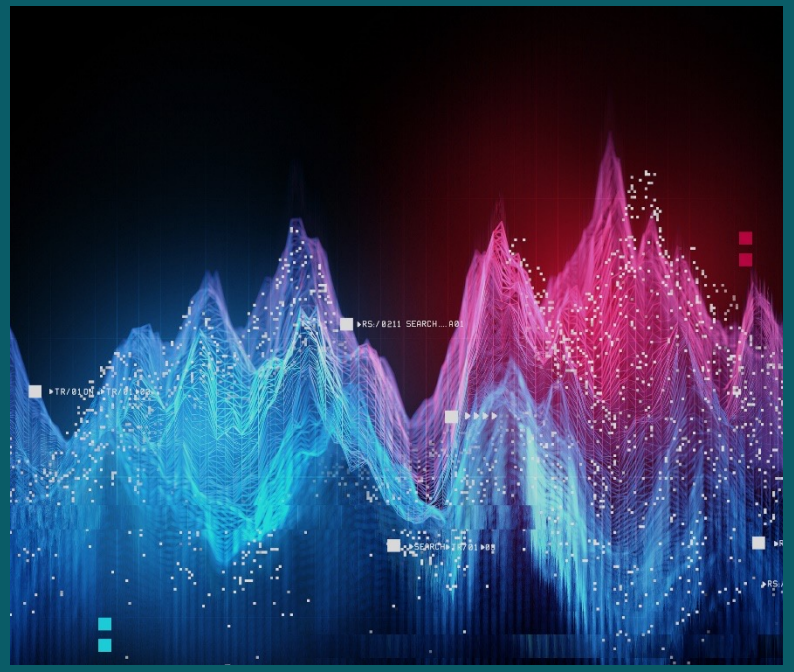
PCI Security Standards Council®

Business Value and Take Aways

Compliance Automation 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

PCI Security Standards Council®

Compliance Reporting Saves 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
Payment Card Industry Data Security Standard

HPE
HPE NonStop Hardening Guide

DFARS
Defense Federal Acquisition Regulation Supplement

GDPR
General Data Protection Regulation

Automation Modernizes Security Resources

Most organizations cannot allocate enough resources to proactively monitor their environment

Data volume, velocity and variety is increasing

Not having the right resources and tools is a risk

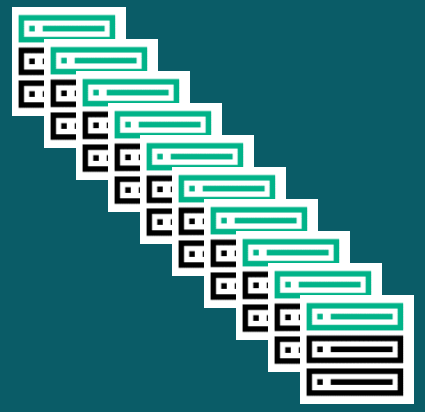
Experience-dedicated resources are shrinking

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

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

PCI Security Standards Council®

Context Enhances Your Enterprise SIEM



SIEM results = $$$$$$$$$$

10 SIEM fees

XYPRO Mission Critical Security = $

1 SIEM fee

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 security events

PCI Security Standards Council

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"

PCI Security Standards Council

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

Thank You

TAKE ACTION

- Sign up for our free security assessment: www.xypro.com/free
- Visit XYPRO: www.xypro.com

- YouTube youtube.com/xyprotechnology
- X @XYPROTechnology
- @SteveTcherchian

- LinkedIn linkedin.com/xyprotechnology
- linkedin.com/stevetcherchian