13TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

cybersecuritysummit.org

RESILIENCE UNLOCKED

TITLE SPONSOR

Island

#cybersecuritysummit #css13

Resilient Networks

Protecting Critical Infrastructure from Ransomware
with Zero Trust

Paul Veeneman

Product & Solution Architecture

BLUERIDGE® NETWORKS

LinkGuard, CyberCloak & AppGuard

https://blueridgenetworks.com

Tony Chiappetta

President, CHIPS

CHIPS

Distributor of AppGuard for North and South America
https://prevent-ransomware.com

Introduction

- Understanding Ransomware Threats
- The Zero Trust Security Framework
- Isolation and Containment Strategies
- Building Resilient Networks
- Implementing a Zero Trust Ransomware Defense Strategy
- Efficiency Gains from Proactive Defense
- Conclusion and Key Takeaways

Understanding Ransomware Threats

Ransomware is a malware designed to deny a user or organization access to files on their computer. Some variants have added additional functionality – such as data theft – to provide further incentive for ransomware victims to pay the ransom.

CheckPoint Software, *https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/*

Threat Vectors

- Phishing Emails: (98% of all threats) The prompting victims to click on a link, download an attachment, or similar malicious activity unbeknown to the target.
- Exploit Kits: Tools cybercriminals use to exploit known vulnerabilities in systems.
- Remote Desktop Protocol (RDP): Taking advantage of exposed RDP service through brute force, credential stuffing techniques. As of October 19th, there are 689,481 exposed RDP service connections in the United States, and approximately 3,604,087 globally. (Source: shodan.io)

Impact, Indirect, & Recovery Costs: US average per ransomware incident was $170,000 - $1.82M.

Varieties of Ransomware: Crypto (most common), Locker, Leakware, RaaS (platform for professionals)

The Zero Trust Security Framework

Zero Trust (ZT) is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated. This is a shift from the traditional model of "trust but verify."

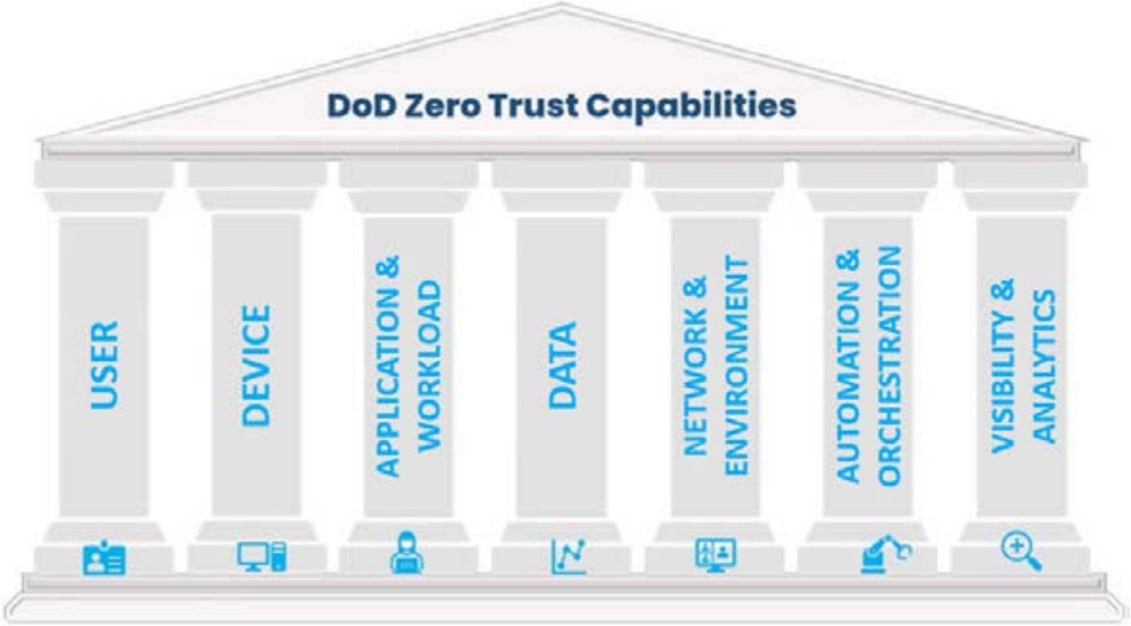
No Implicit Trust: Trust is never assumed for any entity, regardless of their location relative to network perimeters.

Least Privilege Access: Only necessary permissions are provided, and such access is continuously assessed.

Architectural Decomposition: Networks are segmented, separate requests (or data flows) dynamically define access to network resources based on policy.

Continuous Authentication & Authorization: Trust in a resource is continually evaluated and not based on a one-time authentication.

Explicit Policy: Instead of broad network rules, policies are crafted to specify individual transactions.



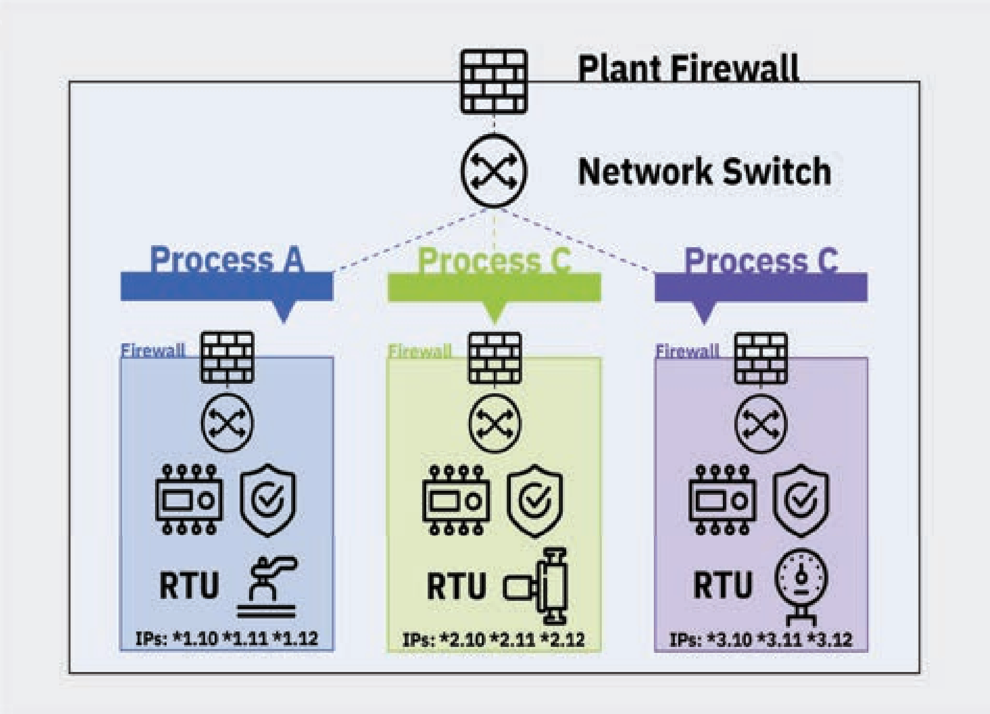
The Zero Trust Security Framework

"The Zero Trust concept has expanded over the years from its early focus chiefly on micro-segmentation of networks. Network segmentation, of course, isn't new. Security teams have used firewalls, access control lists (ACL), and virtual local area networks (VLAN) for network segmentation for years."

Separating the control plane where trust is established from the data plane where actual data is transferred..."Hiding the infrastructure", where all unauthorized packets are dropped for logging and analyzing traffic.

"Micro-segmentation can be effectively achieved...and should always be considered a best practice in implementing a Zero Trust strategy."

Paul Arceneaux, SVP of product and engineering at Mission Secure.



ISA Global Security Alliance, Example of Micro-Segmentation

The Zero Trust Security Framework

Need to continue beyond detection capacities of Antivirus and Endpoint Detection & Response

Stive to:

- Assume the network is compromised
- Minimize uncertainty
- Control use and adoption of Applications
- Enforce Granular Access Control
- Enforce least privilege access

- Ensure only what the organization wants to occur is happening

#StopRansomware Guide v3 released October 2023

Isolation and Containment Strategies

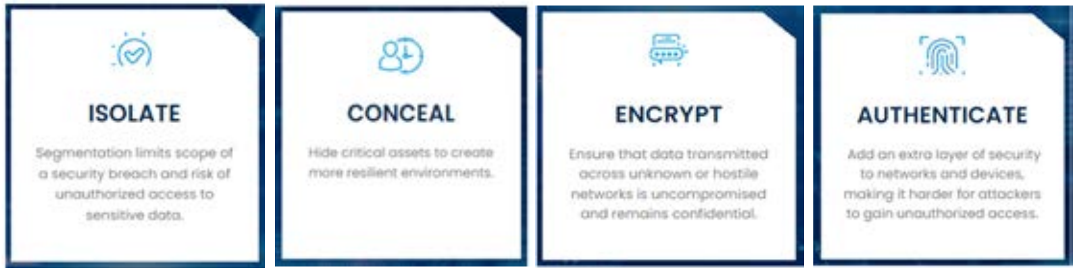
Zero Trust Architecture treats every access request as untrusted, continually validating every interaction.

Network segmentation divides the network into zones, isolating sensitive operations.

Multi-Factor Authentication (MFA) requires multiple verifications, like passwords and biometrics, to grant access.

Advanced endpoint protection offers features beyond traditional antivirus, including behavioral analysis.

No single protection method is foolproof. Best practices involve layers of multiple protective measures to ensure resilience against a variety of threats.



ISOLATE

Segmentation limits scope of a security breach and risk of unauthorized access to sensitive data.

CONCEAL

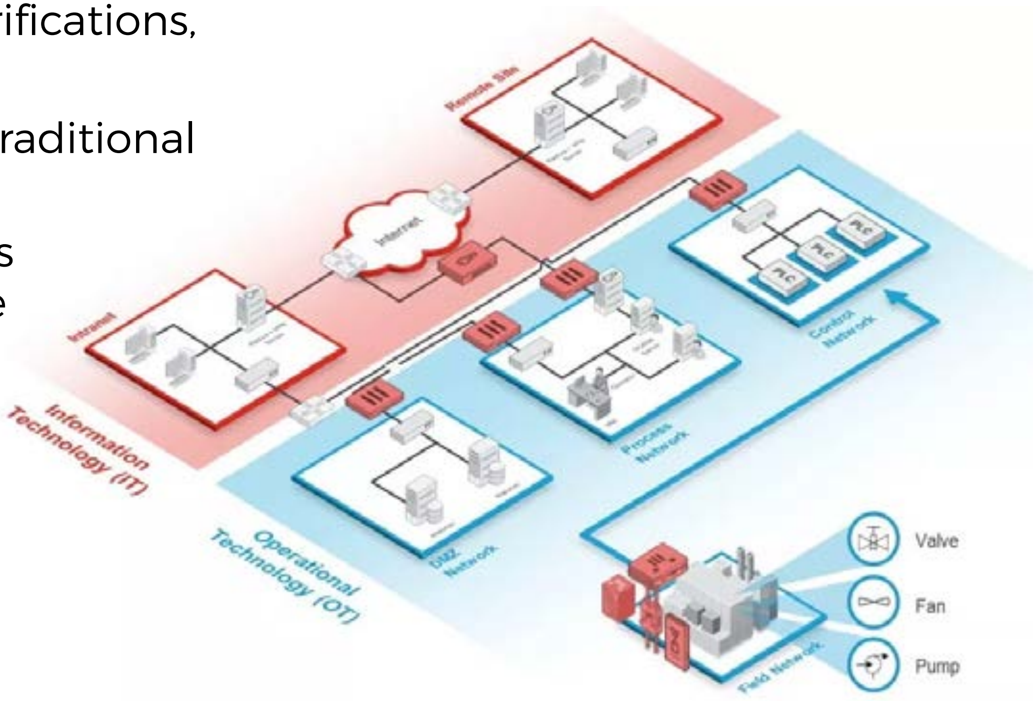
Hide critical assets to create more resilient environments.

ENCRYPT

Ensure that data transmitted across unknown or hostile networks is uncompromised and remains confidential.

AUTHENTICATE

Add an extra layer of security to networks and devices, making it harder for attackers to gain unauthorized access.

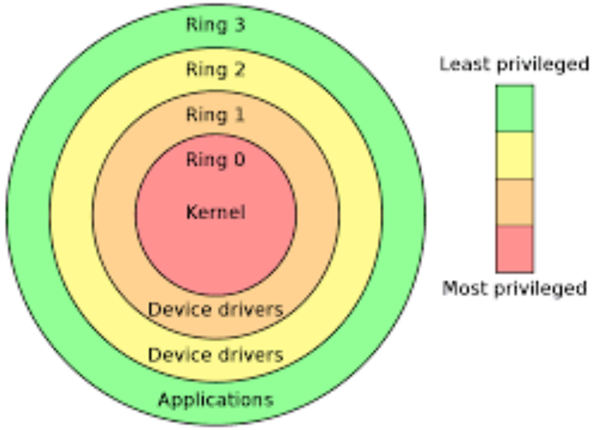


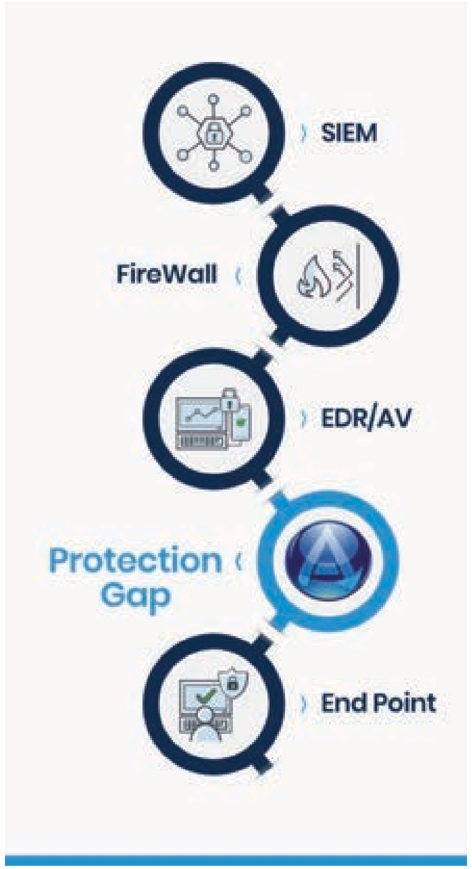
Isolation and Containment Strategies

Users can be the weakest link in the chain

Zero Day Vulnerabilities continue to be discovered within Applications and the Windows OS

Isolation of the OS Kernel ensures integrity and circumvents exploitation.



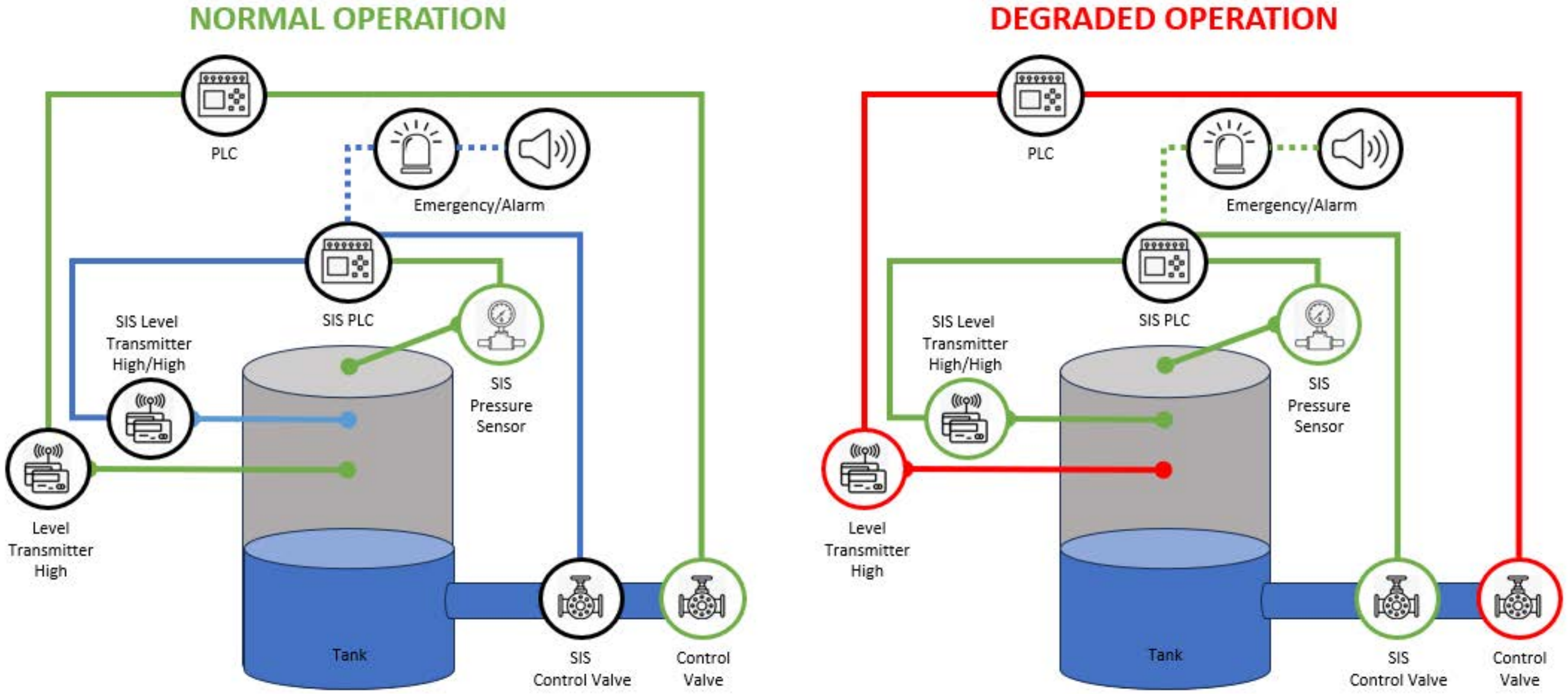


Resilience in OT: Safety First

Safety Instrumented Systems (SIS) in OT environments are critical for activating safety protocols during anomalies. Cyber threats targeting OT systems are on the rise. Isolated SIS are shielded from malicious intrusions and malware attacks, providing robust defense and reducing the risk of jeopardizing critical systems and assets in OT environments.

OT Resilience is dependent on the SRP Triad as opposed to the CIA Triad

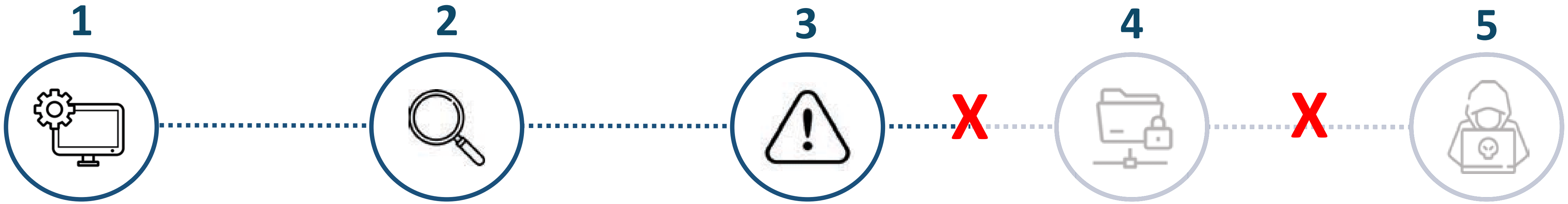
- Safety
- Reliability
- Productivity



Building Resilient Networks

Goals of IT	**How**
• Assume the network is compromised • Minimize uncertainty • Control use and adoption of Applications • Enforce Granular Access Control • Enforce least privilege access • • Ensure only what the organization wants to occur is happening	• Not more Detection, but Strict Policy Enforcement • Only allow Trusted Actions of Trusted Applications • Beyond Whitelisting • Dynamic Application Control • • Isolation and Containment – Running applications can not impact other applications, including the Operating System

Implementing a Zero Trust Ransomware Defense Strategy – Anatomy of an Attack



Gain an Entry Point

- Awareness & Training
- Close Open Ports
- Multifactor Authentication
- Reduce Attack Surface
- Perimeter Boundary Monitoring

Scanning & Discovery

- Isolation & Segmentation
- Cloaking & Obfuscation
- Network Protocol Monitoring
- Network Anomaly Detection

Gain Access to Assets

- Endpoint Protection
- Endpoint Anomaly Detection
- File Integrity Monitoring
- Account Access Monitoring

Encrypt, Lock Files

Demand Ransom

Implementing the Security and Compliance program layered defenses highlighted to the left work in concert to thwart the goals and objectives above of the ransomware cyber criminals.

Proactive Defense Strategies

Advanced Threat Protection tools: Utilizing modern cybersecurity tools that can detect and quarantine ransomware before it begins its encryption process.

Patch and Update: Keeping software, OS, and applications updated to patch vulnerabilities.

Employee Training: Educating staff about the dangers of phishing emails and the importance of strong password practices.

Network Segmentation: Dividing the network into segments to ensure that if one segment is compromised, the ransomware doesn’t necessarily propagate to all parts of the network.

Regular Backups: Ensuring regular and isolated backups of critical data.

Reduced Risks & Vulnerabilities

- ✓ Safety & Continuous Operations
- ✓ Regulatory or Contractual Requirements
- ✓ Qualitative and Quantitative Impact
- ✓ Critical Assets and Data Protection
- ✓ Minimal Incident Response
- ✓ Reallocate Resources to Value-Add Objectives

Conclusion and Key Takeaways

Cybersecurity OT Environments: Organizations must prioritize robust cybersecurity measures to protect their assets and operations.

Layered Defense Strategy: Develop comprehensive strategies against potential threats.

Safety & Resilience: SIS ensures that operations are not only secure but also reliable.

Continuous Vigilance and Adaptation: Response to emerging threats and evolving tactics.

Educate and Train Staff: Human error can often be a vulnerability, ensure that everyone is informed reduces the risk of breaches.

Elevated Cybersecurity Standards: Organizations must raise their cybersecurity expectations and insist on security solutions that deliver a higher standard for protection.

Transition to a Proactive Approach: It's time to shift from relying solely on detection-based solutions to prioritizing prevention-focused measures in our defense strategies.

The Cost of Post-Detonation Response: Waiting to respond after a threat has detonated proves to be too late, as the resulting devastation is often irreparable. This emphasizes the need to shift from a reactive approach to proactive "Isolation and Containment" in security.

Empower Your Workforce: Implement a Zero Trust Operating System to enforce structured company policies and invest in staff training that addresses social engineering and non-IT communication channel threats.

Thank you

Question & Answer

Booth 619 (picture of booth)

APPGUARD
Stops malware EDR/XDR miss
PREVENT UNDETECTABLE MALWARE & ZERO-DAY EXPLOITS WITH APPGUARD!
Prevents Detonation Before Detection
Zero Breach™ Since 2014 Inception
Future Proof
Containment and Isolation
APPGUARD
Stops malware EDR/XDR miss
MAKE HACKERS PLAY BY YOUR RULES
Application Isolation & Containment
Auto-Adaptive Protection
Eliminated Attack Surface
Mitigate Zero-Day Vulnerabilities
Simplified Threat Prevention
End Patching Pressure
Preserve Legacy Systems
Future-Proof Security
APPGUARD
Zero Trust Endpoint Protection
In A Connected World