Cybersecurity and Ransomware Protection Starts with **Hardware & AI**
UNDERSTANDING RANSOMWARE

WHAT IS RANSOMWARE?
• Unauthorized Access + Malicious Software
• Denies Access + Encrypts Data

POTENTIAL OUTCOMES
• System Inaccessibility
• Data Theft or Deletion

RANSOM DEMANDS
• Complete System Control
• Ransom Payment Demanded

MODERN RANSOMWARE TACTICS
• Encryption and Bitcoin Payment
• Harassment + Double/Triple Extortion
• Previous Fail-Safe Insufficient

THE EVOLVING LANDSCAPE OF RANSOMWARE ATTACKS
• Ransomware attacks becoming highly sophisticated.
• In 2022, a malicious ransomware attack eluded detection for 324 days, with an additional 91 days required to regain control from the attack.

An estimated 4,000 attacks occur daily and this statistic is an understatement.
TODAY’S STATE-OF-THE-ART SECURITY SOLUTIONS

Ransomware Vulnerabilities

- Malicious System Access
- Physical Breaches
- Credential Compromise
- "Ports of Entry" Exposure
- Lack of Real-Time Detection

Current mitigation methods

- Traditional Hardware Security Methods
- Perimeter Security (VPN)
- Platform Firmware Resiliency
- DPU Packet Inspection
- Zero-Trust Architecture
CURRENT SECURITY TECHNOLOGY LIMITATIONS

**CANNOT RECOVER FROM AN ATTACK**

Lacks ability to recover from persistent threats without hardware replacement or expensive truck-rolls.

**NO RANSOMWARE PROTECTION, NO FORENSIC DATA**

Existing TPM-based methods are unable to detect exploits of new vulnerabilities.

**DELAYED OR NO PATCHING**

Most existing servers have limited firmware storage that prevent new larger patches. Use of multiple discrete parts grew attack surface that needs frequent patching.

**PIECEMEAL, DISCRETE SOLUTIONS**

Replacing discrete control & management solutions.

**WEAK ZERO-TRUST**

Root keys can be extracted to impersonate an identity. Software-based implementation proven to be easily corrupted to by-pass protection.

**Field upgradability and configuration**

**AI-driven attack prevention, forensic data collection, and learning**

**System-driven proactive monitoring and updates**

**Purpose-built, AI-driven comprehensive security processors**

**Enhancing Zero-Trust model with AI-driven HW**
AXIADO TRUSTED CONTROL/COMPUTE UNIT (TCU)
COMPREHENSIVE PLATFORM SECURITY FOR DATACENTERS

DATA CENTER SERVER

DISTRIBUTED INFRASTRUCTURE OPEN STANDARDS FOR MODULAR SECURITY

Smart SCM
- Ownership transfers
- Upgradeability
- Server-vendor neutral

Accelerated DC-SCM adoption

AXIADO © 2023. ALL RIGHTS RESERVED. | SEPTEMBER 2023 | AXIADO.COM
# AXIADO TCU
## BUILT-IN FEATURES TO MITIGATE THE SPREAD OF CYBERATTACKS

<table>
<thead>
<tr>
<th>1. FORENSICS</th>
<th>2. ANOMALY DETECTION</th>
<th>3. ISOLATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HARDWARE-ANCHORED RANSOMWARE PREVENTION</strong></td>
<td><strong>SIDE-CHANNEL ATTACK DETECTION</strong></td>
<td><strong>MULTI-TENANT VIRTUALIZATION AND MULTI-NODE</strong></td>
</tr>
<tr>
<td>Hardware forensic data enhancing detection efficacy</td>
<td>Monitors all platform sensors in real-time</td>
<td>End-user isolation prevents cyberattack spread</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. KEY MANAGEMENT &amp; OWNERSHIP PROVISIONING</th>
<th>5. RESILIENCY</th>
<th>6. BENEFITS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HW OWNERSHIP PROVISIONING</strong></td>
<td><strong>HIGH RESILIENCY AND FAST INFRASTRUCTURE RECOVERY</strong></td>
<td><strong>RUNTIME ATTESTATION</strong></td>
</tr>
<tr>
<td>Comprehensive and secure commission/decommission for platform lifecycle management</td>
<td>In-service upgrades and recovery w/o service disruption</td>
<td>Monitors integrity of all platform software</td>
</tr>
<tr>
<td><strong>HARDWARE SECURITY MODULE</strong></td>
<td><strong>HW-BASED PLATFORM SECURITY</strong></td>
<td></td>
</tr>
<tr>
<td>Fast secrets and key management</td>
<td>End-to-end supply chain security</td>
<td></td>
</tr>
</tbody>
</table>

**BENEFITS**
- Cost savings with AI-based breach mitigation (average —$3M/breach; IBM Research, 2022)
- ↓ 30% total solution cost
- ↓ maintenance cost (ongoing) through unified firmware
- 1000x more granular lifetime of virtual container (milliseconds)
- 2x capacity at bare metal supported
- 25% less software components lead to smaller attack surface
- Local key and secret management
- ↓ 50% form factor size
HARDWARE-ANCHORED AI-ENABLED SECURITY DETECTION, PROTECTION & PREDICTION

TRAINING CLUSTER

DATA LAKE
- Ransomware datasets
- Sensor datasets
- Network datasets
- Behavioral datasets

MLOPS PIPELINE
1. Customer hosted
2. Axiado hosted

DETECTION
Notifies SecOps

PROTECTION
TCU takes local action
- Example: shutdown network port, server, etc.

PREDICTION
Boot time and runtime vulnerability checks — XDR

Axiado deploying AI methods to mitigate ransomware attacks
AXIADO’S FOCUS PILLARS

*Example players

*Ecosystem OEM/ODM

Open Compute Project (OCP) Community & Startup

Hardware-Anchored AI-Enabled Security

Full-stack DC-SCM, NIC, Software

Axiado Trusted Control/Compute Module (TCU) Building Blocks

*Cloud Service Providers

SENSOR AI SIDE-CHANNEL ATTACK DETECTION FORENSIC AI RANSOMWARE ATTACK DETECTION BEHAVIORAL AI BEHAVIOR ANOMALY DETECTION NETWORK AI NETWORK ATTACK DETECTION

*Example players

AMD wynn Tyan

Gigabyte AI Ericsson

Senao VVDN

Cloudflare Akamai AWS Converge Equinix

Google Oracle Meta

Microsoft NVIDIA Rakuten Jio
AXIADO’S TCU EMPOWERING MODERN SECURITY

AXIADO TCU: A VERSATILE ARSENAL
• Enhanced Security, Visibility, Control
• Serving CSPs, Co-Los, OEMs, and Enterprises

KEY FEATURES
• Hardware-Level Forensic Data Monitoring
• Early Anomaly Detection
• Granular System Control
• Secure Hardware Ownership Transfers

HOLISTIC SECURITY SOLUTION
• Tailored for Modern Infrastructure
• Robust and Intelligent Defense

INNOVATION AND RESILIENCE
• TCUs Lead in Evolving Cybersecurity
• Multifaceted Defense Strategy
• Hardware Monitoring, Anomaly Detection, Granular Control, Secure Management

EMPOWERING CONFIDENCE
• Confronting Evolving Threats with Assurance and Fortitude

ABOUT AXIADO
Axiado is a San Jose, CA-based company focused on cybersecurity semiconductor deploying a novel, hardware-anchored, AI-driven approach to platform security against ransomware, supply chain, side-channel and other cyberattacks in the growing ecosystem of cloud data centers, 5G networks and network switching.

For more info, visit us at axiado.com