AXIADO

Cybersecurity and Ransomware Protection Starts with Hardware & AI

2023

AXIADO.COM

UNDERSTANDING RANSOMWARE

WHAT IS RANSOMWARE?

- Unauthorized Access + Malicious Software
- Denies Access + Encrypts Data

POTENTIAL OUTCOMES

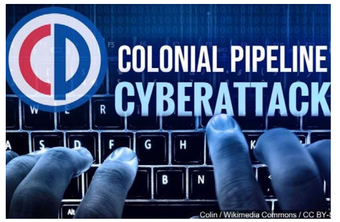
- System Inaccessibility
- Data Theft or Deletion

RANSOM DEMANDS

- Complete System Control
- Ransom Payment Demanded

MODERN RANSOMWARE TACTICS

- Encryption and Bitcoin Payment
- Harassment + Double/Triple Extortion
- Previous Fail-Safe Insufficient



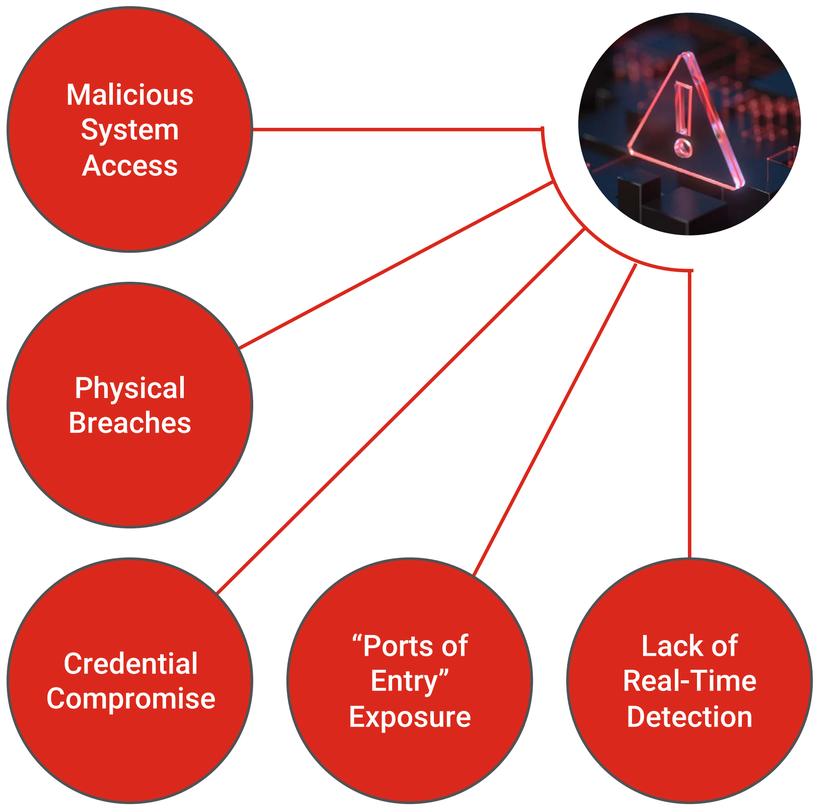
THE EVOLVING LANDSCAPE OF RANSOMWARE ATTACKS

- 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.

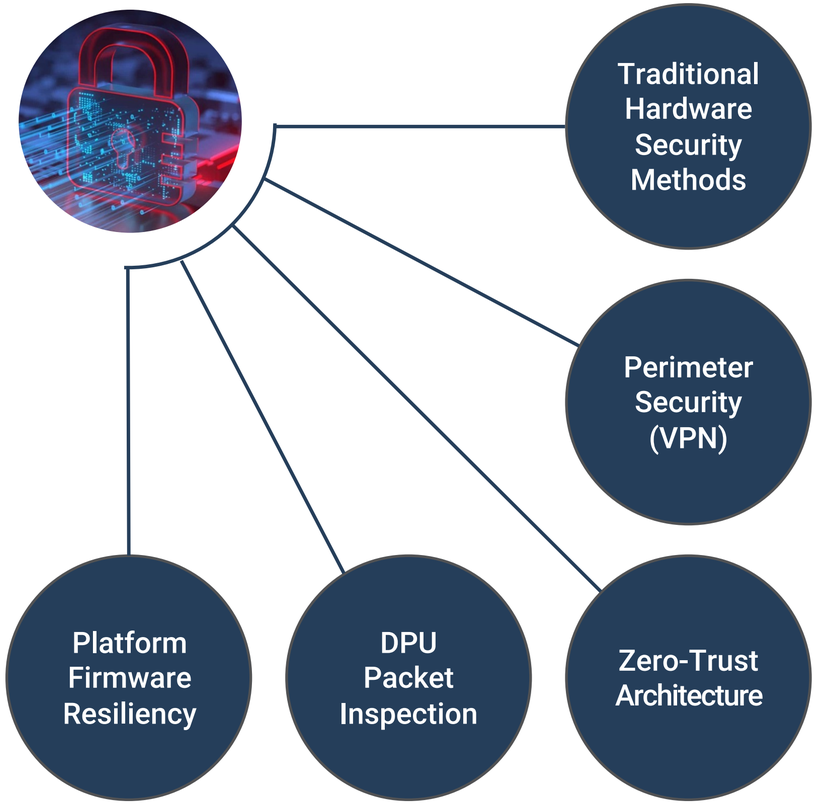
An estimated 4,000 attacks occur daily and this statistic is an understatement.

TODAY'S STATE-OF-THE-ART SECURITY SOLUTIONS

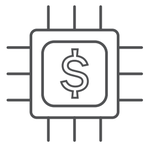
Ransomware Vulnerabilities



Current mitigation methods



CURRENT SECURITY TECHNOLOGY LIMITATIONS



CANNOT RECOVER FROM AN ATTACK

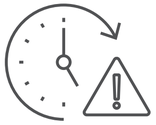
Lacks ability to recover from persistent threats without hardware replacement or expensive truck-rolls.

TCU **Field upgradability and configuration**

NO RANSOMWARE PROTECTION, NO FORENSIC DATA

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

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



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.

TCU **System-driven proactive monitoring and updates**

PIECEMEAL, DISCRETE SOLUTIONS

Replacing discrete control & management solutions.

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

WEAK ZERO-TRUST

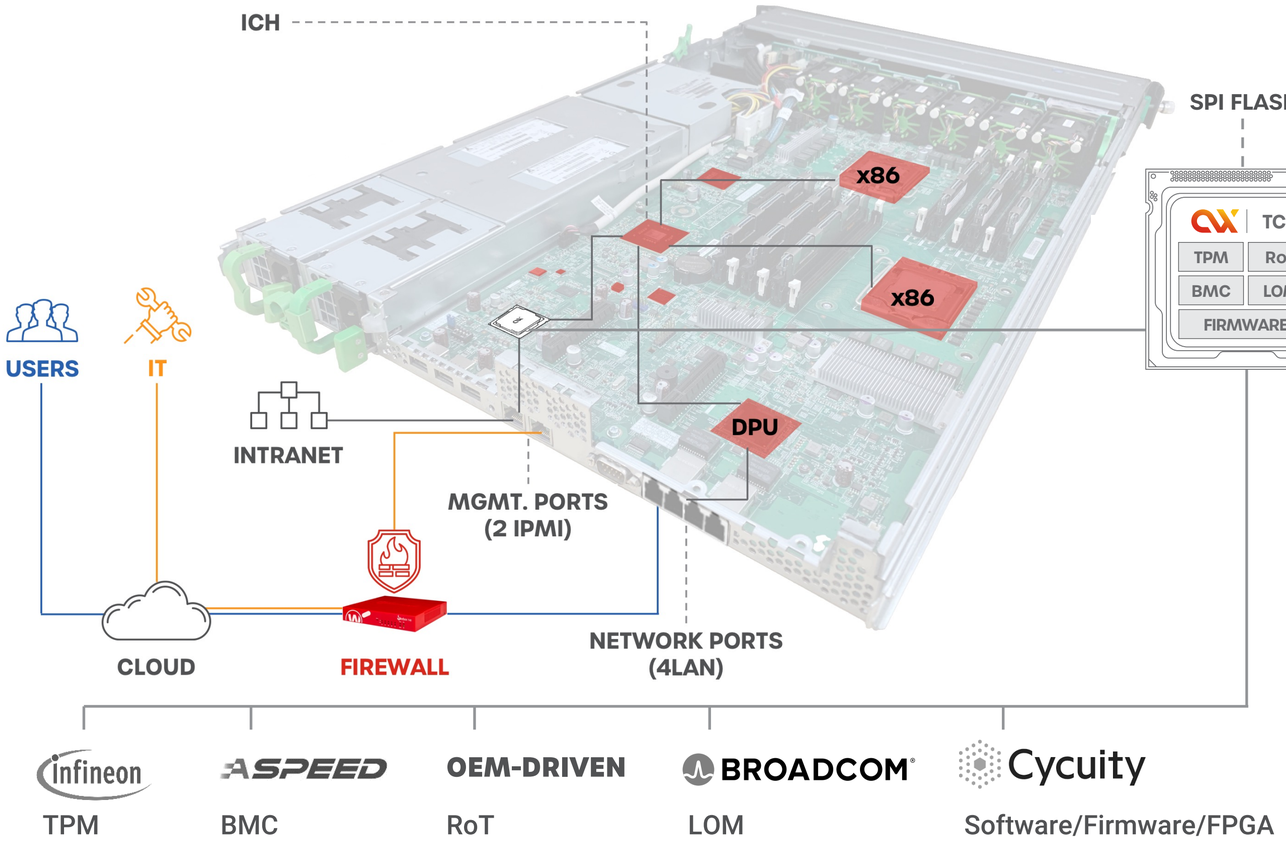
Root keys can be extracted to impersonate an identity.

Software-based implementation proven to be easily corrupted to by-pass protection.

TCU **Enhancing Zero-Trust model with AI-driven HW**

AXIADO TRUSTED CONTROL/COMPUTE UNIT (TCU)
COMPREHENSIVE PLATFORM SECURITY FOR DATACENTERS

DATA CENTER SERVER

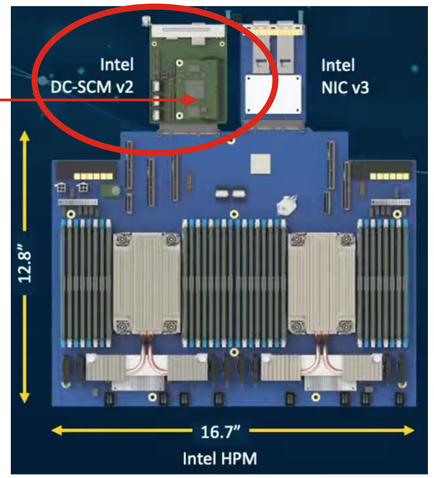


DISTRIBUTED INFRASTRUCTURE OPEN STANDARDS FOR MODULAR SECURITY

Smart SCM

- Ownership transfers
- Upgradeability
- Server-vendor neutral

OPEN STARTUP™



Accelerated DC-SCM adoption

AMD · ami · AMPERE · CLOUDFLARE · DELL · Google · Hewlett Packard Enterprise · IBM · inspur · intel · Microsoft · ORACLE · TYAN

AXIADO TCU
BUILT-IN FEATURES TO MITIGATE THE SPREAD OF CYBERATTACKS

1. FORENSICS

HARDWARE-ANCHORED RANSOMWARE PREVENTION
Hardware forensic data enhancing detection efficacy

2. ANOMALY DETECTION

SIDE-CHANNEL ATTACK DETECTION
Monitors all platform sensors in real-time

FAST ANOMALY DETECTION (<1 MINUTE)
On-board runtime protection minimizes impact of an attack

3. ISOLATION

MULTI-TENANT VIRTUALIZATION AND MULTI-NODE
End-user isolation prevents cyberattack spread

4. KEY MANAGEMENT & OWNERSHIP PROVISIONING

HW OWNERSHIP PROVISIONING
Comprehensive and secure commission/decommission for platform lifecycle management

HARDWARE SECURITY MODULE
Fast secrets and key management

5. RESILIENCY

HIGH RESILIENCY AND FAST INFRASTRUCTURE RECOVERY
In-service upgrades and recovery w/o service disruption

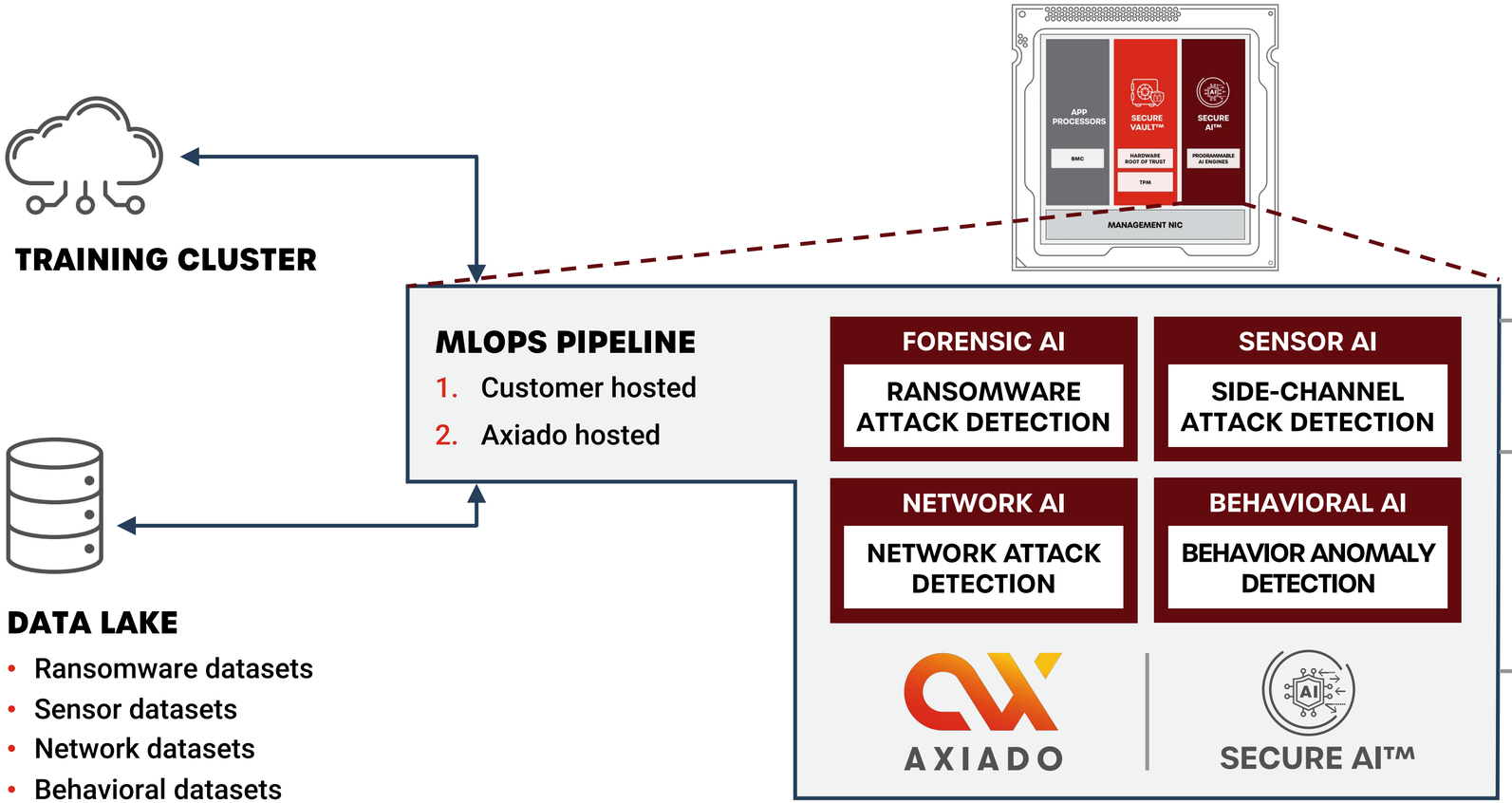
HW-BASED PLATFORM SECURITY
End-to-end supply chain security

RUNTIME ATTESTATION
Monitors integrity of all platform software

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



Axiado deploying AI methods to mitigate ransomware attacks

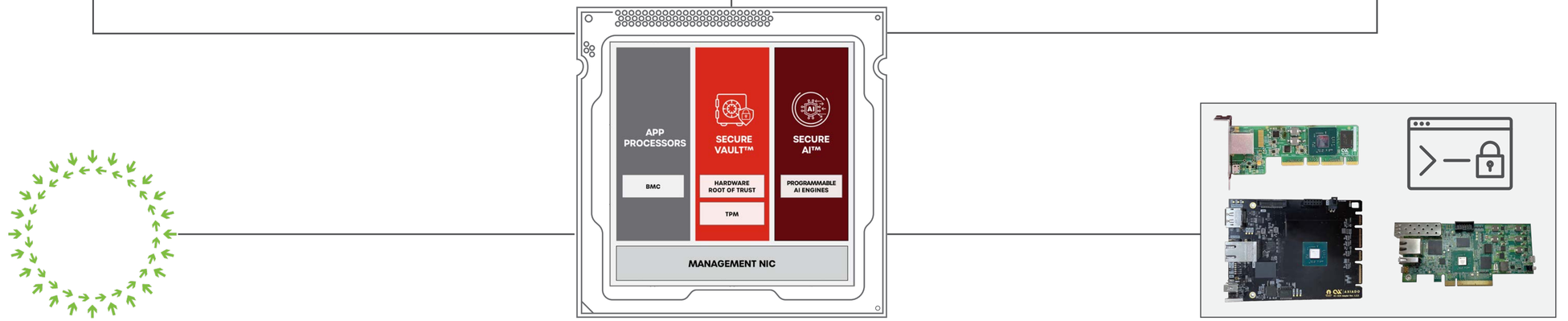
AXIADO'S FOCUS PILLARS

*Example players

*Ecosystem OEM/ODM

*Cloud Service Providers

Hardware-Anchored
AI-Enabled Security



Open Compute Project (OCP)
Community & Startup

Axiado Trusted Control/Compute Module (TCU)
Building Blocks

Full-stack
DC-SCM, NIC, Software

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

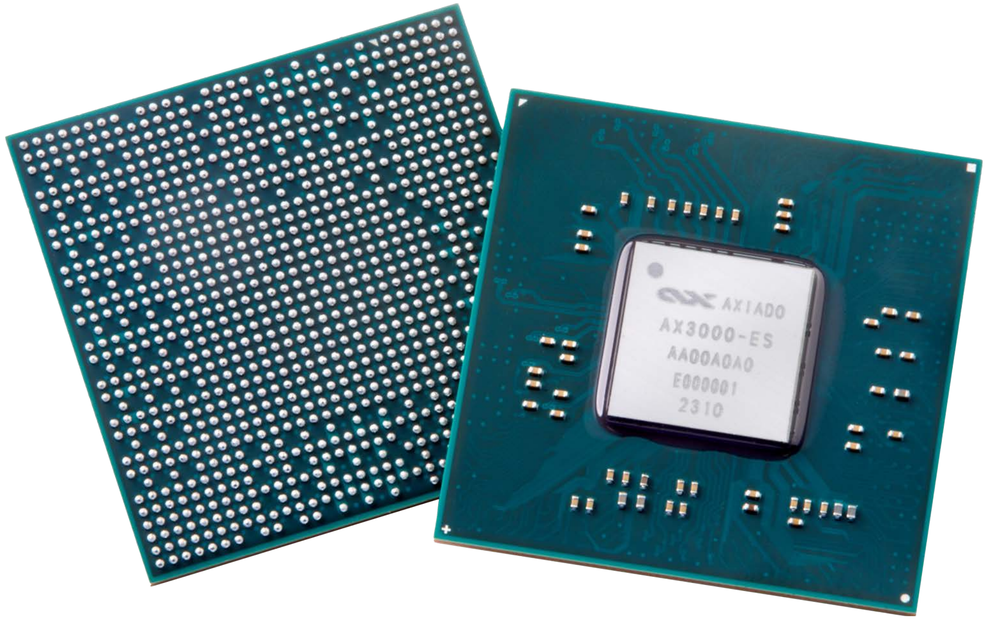
- Tailored for Modern Infrastructure
- Robust and Intelligent Defense

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