PLAYBOOK_

6 Steps to Implement Hardware Supply Chain Security for Banking

A Practical Guide for Cybersecurity Leaders

EXECUTIVE SUMMARY

Banking institutions face a critical but often overlooked vulnerability: the hardware that powers their operations. While cybersecurity teams focus heavily on software threats, malicious actors increasingly target the physical infrastructure itself. From compromised network switches to tampered server components, hardware-level attacks can bypass traditional security controls and establish persistent footholds in banking networks.

This guide provides cybersecurity leaders with actionable strategies to secure their hardware supply chains, from vendor selection through operational monitoring. The financial sector's reliance on complex, interconnected infrastructure makes hardware security not just important, but essential for maintaining customer trust and regulatory compliance.

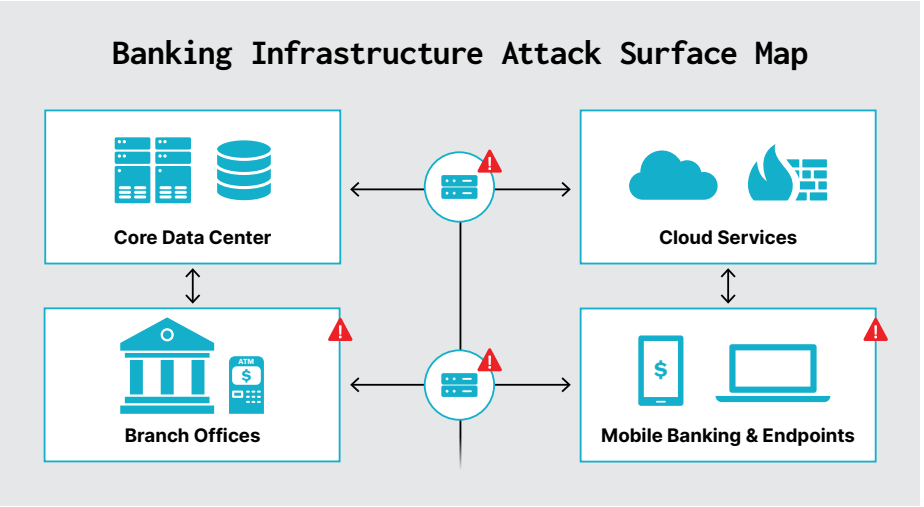
Table of Contents

Understanding the Hardware Threat Landscape

The Expanding Attack Surface

Modern banking infrastructure depends on thousands of hardware components: servers processing transactions, network equipment routing sensitive data, security appliances protecting perimeters, and endpoint devices accessing critical systems. Each component represents a potential entry point for attackers.

Hardware-level compromises differ fundamentally from software attacks. Malicious modifications to firmware or physical components can survive operating system reinstalls, security patches, and even complete software rebuilds. These attacks operate below the level where most security tools can detect them, making them particularly dangerous for financial institutions.



Common Hardware Attack Vectors

Supply Chain Infiltration

Malicious components inserted during manufacturing or distribution. Attackers may target specific organizations or deploy widespread modifications hoping to compromise valuable targets.

Firmware Manipulation

Unauthorized changes to device firmware that alter device behavior while maintaining normal appearance. These modifications can create backdoors, steal credentials, or exfiltrate data. For more examples, check out the *Top 5 Firmware and Hardware Attack Vectors*.

Physical Tampering

Direct modification of devices after delivery but before deployment, or compromise of devices already in production environments.

Vendor Compromise

Attackers target hardware vendors or their supply chains, using legitimate update mechanisms to distribute malicious firmware or software.

The Financial Impact

Hardware compromises can result in extended network access for attackers, often going undetected for months or years. The cost of response includes not just incident remediation, but hardware replacement, network reconstruction, and potential regulatory penalties. Recovery time extends far beyond typical software incidents, as organizations must verify the integrity of their entire infrastructure.

Step 1: Assess Your Hardware Security Posture

Infrastructure Inventory and Classification

Effective hardware security begins with understanding what you have. Create comprehensive inventories of all network infrastructure, servers, security appliances, and critical endpoints. Document hardware models, firmware versions, vendor information, and deployment locations.

Most organizations already have some level of inventory and asset management in place. This is great news! You probably already have some of the tools you need.

However, there are common gaps when it comes to infrastructure visibility, which may require new tools or processes to account for:

- **Component level inventory:** Knowing which hardware components, chips, and firmware versions are present within your network infrastructure is critical. Network devices are often not built to be scanned, inventoried, or protected by traditional network tools. You can't install EDR on a firewall.
- **Monitor integrity Over Time:** Knowing which firmware versions you have in place is one thing. Knowing when they change, whether authorized or not, is another. The ability to monitor for unauthorized changes in the firmware, BIOS, and hardware components over time is an important part of hardware and supply chain security.
- **The computer inside the computer:** Every server, laptop, and network appliance contains components such as baseboard management controllers (BMCs) that run their own operating systems, separate from the host operating system on the computer. These often run versions of Linux, which have their own vulnerabilities and attack vectors. These systems are often unmonitored, leaving the door open for attackers to break in and hide their activities.

33%

of all incidents investigated by Mandiant started with exploitation of a vulnerability as the initial intrusion vector.

Most Frequently Exploited Vulnerabilities

- **PAN-OS GlobalProtect (Palo Alto Networks)** CVE-2024-3400
- **Connect Secure VPN (Ivanti)** CVE-2023-46805
- **Policy Secure (Ivanti)** CVE-2024-21887
- **FortiClient EMS (Fortinet)** CVE-2023-48788

Classify devices based on their criticality and exposure. Core banking systems, internet-facing infrastructure, and devices with administrative access require the highest security standards. Branch office equipment and employee workstations need appropriate protections based on their access to sensitive systems.

Identifying Vulnerable Components

Focus attention on devices that process sensitive data, provide network connectivity, or have privileged access. Network switches and routers handle all traffic and represent high-value targets. Servers running core banking applications require protection due to their access to customer data. Security appliances themselves can become attack vectors if compromised.

Consider the age and update status of your infrastructure. Older devices may lack modern security features or receive infrequent updates. Devices from manufacturers with poor security track records need additional scrutiny.

Additionally, End of life devices often remain deployed in production long after their sell-by date. These devices often fall victim to both new and previously discovered vulnerabilities and cyberattacks. Attackers can scan the internet to discover EOL devices to target with new or existing exploits. To learn more about the risk of attacks against end-of-life hardware and infrastructure like network routers and switches, check out our blog post: EOL Devices: Exploits Will Continue Until Security Improves.

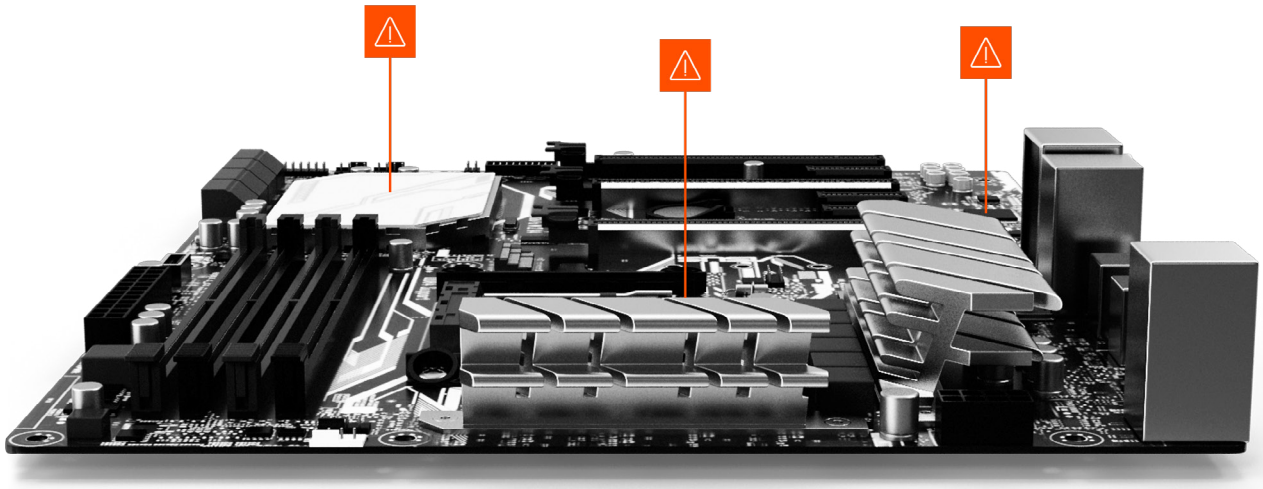
Current State Assessment

Evaluate your existing hardware security practices.

- How do you verify hardware integrity when devices arrive?
- What processes govern firmware updates?
- How do you detect unauthorized hardware changes?

Document gaps between current practices and security requirements.

Review vendor relationships and procurement processes. Understand your supply chain dependencies and assess vendor security practices. Identify single points of failure where compromise could have widespread impact.



Step 2: Secure Your Hardware Procurement Process

Vendor Selection and Management

Choose hardware vendors based on security practices, not just features and price. Evaluate vendors' manufacturing security, supply chain controls, and incident response capabilities. Require vendors to provide detailed security documentation and undergo security assessments.

Establish ongoing vendor management processes. Security is not a one-time evaluation but requires continuous monitoring of vendor security posture, incident notifications, and regular reassessments.

Supply Chain Security Requirements

Implement contractual requirements that address security throughout the supply chain. Require vendors to maintain chain of custody documentation, implement tamper-evident packaging, and provide cryptographic verification of firmware integrity.

Consider geographic and geopolitical risks in your supply chain. Understand where components are manufactured, assembled, and distributed. Implement additional controls for hardware from higher-risk regions or vendors.

Procurement Process Controls

Establish secure receiving procedures for new hardware. Inspect packages for signs of tampering, verify serial numbers against purchase orders, and document chain of custody. Consider using trusted delivery services and requiring direct shipment from manufacturers.

Implement hardware staging areas where devices undergo security verification before production deployment. This isolation prevents potentially compromised devices from accessing production networks during testing.

Trust and Regularly Verify_

Every change to hardware and firmware can be audited throughout the entire life of the device from creation to retirement.

Step 3: Pre-Deployment Verifications

Hardware Integrity Verification

Develop procedures to verify hardware authenticity and integrity before deployment. This includes physical inspection for tampering, verification of serial numbers and authenticity markers, and comparison against known good configurations.

Use manufacturer-provided tools to verify firmware integrity where available. Many enterprise hardware vendors provide cryptographic verification capabilities that can detect unauthorized firmware modifications.

Baseline Configuration Management

Establish secure configuration baselines for all hardware types in your environment. Document required firmware versions, configuration settings, and security features. Use these baselines to verify new devices and detect configuration drift in production.

Implement automated tools where possible to apply and verify configurations. Configuration management systems can reduce human error and ensure consistent application of security settings across large deployments.

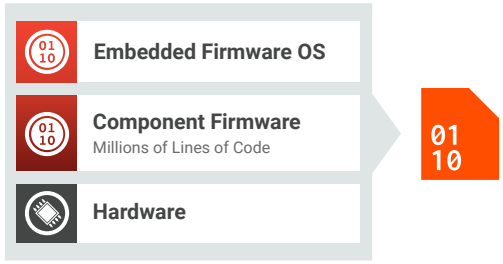
Testing and Validation

Create testing procedures that verify both functionality and security before production deployment. Test network isolation, access controls, logging capabilities, and integration with existing security infrastructure.

Document all verification steps and maintain records of hardware that has passed security validation. This documentation supports compliance requirements and helps with incident response.

SENSOR_

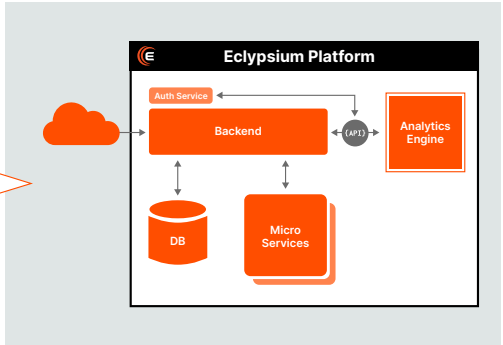
EXTRACTION_



Firmware, OS, and hardware information is extracted, compressed, encrypted, and written to a file for transport.

- Host metadata (IP/Mac/OS info)
- Detailed hardware information
- PCI & Option ROM firmware
- Bootloader information
- BIOS UEFI, SMBIOS, ACPI
- TPM & PCRs
- Intel ME/AMT
- BMC, NIC

ASSESSMENT_



Assessment data is analyzed for:

- Threats—IOC/YARA
- Vulnerabilities
- Configuration Risks
- Change Tracking
- Known Good Verification

Step 4: Operational Security and Monitoring

Continuous Monitoring

Deploy monitoring systems that can detect unauthorized changes to hardware configurations, firmware versions, and device behavior. Network monitoring tools can identify unusual traffic patterns that might indicate compromised devices.

Note: Existing cybersecurity monitoring tools may offer some of these capabilities, but infrastructure has common blind spots not covered by widely deployed security solutions. For example:

- **Endpoint Detection and Response:** While EDR is a critical component of a security toolset, it does not monitor firmware, UEFI, BIOS, and other areas where cyberattacks and vulnerabilities can emerge. Read our e-book: *5 Reasons EPP & EDR Can't Do Supply Chain Security*
- **Vulnerability Management:** Vulnerability management tools can collect versions and let you know of potential, known vulnerabilities, but they lack visibility into the integrity of hardware and firmware over time. You may need new tools to cover malicious firmware modification, configuration drift, and zero day vulnerabilities in hardware and firmware components.

Check out Eclypsium's ebook on *Top 5 Firmware and Hardware Attack Vectors* to understand these risk areas that are not covered by standard security tooling.

Implement regular automated scans to verify firmware versions and configuration settings match approved baselines. Alert on any deviations that might indicate tampering or unauthorized changes.

Physical Security Controls

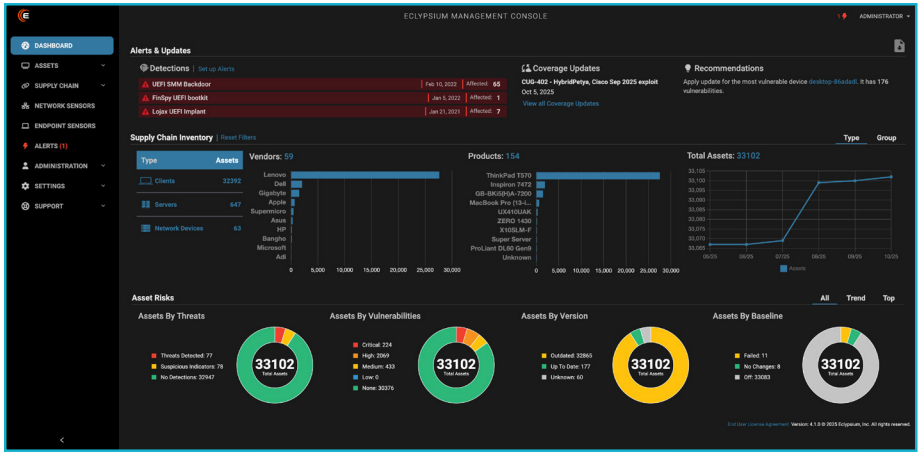
Secure physical access to critical infrastructure. Use locked cabinets, monitored data centers, and access controls to prevent unauthorized physical access to hardware. Consider tamper-evident seals for critical devices in distributed locations.

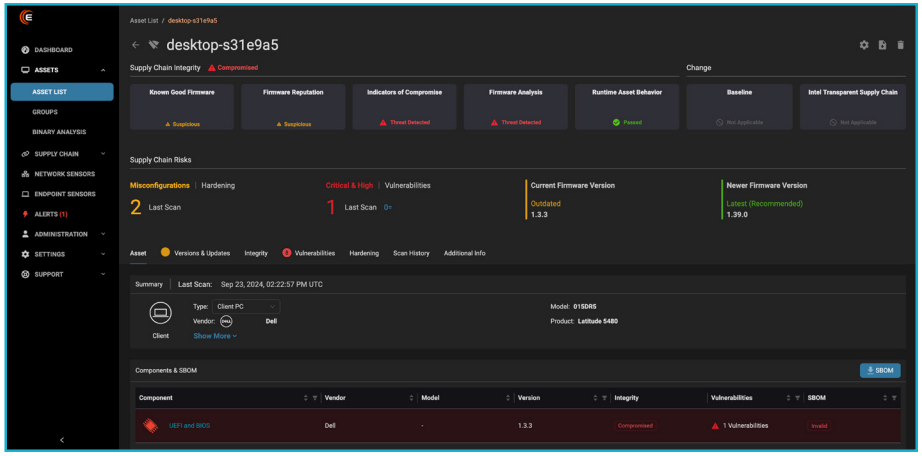
Implement change management procedures that require documentation and approval for any physical changes to infrastructure. This includes cable changes, component replacements, and device relocations.

Incident Response

Develop specific incident response procedures for suspected hardware compromises. These incidents often require different response actions than software-based attacks, including physical isolation of devices, forensic imaging of firmware, and potentially replacing entire hardware platforms.

Plan for extended recovery times when hardware integrity is questioned. Validating the security of an entire infrastructure may require significant time and resources.





Step 5: Build Your Hardware Security Program

Organizational Structure

Assign clear responsibility for hardware security across procurement, operations, and security teams. Procurement teams need training on security requirements and vendor assessment. Operations teams must understand configuration management and monitoring requirements. Security teams need expertise in hardware-specific threats and forensics.

Create cross-functional processes that bring together expertise from different teams. Hardware security requires coordination between groups that may not traditionally work closely together.

Policy and Procedures

Develop comprehensive policies covering hardware procurement, deployment, monitoring, and incident response. Policies should specify security requirements, assign responsibilities, and define escalation procedures.

Create detailed procedures that translate policy requirements into actionable steps. Include checklists, workflows, and decision trees that help staff implement security controls consistently.

Training and Awareness

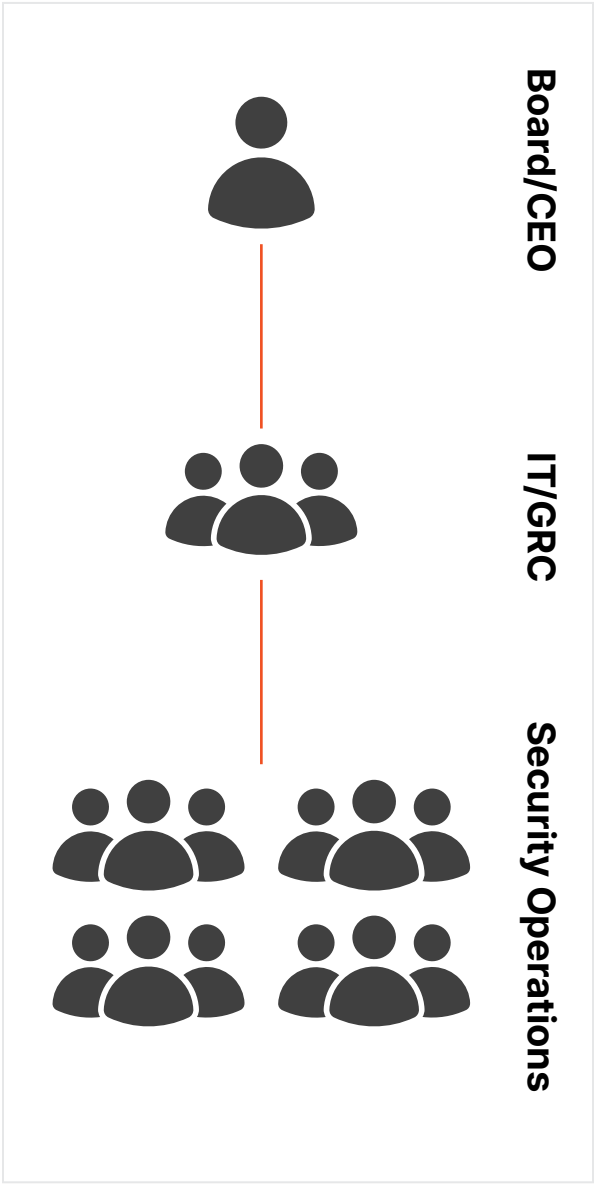
Provide targeted training for different roles in your organization. Procurement staff need awareness of supply chain threats and vendor assessment techniques. Technical staff need skills in hardware verification, monitoring, and incident response.

Maintain awareness of evolving threats through industry information sharing, vendor communications, and security research. Hardware threats evolve more slowly than software attacks but require ongoing attention.

Metrics and Measurement

Define metrics that demonstrate program effectiveness and identify areas for improvement. Track vendor security assessment scores, hardware verification compliance, configuration drift incidents, and response times for security issues.

Use metrics to communicate program value to leadership and justify continued investment in hardware security capabilities.



Step 6: Implementation Strategy

Phased Implementation Approach

Start with the most critical infrastructure and highest-risk components. Focus initial efforts on core banking systems, internet-facing devices, and infrastructure with administrative access. This approach provides immediate security improvements while building experience with new processes.

Phase 1: Establish vendor assessment processes and implement verification procedures for new hardware acquisitions.

Phase 2: Deploy monitoring capabilities for critical infrastructure and implement configuration management baselines.

Phase 3: Extend controls to all infrastructure categories and implement comprehensive incident response capabilities.

Quick Wins

Identify improvements that can be implemented immediately with existing resources. These early victories build momentum and demonstrate program value while more comprehensive controls are being developed.

Immediate Actions (Week 1-2):

- Add hardware security clauses to existing vendor contracts and RFP templates
- Create simple hardware inspection checklists for receiving staff
- Document current firmware versions across critical infrastructure using existing network scanning tools
- Establish secure storage areas for new hardware awaiting deployment
- Review and update physical access controls for network equipment locations

Short-term Improvements (Month 1-2):

- Assess existing monitoring tools for their ability to alert on firmware version changes and known and unknown firmware vulnerabilities.
- Implement tamper-evident seals on critical devices in remote locations
- Create hardware inventory spreadsheets with security-relevant details (vendor, model, firmware version, criticality)
- Establish direct shipping requirements for critical hardware purchases
- Train procurement staff on basic supply chain security risks during existing team meetings

Early Process Changes (Month 2-3):

- Require vendor security questionnaires as part of existing vendor onboarding
- Implement basic configuration backup procedures before any hardware maintenance
- Create simple incident response playbook for suspected hardware tampering
- Schedule regular firmware update reviews using existing change management meetings
- Establish hardware disposal procedures that ensure secure data destruction

Integration with Existing Programs

Align hardware security initiatives with existing cybersecurity frameworks and compliance requirements. Many organizations already have vendor management, configuration management, and incident response programs that can be extended to address hardware-specific risks.

Leverage existing tools and processes where possible to minimize additional overhead and complexity.

Budget and Resource Planning

Hardware security programs require investment in tools, training, and potentially additional staff. Justify investments by quantifying the risks of hardware compromise and the costs of incident response and recovery.

Consider both capital expenses for new tools and technologies, and operational expenses for additional processes and staff time.

Conclusion

Hardware supply chain security represents a critical but manageable risk for banking institutions. While the threats are serious and the potential impact significant, practical controls can substantially reduce risk and improve your security posture.

Success requires commitment from leadership, coordination across multiple teams, and investment in appropriate tools and training. The financial sector's increasing reliance on complex technology infrastructure makes hardware security not just advisable, but essential.

Organizations that proactively address hardware security will be better positioned to detect and respond to sophisticated attacks, maintain customer trust, and meet evolving regulatory requirements. The time to start is now, before hardware-level compromises become the next major threat to the financial services industry.

Start with an assessment of your current hardware security posture, identify the most critical gaps, and begin implementing controls for your highest-risk infrastructure. Building hardware security capabilities takes time, but every step forward reduces your exposure to this growing threat vector.

This guide provides general information about hardware security for banking institutions. Specific implementation should be tailored to your organization's risk tolerance, regulatory requirements, and technical environment.

CHECK LIST

Step 1: Assess Your Hardware Security Posture

- Infrastructure Inventory and Classification ☐
- Identifying Vulnerable Components ☐
- Current State Assessment ☐

Step 2: Secure Your Hardware Procurement Process

- Vendor Selection and Management ☐
- Supply Chain Security Requirements ☐
- Procurement Process Controls ☐

Step 3: Pre-Deployment Verification

- Hardware Integrity Verification ☐
- Baseline Configuration Management ☐
- Testing and Validation ☐

Step 4: Operational Security and Monitoring

- Continuous Monitoring ☐
- Physical Security Controls ☐
- Incident Response ☐

Step 5: Build Your Hardware Security Program

- Organizational Structure ☐
- Policy and Procedures ☐
- Training and Awareness ☐
- Metrics and Measurement ☐

Step 6: Implementation Strategy

- Phased Implementation Approach ☐
- Quick Wins ☐
- Integration with Existing Programs ☐
- Budget and Resource Planning ☐

info@eclypsium.com | eclypsium.com