



CUSTOMER SUCCESS STORY

SISA Helps Detect and Prevent
Unauthorized Communications in
POS Terminal Environment

ABOUT US

ABOUT THE CUSTOMER

The client is a leading provider of Point-of-Sale terminals used in financial transactions across the world. The company specializes in the retail sector and is the favoured POS provider for major acquiring institutions across the world. Headquartered in Shenzhen, China, the company is known for its innovation in the SmartPOS terminal industry and is the second largest payment terminal solutions provider worldwide. The client has a strong presence in various markets and also boasts a growing presence in India, Japan and Southeast Asia.

THE CHALLENGE

Point-of-Sale (POS) terminals are mission-critical endpoints in the payment ecosystem, processing sensitive financial data and interfacing with multiple cloud-based systems. In an era where advanced cyber threats target not just networks but the edge devices themselves, ensuring the integrity and behaviour of POS terminals has become a strategic imperative.

The client sought a deep-dive security assessment focused on a POS terminal, aiming to validate that the device communicated exclusively with trusted, authorized entities. The primary objective was to detect any anomalous or unauthorized network behaviour over a one-week observation window thereby ensuring no data exfiltration, command-and-control activity, or policy violations could occur unnoticed.

ADDING TO THE COMPLEXITY WAS A DIVERSE AND INTERCONNECTED POS ECOSYSTEM, COMPRISING:

**POS Terminal Management Platform:**

A cloud-based application management system used to deploy and monitor applications remotely. While central to operational efficiency, any misconfiguration in this platform could potentially expose terminals to external threats or non-compliant software behaviour.

**Remote Support Utility for POS Terminals:**

A remote access tool enabling real-time support and administration of POS terminals. Despite its benefits, insecure configurations of this tool could open pathways for unauthorized access or lateral movement within the network.

**Tencent Geo-Location Services:**

Integrated to track physical terminal locations, this service raised concerns around data privacy and network exposure. The client needed to assess whether transmitting geolocation data increased the attack surface or introduced latent vulnerabilities.

Against this backdrop, the client required a comprehensive behavioural and traffic analysis to proactively identify risks, validate secure configurations, and ensure the POS terminals were not silently communicating with unapproved destinations.

SOLUTION

SOLUTION OFFERED BY SISA

SISA adopted a forensic-led, phased approach to evaluate the security posture of the client's POS terminal, focusing on network behaviour, trust boundaries, and anomaly detection.



OUR ASSESSMENT WAS ANCHORED IN FOUR KEY PILLARS



Establishing a Baseline: Network Activity Under Controlled Conditions

To accurately assess deviations, SISA first monitored the POS terminal with no third-party service providers enabled. This step helped establish a clean baseline of expected network behaviour, packet volume, and communication endpoints—essential to identify anomalies during subsequent testing phases. client's wireless network infrastructure across locations.



Impact Assessment of Tencent Services: Behaviour with Geo-Location Enabled

With Tencent Geo-Location services activated, SISA observed the changes in network activity to assess if enabling location tracking introduced new communication endpoints, increased data transmission, or posed any privacy or security concerns. This comparison was critical in evaluating the trade-off between operational functionality and potential risk.



Trust Validation: Comparison Against Whitelisted IPs and Domains

All outbound and inbound communications were analysed against a predefined whitelist of trusted IP addresses and domains. This trust-based filtering ensured that the POS terminal was connecting only to known and authorized entities. Any deviation from this list signalled a potential breach of policy or compromise.



Anomaly Detection: Identification of Unauthorized or Suspicious Connections

SISA employed deep network traffic inspection to uncover unauthorized external connections, which could suggest malware callbacks, unauthorized remote access, or data exfiltration. These connections were flagged, categorized, and reported with contextual risk insights to guide remediation.

SISA RECOMMENDATIONS: IMPROVING POS TERMINAL NETWORK AND DEVICE SECURITY

A comprehensive security improvement plan was developed to address the identified vulnerabilities and enhance the overall security posture of the device.

01**Harden Remote Access Controls**

Verify whether the connection request is legitimate before approving it.

04**Limit External Communication Pathways**

Limit outbound communication strictly to whitelisted IPs or trusted entities.

02**Enforce Strong Authentication**

Implement multi-factor authentication (MFA) for all remote sessions.

05**Secure Data in Transit**

Limit outbound communication strictly to whitelisted IPs or trusted entities.

03**Monitor Remote Access Activity**

Regularly audit access logs to detect unauthorized use or anomalies.

BUSINESS IMPACT

By assessing the integrity of the network traffic of the POS machine, the client reinforced the operational resilience and market trust in their products. The assessment also supported regulatory and privacy compliance by ensuring communications were confined to trusted entities, thereby safeguarding sensitive data and minimizing risks associated with data breaches. Furthermore, proactive recommendations provided by SISA's team such as restricting remote access, enhancing encryption, and refining access controls directly translated into reduced vulnerabilities and a stronger security posture, which, in turn, boosted customer confidence and improved transparency in digital payment transactions.

While this analysis focused on a single device, the findings and remediation strategies directly translate into reduced vulnerabilities across similar deployments as well.

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective cybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

Compliance	Security Testing	Cyber Defense	Data Protection & Governance	Trainings & Certifications	Leading Tech Security
Payment Data Security • PCI DSS • PCI PIN • PCI 3DS • PCI P2PE • PCI S3 • PCI S-SLC • PCI CP (Card Production) • Facilitated PCI SAQ • Quarterly Health Check-ups • Central Bank Compliance • SWIFT Strategy and Risk • CCPA • GDPR • HIPAA • ISO • NIST • SOC 1 • SOC 2 • Cloud Security • HITRUST Unified Audits Managed Compliance	Application Security • Application Penetration Testing • CREST/CERT-in Approved Security Testing • API Security Testing • Secure Code Review Network Security • Vulnerability Assessment • Penetration Testing • Configuration Review • Firewall Rule Review • PCI ASV Scan Phishing Simulation Red Teaming Exercise • Layer Security Testing	Managed Extended Detection and Response Solution - SISA ProACT • 24x7 Monitoring • UEBA • Threat Intel • Advanced Threat Hunting • Breach & Attack Simulation • SOAR • Use-case Factory Digital Forensics and Incident Response • Incident Response / Compromise Assessment Services • Forensic Readiness Audit • Forensic and Incident Response Retainer Service • Payment Forensics Investigation • Internal Forensics Investigation • Ransomware Simulation	Data Discovery and Classification • PCI/PII/PHI Data Discovery • Data Classification in Endpoint (Windows, Linux) • Data Classification in O365, Metadata • Dynamic Masking, Redact, Truncation • Integration to DRM, DLP, SIEM Data Privacy Professional Services • Assessments (Unified Privacy Maturity, DPIA, 3rd Party Risk) • Data Inventory, Mapping and Process flow, RoPA • Data Privacy Framework - Policy, Notice, SoPs • Consent and Notice Management framework • Data Breach and Management • Principal management • Privacy by Design implementation guide • Define Data Retention Guidelines and processes • Technical/Organization measures • Privacy Training/Awareness	Payment Data Security Training and ANSI Accredited Certification • CPISI (2 Day Program) • CPISI (3 Day Program) • CPISI- Advanced (3 Day Program) • CPISI-D (Developers) • CPISI Hybrid (4 Weeks) Certification Program in Cybersecurity for AI – CSPAI • CSPAI • CSPAI - Developers Forensic Briefing Sessions for Senior Management	AI PRISM • AI PRISM LLM Vulnerability Scanner Solution • AI Risk Management and Governance Solution Framework • AI Compliance and Governance Consulting Service Hardware and IoT Security Testing • Firmware Security Testing • Hardware/Embedded Security Testing • IoT Network Security Testing • IoT/Embedded Application and Management Layer Security Testing • MPOC/ PCI PTS Quantum Security • Quantum Cryptographic Consulting • Quantum Security Risk Assessment • Quantum Security Standards Compliance

For more Information visit us at www.sisainfosec.com
or
write to us at contact@sisainfosec.com

Follow us

