



Information Security Risk and Compliance

Dedicated to continually enhancing
security at every level



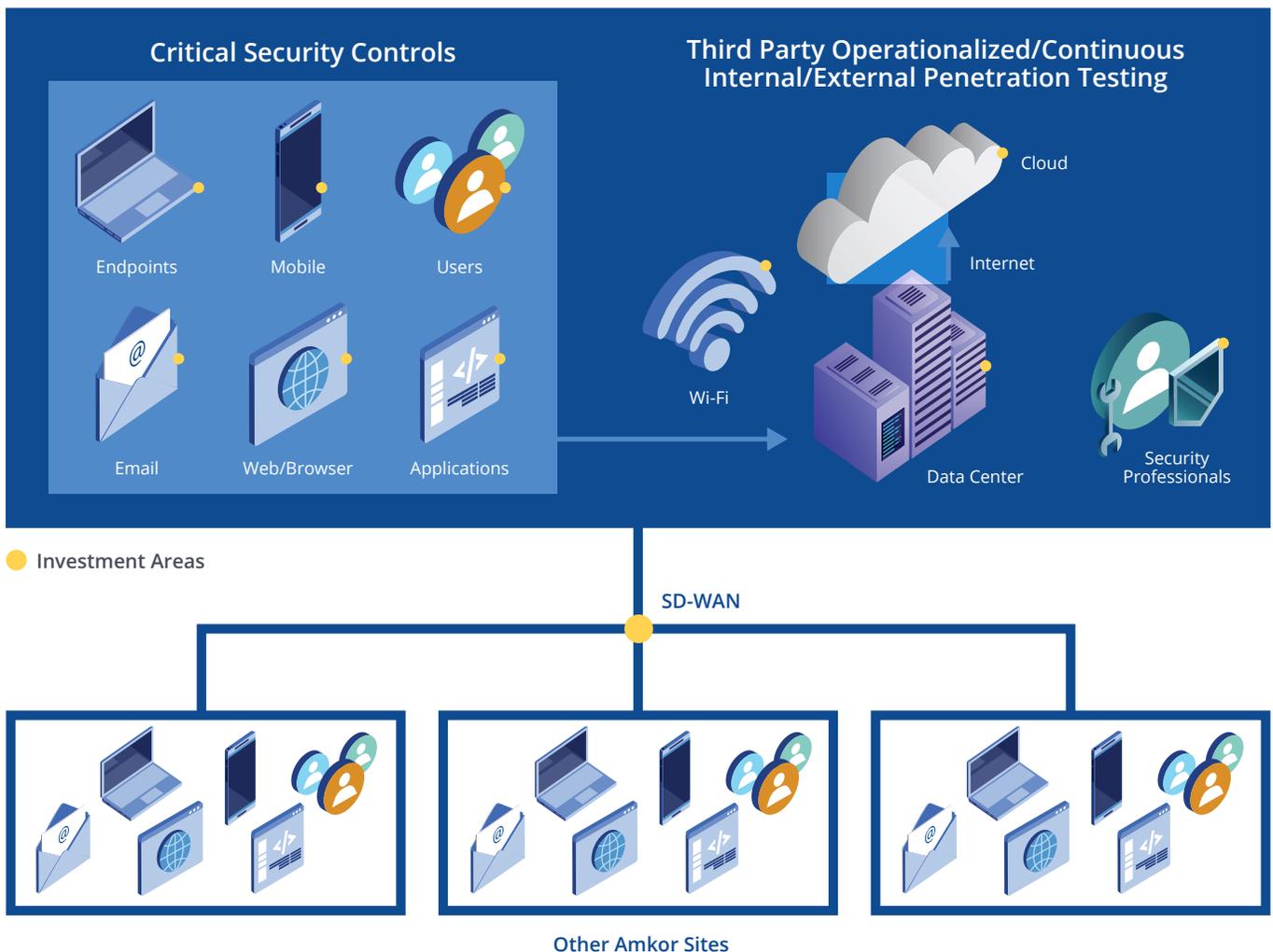
Protecting Your IP

Protecting your intellectual property is as important to us as it is to you. Amkor has invested in a focused cybersecurity team with a mission to continually monitor and improve our overall security and that of our customer data and interfacing systems.

Amkor has adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) globally.

We utilize a risk-based defense in depth approach to prioritize, address and manage cyber security risk from end user devices to global networks, data centers, operational technology and our supply chain. Amkor takes cyber defense seriously. Existing substantial and continuous investment will further strengthen Amkor's global cybersecurity posture.

Amkor Security Investments



Notes

1. Some variations may exist among different locations and not all services are replicated at all sites.
2. Amkor continues to invest heavily in security with a risk-based defense in depth strategy.
3. Relevant sections of the security roadmap can be shared in a face-to-face meeting.

Strengthening Cybersecurity

Amkor Technology provides an extensive range of information security capabilities to all members of the Amkor global community.



Infrastructure Protection

Physical Security

- ▶ CCTV: 24/7/365 monitored areas
- ▶ 24/7 Security hotline
- ▶ Badge and RFID controls to all gates, turnstiles and doors
- ▶ Metal detectors and physical pat-downs

Key Infrastructure Protection

- ▶ Privileged Access Management (PAM) for all admin accounts
- ▶ Firewall IPS/IDS for ingress/egress points
- ▶ Global SIEM with threat intelligence enrichment
- ▶ Vulnerability management and patching program

Perimeter Security

- ▶ Monitored and controlled DMZ
- ▶ Managed SFTP
- ▶ URL filtering/cloud detonation/DNS sinkhole

Network Infrastructure

- ▶ Software-Defined Wide Area Network (SD-WAN)
- ▶ Wireless LAN access controls
- ▶ Network segmentation zones/VLANs/ACLs
- ▶ Multifactor always-on VPN

Data Centers

- ▶ Controlled and monitored physical access
- ▶ CCTV: 24/7/365 monitored areas
- ▶ Firewall separation of data centers



Dedicated Information Security Team

Security Organization

- ▶ Global information security team led by CISO
- ▶ Dedicated patch and operational technology teams
- ▶ Global security program based on the NIST CSF
- ▶ Global information security policies and procedures
- ▶ Designated information security leader and incident response team at each site
- ▶ Continued investment in enhancing cybersecurity
- ▶ Global 24/7/365 security operations center

Regulatory Compliance

- ▶ Sarbanes Oxley/ITAR/ITGC

Customer Compliance

- ▶ Customer-driven security audits
- ▶ Periodic security assessments

Awards

- ▶ CS050 2016 and 2017 IDG Award



End User Protection

Application Controls

- ▶ Quarterly account and access reviews
- ▶ Single Sign-On (SSO) with Multifactor Authentication (MFA)
- ▶ Role-Based Access Control (RBAC)

End User Devices (Desktops, Laptops, Tablets)

- ▶ Next-gen antivirus and malware protection clients
- ▶ Laptop whole disk encryption
- ▶ Mobile device management
- ▶ DRM for critical apps and data
- ▶ Local administrator password solution

Email (O365) and Anti-Phishing

- ▶ DomainKeys Identified Mail (DKIM)
- ▶ Data Loss Prevention (DLP) light
- ▶ Security gateway with advanced threat protection

End Users/Operators

- ▶ Mandatory cybersecurity awareness training
- ▶ Global directory
- ▶ Tone at the top cybersecurity culture
- ▶ RFID badge integration
- ▶ User Behavior Analytics (UBA)
- ▶ OS and AD hardened configurations
- ▶ Monthly phishing campaigns with automated re-training
- ▶ Cyber awareness campaigns



Cyber Resiliency

Continuous Improvement

- ▶ Continuous third party penetration testing
- ▶ Biannual incident response tabletop exercises
- ▶ Collective Risk Model (CRM) framework
- ▶ BC-DR-IR harmonization
- ▶ Supply chain managed third party security reviews



Add-On Services

Customized Security Services for Additional Fees

- ▶ Access controlled and encrypted repositories
- ▶ DRM for critical documents
- ▶ Network-isolated server rooms
- ▶ Dedicated circuits
- ▶ Dedicated firewalls
- ▶ Dedicated servers
- ▶ Dedicated SFTP server
- ▶ Remote access with critical security controls
- ▶ Customer-specific partitioning on some systems

Amkor Cybersecurity

by the Numbers

GLOBAL
CRITICAL SECURITY CONTROLS



24/7/365 SECURITY OPERATIONS CENTER



37 INFORMATION SECURITY PROFESSIONALS

- amkor.com
- the industry

CERTIFICATIONS



GSMA Security Accreditation Scheme

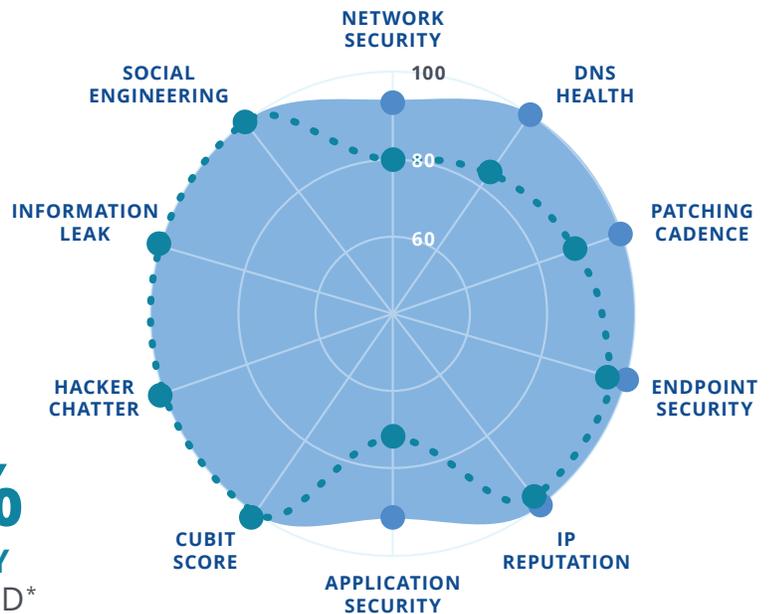


VIEW FULL LIST AT

<https://amkor.com/quality-management/#certifications>



97%
SECURITY SCORECARD*



TIMELINE

- 2016**
 - ▶ Center for Internet Security Critical Security Controls
 - ▶ Third Party Continuous Global Penetration Testing
 - ▶ Common Criteria for Information technology Security (ISO/IEC 15408 Certification)
- 2021**
 - ▶ Third Party Cybersecurity Maturity Assessment
 - ▶ National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- 2022**
 - ▶ Global System for Mobile Communications Association (GSMA Certification)
 - ▶ Common Criteria for Information Technology Security (ISO/IEC 15408 Certification)
- 2023**
 - ▶ Cyber Risk Management Framework
 - ▶ Operational Technology Controls
 - ▶ Zero Trust Network Architecture
 - ▶ Expanded IT General Controls
- 2024**
 - ▶ Third Party NIST CSF Audit
- 2025**
 - ▶ ISO/IEC 27001 Certification



71
SUCCESSFUL CUSTOMER AUDITS[†]

[†]2022 RESULTS



Visit amkor.com or email sales@amkor.com for more information.

With respect to the information in this document, Amkor makes no guarantee or warranty of its accuracy or that the use of such information will not infringe upon the intellectual rights of third parties. Amkor shall not be responsible for any loss or damage of whatever nature resulting from the use of, or reliance upon it and no patent or other license is implied hereby. This document does not in any way extend or modify Amkor's warranty on any product beyond that set forth in its standard terms and conditions of sale. Amkor reserves the right to make changes in its product and specifications at any time and without notice. The Amkor name and logo are registered trademarks of Amkor Technology, Inc. All other trademarks mentioned are property of their respective companies. © 2023 Amkor Technology, Incorporated. All Rights Reserved. BRIT102E-EN Rev Date: 07/23

