Security & Solutions Architectures

At Mantis Security, information security practices are pervasive throughout the systems development lifecycle. Security architecture begins with project initiation and asset classification, and matures in lockstep with System and Solutions Architectures, and as features are implemented to produce a well-reasoned and flexible information security foundation. Our security and solutions architectures are grounded in the latest risk management practices and security controls, and are tailored to the data integrity, availability, and confidentiality needs of each information system.

Our Security Architects and Solutions Architects are passionate about secure system design, cloud and network security, access control, data privacy, data integrity, high availability, and vulnerability and risk analysis. We work with data owners, information system owners (ISOs), security managers and engineers, and system architects to provide a special focus on information security and asset protection.

Our team specializes in systems and software architects that are comprised of security controls that are tailored towards the risk of data loss or compromise of each information system, and in each IT ecosystem (cloud, virtualized, or physical IT assets). We provide subject matter expertise in cloud readiness assessments and cloud migration roadmaps for major vendors such as Amazon Web Services (AWS) -- including federal regions such as AWS GovCloud and AWS C2S. Our certified cloud solutions architects are trained in the latest cloud security and architectural offerings to assist in the design and development of robust and secure information systems.

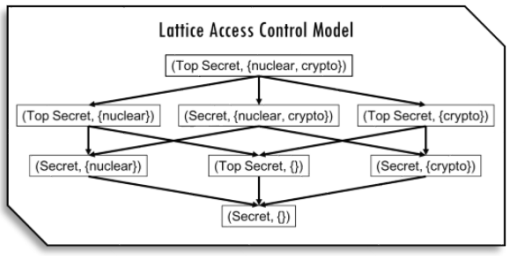
From sensitive compartmented data systems that require layered physical and technical security controls and custom security administrative procedures, to high assurance cryptographic transmission protection, to insider threat mitigation, to digital rights management, to data security. We have the deep security expertise to complement your IT solutions and development teams.

We work closely with your entire security team, data owners, ISOs, and security assessors to interpret IA Policy and provide security requirements and security architectures that protect your vital mission assets.

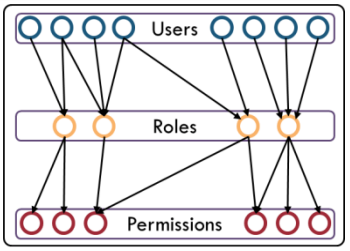
Security & Solutions Architecture Expertise

- FISMA, NIST, and Agency-specific security controls
- Security architecture assessments
- Cloud and network enclave security
- Security labeling and data access control solutions
- Encryption of data at rest, in transit, and at runtime
- PKI and private key management
- Multi-level Systems (MLS)
- Amazon Web Services (AWS) security and solutions architectures
- Network cryptographic protections
- IT and Security Strategy Alignment
- Architectural frameworks (DoDAF, TOGAF, ISO 42010)

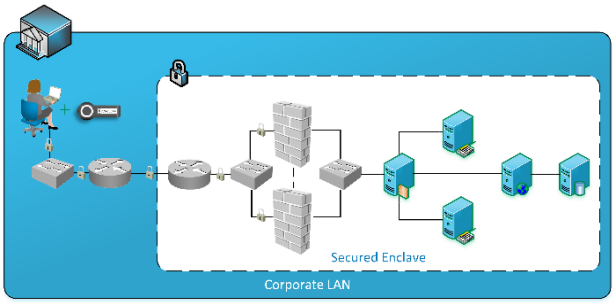
Consulting



Our Security Solutions Architects are practiced system architects with a wide range of deep security expertise and training. We excel in applied access control models ranging from DoD/IC tailored models (Lattice and Mandatory Access Control (MAC)), to common industry models (Discretionary Access Control (DAC) and Role Based Access Control (RBAC)), to dynamic models such as Attribute Based Access Control (ABAC).



Our security architectures are based on our knowledge of the latest cryptographic algorithm suites that meet FIPS 140-2 and NIST 800-52 encryption requirements. We are knowledgeable of asymmetric cryptography, including expertise implementing Public Key Infrastructure (PKI) authentication, PKI certificate management, and network security practices including firewalls, VPNs, load balancers, network encryptors (such HAIPEs), reverse proxies, and hardware security modules (HSM), and key management. Our Information Assurance (IA) engineers are knowledgeable of Security Information and Event Management (SIEM) software, and work with system and data owners to provide active system monitoring, reporting, and metrics.



Our security architects have designed secure enclaves with physical and network isolation, as well as cloud/physical hybrid systems that provide a best in breed of data availability and security. We have designed information system architectures that operate across domains, as well as multi-level systems (MLS) that operate with varying user authorizations on a single domain. Mantis Security further supports customer security and IT strategy, including IA policy alignment, cybersecurity and auditing, cloud and virtualization, and COTS consolidation (open source adoption)--all with a mindset towards security.

Security Solutions

Cloud and Network Enclave Security Architectures

- Multi-factor Authentication (MFA)
- VPNs and Network/HAIPE Encryptors
- High Availability, Integrity, and Confidentiality Architectures
- Cloud, On-Premise, Data Center, and Hybrid Solutions
- Hardware Security Modules (HSMs) and Key Management
- Firewalls and Information Flow Protection
- Security Information and Event Management (SIEMs) solutions

Systems and Software Security Architectures

- Secure web services and REST services
- User management and access control
- Secure session management
- Secure web development
- Application and data access control (ABAC, DAC, RBAC, MAC)
- Single-sign On
- PKI authentication
- FIPS 140-2 and NIST 800-52 cryptographic requirements
- Reverse proxies, traffic managers, and load balancers