servicenow

QUICK REFERENCE GUIDE

Security Architecture

Security architecture translates business requirements into executable security requirements. A security mindset is beneficial to address security risks in the platform. Use threat modeling, a risk-based approach designing security systems, to provide stakeholders with a systematic method to identify potential threats and develop mitigations to them.

Practice the threat modeling process and ask the following two questions:

1. What might go wrong?
2. What can we do to prevent this?

Three layers of security used in platform security architecture

Security layers	Description
Network layer	This first layer of the application architecture includes network routers, switches, load balancers, firewalls, and intrusion detection systems. Consider the following security controls in the network layer, • Edge encryption • IP address access control
Application layer	In the second layer, application servers are in a discrete network segment. Consider the components when looking at the application layer security architecture. • Pre logon (adaptive authentication) • Authentication (SSO, multifactor, social logon) • Authorization (roles, encryption) • Instance settings • Platform encryption • IP address access control
Database layer	In the third layer, database servers are installed in a discrete, non-internet routable network segment. Database encryption: • Helps to encrypt ALL stored data • Is transparent to the application and its users • Protects the entire database

Encryption similarities and differences

	Database Encryption	Platform Encryption	Edge Encryption
Description	Encryption of data at rest when not being processed in the instance	Equality preserving encryption of data at rest within the database based on user role in the instance	• Standard, equality preserving, and order preserving encryption of data at rest within the database and instance • Data sent from the organization to ServiceNow is already encrypted
Field types supported for encryption	All	• String text • Date • Date/Time • Attachments • URL	• String text • Date • Date/Time • Attachments • URL • Journal
Encryption types	AES-256	AES-128 and AES-256	AES-128 and AES-256
Tokenization	No	No	Yes, for pattern-matched data
Encryption key management	Managed by ServiceNow	Managed by ServiceNow and the customer	Managed by the customer
Other requirements	None	None	• On-premises encryption proxy • Encryption key store • Optional on-premises MySQL database for tokenization and order preserving encryption