Technical Paper

Plain talk about Infor CloudSuite security

Infor CloudSuite

When it comes to Cloud deployment, security is top of mind for all concerned. The Infor® CloudSuite team uses best-practice protocols and a thorough, continuous improvement approach that gives you both confidence and peace of mind. The following information provides a detailed look at Infor's security approach.

Defense-in-depth

Infor CloudSuite does not rely on any single security device, technique, or practice for data assurance. Instead, Infor CloudSuite employs a "defense-in-depth" strategy to implement multiple layers of overlapping security that safeguard your data through each link of the chain and ensure a high level of solution availability.
These security controls are enforced by a team of specialists who are constantly monitoring and improving our security posture to stay ahead of threats.

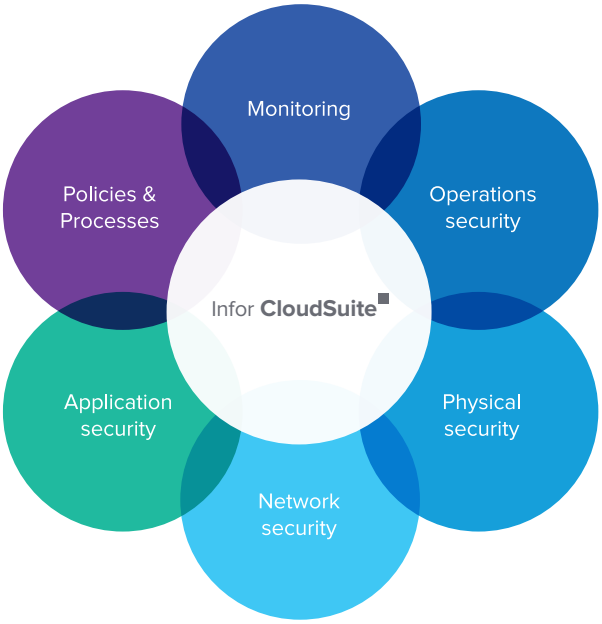

Figure 1—Infor CloudSuite security: Defense-in-depth

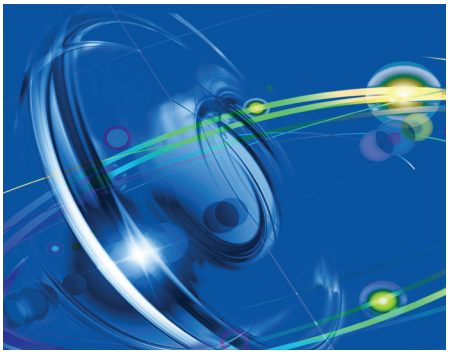

Table of Contents

Application security

Infor developers place a strong emphasis on security throughout the software development life cycle. Through a combination of self-study and regular security training sessions provided by the development staff, they are constantly kept up to date on developments in this critical area and reminded of security policies that must be followed. To ensure security is built into Infor's applications from the start, security requirements for each product are defined and then architected into the software design. Code reviews allow product teams to share secure coding practices they have gathered through own research or past implementations, while a focus on the Top 10 Open Web Application Security Project ensures that the most prevalent threats are being acknowledged and mitigated. Periodic vulnerability and penetration testing is also performed to identify potential problem areas, allowing developers to get a first-hand view of how poor coding practices can negatively impact applications when they are released. Vulnerabilities identified are then added to testing processes to prevent their reappearance in the future.

Network security

Security through separation

Infor CloudSuite's networks are independent, meaning they are separated from the general Infor corporate network. This separation gives our network engineers the freedom to design a solution that meets your performance, availability, and security needs.

Layered defense architecture

Infor CloudSuite's emphasis on security has resulted in an architecture that has multiple layers. These layers are built to protect against both very specific attacks (e.g., DDoS) and more general information gathering attacks (e.g., vulnerability scanning). The implemented mechanisms have the ability to proactively defend against an attack, while also providing real-time monitoring of current threats from the Internet. Firewalls allow for grouping of networks into segments and isolation of critical components to prevent access from an external network. They also work in concert with load balancers that spread traffic across numerous servers to ensure high availability and provide the best possible performance.

Wired and purposeful—never wireless

At no point is traffic within the Infor CloudSuite network broadcast from an antenna or wireless transmitter that would expose it to interception by third parties equipped for wireless snooping, now a sophisticated and accessible field. All remote access requires a virtual private network with two-factor authentication.

Secure environment in an insecure world

The Infor CloudSuite system had to be designed to maintain network security even when serving clients who don't use best security practices. For example, Infor CloudSuite would need to be protected from a user with a compromised system not running the latest anti-virus protection. The solution's designers, therefore, implemented rigid protocols that enforce security within Infor CloudSuite devices to provide reasonable assurance that the network remains secure.

Physical security

Physical security of Infor CloudSuite's IT infrastructure

Physical security is paramount and pervasive throughout the implementation of Infor CloudSuite however, it is most easily identified around our best-in-class data centers. These biometric-protected data centers house the solution's network and IT infrastructure. To safeguard the Infor CloudSuite, our data center observes specific best practices, including guard-controlled access with man-trap technology, registered guest restrictions, locked cage spaces, closed-circuit television monitoring, and additional systems for physical intrusion monitoring, detection, and alerting.

Operations security

Infor recognizes that good security cannot depend on application and network controls alone. Security must be maintained at the IT operational and infrastructure level.

IT infrastructure security

Deploying and managing IT infrastructure is one of our fundamental strengths. Infor CloudSuite's strategic IT services are built, maintained, and administered in compliance with the security standards required for global data centers.

Some of our mandatory security requirements include restricted access (logical and physical), administration of limited user-account permissions, hardening and managed patching of operating systems, separation of server duties, monitoring and automated logging of security events, and the ongoing management of backups.

In addition, technical elements of Infor CloudSuite security are supported by operational practices. Our Operations department is where purposeful design and careful configuration of technologies meet the people, procedures, and practices that make up a secure end-to-end solution. Infor CloudSuite's security ethic has been carried over into the structure of its operations, where specific teams have prescribed roles and responsibilities. Access to critical Infor CloudSuite systems is structured to ensure separation of duties and administered under the principle of least privilege. Staff members are given no more access—no more privilege—than they require to complete their duties, and individuals with access to customer data are required to pass background checks. Customers also have no access to Infor CloudSuite's supporting operating systems or lower-level functions. In fact, the only access provided is to their portal, where all requests are handled and sent to back-end databases protected within different network segments.

Strict data transmission protocols

The architecture of the Infor CloudSuite software allows Infor to leverage the concept of defense-in depth-security by using technologies such as SSL/TLS and transaction-based business logic.

Encryption and privacy

Encryption is used extensively within the Infor CloudSuite environment to ensure that data is protected. While in-transit, data is encrypted using appropriate mechanisms that include TLS/SSL, PGP, and secure FTP. When required, data-at-rest is encrypted using database, file system, or other appropriate encryption capabilities.

Staff dedicated to personal service and security

Infor CloudSuite's staff is not part of Infor's larger IT organization, and they do not have general IT responsibilities. These individuals are dedicated to Infor CloudSuite. This promotes ownership, visibility, and direct accountability within the organization.

During Infor CloudSuite sessions and at all other times, 24/7, the staff works actively behind the scenes, monitoring network characteristics but not observing customer data. If customers require more active collaboration to address issues or concerns, our staff is readily available and easily engaged.

Infor and the Infor CloudSuite team are absolutely committed to protecting the privacy of customer data. Therefore, specific security/privacy policies, procedures, and technical controls are applied to our operations to ensure we provide unparalleled support without infringing on confidentiality.

Monitoring

Dynamic password management

Passwords are a fundamental tool for authentication and authorization. Infor CloudSuite maintains centrally managed passwords to protect administrative access points to the Infor CloudSuite network, applications, and IT infrastructure. Periodically changing passwords reduces the time available to discover passwords by observation or repeated trial-and-error. It also suppresses the risk of access via misappropriated passwords. To defeat password cracking by brute force, the system registers unsuccessful password attempts and patterns, alerting network management staff to investigate.

Management of digital certificates

Every secure session with a web server has an important aspect—the ability to authenticate the server. Certificates are the foundation of a secure cloud implementation, where each primary element of the Infor CloudSuite solution presents a verifiable identity. By providing robust identity to critical Infor CloudSuite hardware, certificates ensure that Infor CloudSuite sessions occur with only authenticated Infor CloudSuite systems.

Managed configurations

Configuration is about choices. When Infor CloudSuite's network and systems architects design and configure our systems, they make choices that promote and enable security. Furthermore, Infor CloudSuite observes formal configuration and change management practices, controlling the evolution of Infor CloudSuite via enforced and audited processes.

Data ownership

Within Infor, customers own their data, and it is accessible at all times. Customers can also have all data returned at the end of the engagement.

Logging, monitoring, auditing, and incident response

The logging and monitoring of security incidents is essential to ensuring that a solution has not been compromised and is being protected from misuse. Infor CloudSuite's staff monitors the network using a set of tools, specifically configured for this solution, to effectively manage logs and alerts. Infor collaborates with customers to investigate attempts at intrusion, whether accidental or purposeful.

Customer data not captured by monitoring processes

The only network details collected by our logging and auditing systems are application, system, and network logs and metadata. Our policy is to not collect log information that contains actual customer data. We purposefully limit the information we collect to ensure data privacy to the greatest extent possible, while maintaining our ability to track critical activities.

Security event recognition

Infor CloudSuite security encompasses monitoring, characterizing, reporting, and handling of security incidents, including technical escalation and customer notification paths. This information is captured and analyzed by our Intrusion Protection Engine, which generates alerts when an intrusion is attempted. These alerts are then handled by our security and network teams to determine the appropriate actions.

Policies and procedures

Infor CloudSuite has implemented a comprehensive security policy that focuses on the ISO 27001 best practice standard to provide the guiding principles for our focus on confidentiality, integrity, and availability. Our employees are trained on their responsibility to follow these policies and to alert appropriate personnel when these principles are not being followed. Procedures are written based upon these policies.

ISO-27001 compliance

The ISO-27001 standard is an internationally recognized credential of a securely designed and soundly run information security management system. We are fully committed to complying with this standard and will be pursuing certification in our SaaS environment. This best-in-class certification will require an audit consisting of an extensive analysis and reporting of all domains of security described in the companion document, the ISO-27002 standard. (For details see http://www.iso.org.)

SSAE 16 assessments

The Infor CloudSuite's Data Centers undergo SSAE 16 SOC 1 Type II assessments to provide an independent auditor's assessment of the controls and adequacy of the identified controls in meeting their objectives.

Regulatory compliance

Whenever an application deals with data that requires regulatory compliance (e.g., HIPAA, SOX, PCI, GLBA, regional privacy laws, etc.), Infor CloudSuite works with customers to ensure that the controls needed to meet those requirements are in place. Infor is always ready to support customers in addressing auditors' questions about how we securely manage our environment.

Security, delivered

Recognizing the needs of our customers across the pharmaceuticals, financial services, manufacturing, and other information-critical industries, Infor has put the technologies and practices of security assurance in place across the breadth of the Infor CloudSuite solution.

For more information, please visit: www.infor.com/solutions/ion-technology/cloud/.

641 Avenue of the Americas
New York, NY 10011
800-260-2640
infor.com

About Infor

Infor is fundamentally changing the way information is published and consumed in the enterprise, helping 70,000 customers in 194 countries improve operations, drive growth, and quickly adapt to changes in business demands. To learn more about Infor, please visit www.infor.com.

Disclaimer

This document reflects the direction Infor may take with regard to the specific product(s) described in this document, all of which is subject to change by Infor in its sole discretion, with or without notice to you. This document is not a commitment to you in any way and you should not rely on this document or any of its content in making any decision. Infor is not committing to develop or deliver any specified enhancement, upgrade, product or functionality, even if such is described in this document.

INFDTP1406060-EN-US-1213-2