

Cloud Security

Trust Cisco to Protect Your Data

As cloud adoption accelerates, organizations are increasingly placing their trust in third-party cloud service providers (CSPs). But can you fully trust your most sensitive data to cloud providers? And how can you be assured that they will deliver the security and data protection you need?

CSPs can earn this trust by demonstrating that they comply with the most robust security and data protection policies and procedures. These policies need to support a coordinated, tightly integrated combination of internal policy compliance, regulatory compliance, external auditing, and governance.

The Cisco® public Intercloud-based services platform, Cisco Intercloud Services, offered in conjunction with our partners, is an example of our commitment to cloud security and data protection. To keep data in the cloud secure, we and our partners adhere to a rigorous,

industry-competitive set of security and data protection standards. This white paper outlines the specific security and data protection measures in place for CIS infrastructure and operations.

Our dedication to security isn't just limited to public Intercloud-based services; it's fundamental to the entire [Journey to the Intercloud](#). Security is integral to each step in this journey. Beginning with strategy development and extending to private cloud deployment, "as-a-service" offerings, and reaching to the hybrid cloud, you can trust CIS with your most sensitive data.

At Cisco, our commitment to cloud security is based on these principles:

SIMPLICITY AND TRANSPARENCY

CIS offers a common, unified set of controls based on multiple standards and frameworks that enhance your visibility into the cloud. They support continuous improvement by identifying, assessing, measuring, and mitigating risk.

SECURITY AND COMPLIANCE

CIS provides independently audited and certified technical, operational, facility, and personnel controls, safeguards, and procedures. You can be confident that your applications and data are in a highly secure and compliant environment.

SHARED RESPONSIBILITY

CIS offers a degree of control at the individual service level that meets or exceeds most customers' requirements. By collaborating and sharing responsibility, we can help you reduce risk, cost, and quality issues.

Cisco as a Trusted Security Partner

Cisco offers a level of threat research and intelligence beyond that available to most CSPs.

Our security ecosystem, the Cisco Collective Security Intelligence, collects threat intelligence from across the organization. Our Talos Security Intelligence and Research Group, and our Security and Trust, Managed Threat Defense, and Security Operations teams deliver security protection and managed security services that protect our customers from known and emerging threats.

By aggregating and analyzing telemetry data across our ecosystem, we create a security intelligence cloud that we call “big intelligence.” Our reputation analysis service tracks threats across networks, endpoints, mobile devices, virtual systems, web, and email. With this data, we gain a holistic understanding of threats, their root causes, and the scope of outbreaks. All this information helps increase the effectiveness of our security solutions.

For example, the Cisco Security Incident Response Service combines the latest intelligence with best security practices to engage all layers of defense. It helps organizations prepare, manage, respond, and recover from incidents quickly and effectively.

Working directly with the Collective Security Intelligence group, the Incident Response team identifies known and unknown threats and quantifies and prioritizes risk to reduce risk in the future. The service uses leading monitoring systems and diagnostic procedures to quickly resolve events that affect business operations.

In addition to our cloud security service teams, Cisco’s network **security products, software, services and solutions** provide highly secure firewall, web, and email services while helping protect mobile and teleworking environments.



THESE SECURITY OFFERINGS INCLUDE:

- Cisco Advanced Malware Protection (AMP)
- Next Generation Network Security
- Secure Access and Mobility
- Secure Data Center
- Robust native security capabilities of Cisco Nexus, ASR, and UCS products
- Content Security
- Managed Threat Defense Service

Cisco designs, operates, and maintains our products and services to defend against security risks regardless of their origin. We don’t engineer undocumented features or functions, and we are committed to a policy of secure engineering throughout the development lifecycle. Our products undergo rigorous testing by employees, customers, third-party labs, and some of the best engineers in the world.

Securing Your Data in the Cloud

For strong security in our Intercloud-based services, we use leading capabilities, approaches, methods, and tools. Our organization wide information security management system (ISMS) operates in accordance with the ISO (International Organization for Standardization) 27001:2013 security standard and SOC (Service Organization Control) trust criteria principles and practices (Table 1).

The CIS approach to security is wide and deep, spanning physical, logical, and virtual environments throughout our cloud facilities. It encompasses computing, storage, network, operations, personnel, and tools.

Table 1. Cisco Cloud Services Information Security Management System

Component	Description
Information security policies	Management direction for, and organization of, information security, including roles and responsibilities, segregation of duties, and contacts with authorities and special interest groups
Human resources security	Screening, background checks, disciplinary actions, and security awareness and training
Asset management	Asset inventory, acceptable use, and information classification
Access controls	Access policy, access authorization, network access, user responsibilities, and application and systems access
Cryptography	Cryptographic-controls policy and key management
Physical and environmental security	Securing physical access to facilities, protection of equipment, and protection against external and environmental threats
Operations security	Operational policy, procedures, and responsibility, change management, capacity management, protection from malware, data recovery, logging and monitoring, control of operational software, technical vulnerability management, and audit controls.
Communications security	Network security management and information transfer
System acquisition, development and maintenance	Security requirements, development requirements, and test data
Supplier relationships	Policies and monitoring
Information security incident management	Response process and reporting
Information security aspects of business continuity management	Planning and data recovery
Compliance	Legal and contractual requirements, intellectual property, protection of records, and information-security reviews

We also put measures in place to protect customer data against accidental or unlawful loss, destruction or alteration, and unauthorized disclosure or access. They include policies, procedures, and internal controls for Intercloud-based services personnel, equipment and processes, and for the facilities where we deliver our services. We also enforce similar measures with our vendors and subcontractors.

For customers using our Cisco Intercloud-based services, we provide the location of the Cisco data centers that deliver services.

Protecting Personal Data and Privacy in the Cloud

Privacy is a top priority for Cisco. We comply with the privacy and data protection laws that apply to our cloud services delivery wherever we do business. We are aware of the legal obligations we must meet in the jurisdictions where we operate, and we address them through a common control framework that is the basis for our global privacy policies.

One of the most important considerations in privacy and data protection is defining and understanding the different types of data that may be migrated, processed, or stored in the cloud.

THIS DATA INCLUDES:

- Personally Identifiable Information (or “personal data”) defined by applicable laws
- Sensitive business information as defined by applicable laws or considered sensitive by our customers
- Data that is subject to data-residency restrictions by law
- Sensitive data that is subject to data-residency restrictions by customer requirements
- Telemetry data
- Geolocation data

Cisco works with you to understand how your data flows and to clearly identify the different types of data in the cloud, including customer data, Cisco data, and third-party data.

Cisco is constantly improving its strategy to enhance its privacy and data protection efforts, in light of evolving customer requirements but due to also a rapidly changing regulatory landscape.

Cisco safeguards and enables the transfer of personal information in a number of different ways, including adherence to European data privacy principles with respect to the collection and use of personal data from European Union member countries and Switzerland, unambiguous consent of individual data owners, and necessary performance of contracts and the standard contractual clauses or EU Model Clauses established by the European Commission under Article 26(4) of the EU Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995). Cisco is actively and closely monitoring any further regulatory developments in this area.

Please see our privacy statement at http://www.cisco.com/web/siteassets/legal/privacy_full.html for the latest updates and information.

Supporting Data Residency and Data Sovereignty in the Intercloud

Data residency and data sovereignty are just as important as privacy and security for many enterprises that are considering moving their workloads to the cloud. And many governments consider their citizens’ data privacy to be of paramount importance. Some have passed or are considering legislation that would require data, including backup data sets, to be physically located within their country.

¹Recommended contractual clauses established by the European Commission on the basis of Article 26(4) of the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 (the ‘EU Data Protection Directive’).

Cisco supports data-residency and data-sovereignty needs through a variety of options to create an efficient and cost-effective hybrid cloud. This is a key differentiator of Cisco's Intercloud strategy.

THEY INCLUDE:

- A**

Building the infrastructure to privately host your most critical data

B

Offering our Intercloud infrastructure data centers located around the world

C

Working with a local Cisco partner that has local infrastructure, local compliance, and local people.

In private or hybrid clouds, highly sensitive information should be managed by you and stored behind your firewall. Whether you use a data center owned by Cisco or a Cisco partner, we strongly encourage you to encrypt your data before sending it to any cloud.

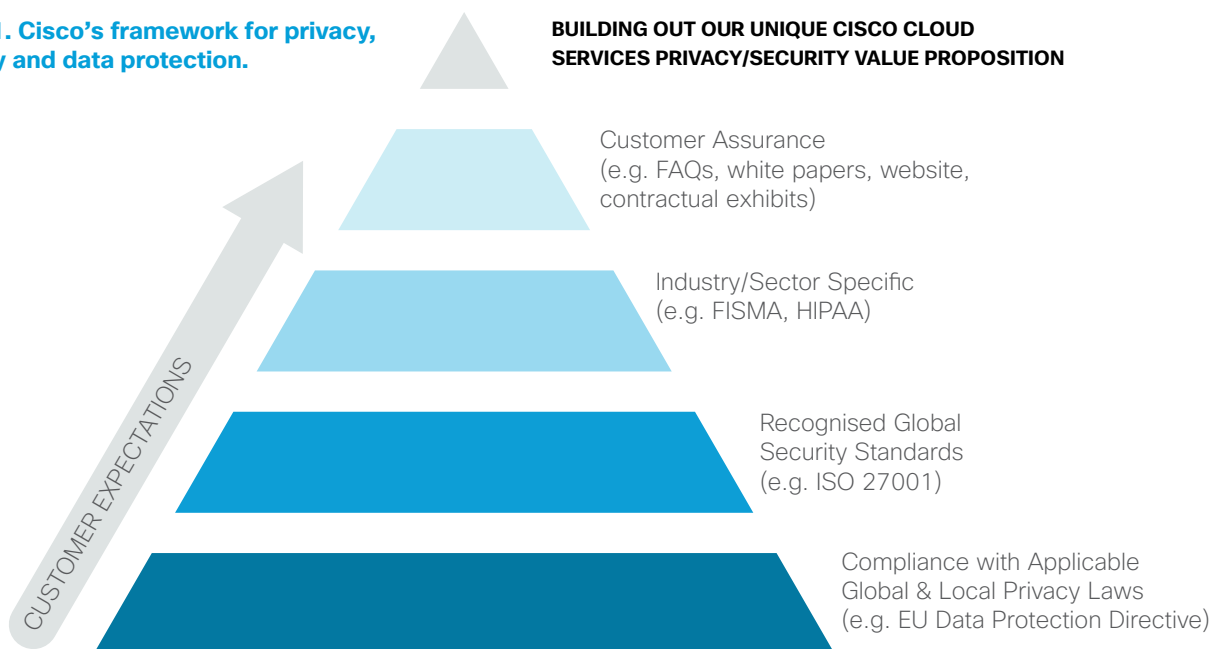
Sharing Responsibility and Governance

Our cloud security efforts focus on the underlying platform infrastructure, from the physical to the virtual environment. Customers and tenants who use Cisco Intercloud services own the compliance, security, and privacy controls for their data on the Intercloud platform.

Compliance with Standards and Certifications

We believe that security is strengthened by following globally recognized industry compliance standards. This means becoming certified, producing detailed security reports, and adhering to Cisco's information-security standards and applicable in-country laws. This framework is the foundation of our privacy, security, and data protection value proposition (Figure 1).

Figure 1. Cisco's framework for privacy, security and data protection.



Cisco CIS has achieved certification or audits according to the following standards:

- ISO 27001:2013—Certification received, June 15, 2015.
- SOC 1 (formerly Statement on Auditing Standards [SAS] 70) under the Statement on Standards for Attestation Engagement (SSAE) 16 and International Standard on Assurance Engagements (ISAE) 3402 standards
- SOC 2 for trust criteria principles for security and availability

Our plans include seeking certification for Federal Information Security Management Act (FISMA) and Federal Risk and Authorization Management Program (FedRamp) standards for two US-based CIS data centers by late 2016. This effort will support our US Federal, State and Local Government customers.

A Reputation Built on Trust by Design

Cisco's reputation as a trusted security provider rests on our ability to deliver a complete security and data protection experience in the cloud. Our criteria for trust – security, privacy, confidentiality, availability, and integrity – are the foundation. And this foundation is supported by our promise of trust by design and by our guiding principles of improving simplicity and transparency, accelerating time to market, and improving the ease of doing business with Cisco.

Working together with our customers and partners, and with industry-leading security expertise, strict internal controls, and a growing number of certifications, we are confident of our ability to be a trusted business partner for secure cloud services.

Conclusion

Defending against threats and protecting data in the cloud are complex tasks. A strong defense requires the constant monitoring of threats wherever they occur and the skill to analyze their causes and the scope of outbreaks. Not every organization can support this level of threat intelligence, but the Cisco security ecosystem is unmatched. Along with our full support for international data protection regulations, we are firmly committed to maintaining leadership in cloud security and trust.

For More Information

Please visit <http://www.cisco.com/c/en/us/products/security/index.html>