Umbrella Cloud Hosted Services

Umbrella Data Centers | FAQ | Vulnerability Notification

Umbrella Trust Overview

Cisco Umbrella LLC ("Umbrella" or "Company") is a leading provider of network security and Domain Name Server (DNS) services. It handles 2 percent of internet requests, with 80 billion daily DNS requests. This helps the world to connect to the internet with confidence on any device, anywhere, anytime. The umbrella cloud-delivered network security service blocks advanced attacks, as well as malware, botnets, and phishing threats, regardless of port, protocol, or application. Its predictive intelligence uses machine learning to automate protection against emergent threats before they can reach customers. Umbrella protects all devices globally without hardware to install or software to maintain.

Umbrella is trusted by thousands of IT professionals, from enterprises to hospitals, banks, and retailers.

This is the central repository of information regarding security, privacy, and reliability as related to Umbrella cloud hosted services. Here you will find information concerning:

- Our data centers, our security processes, and certifications
- How we safeguard your data

Umbrella Data Centers

The Umbrella service is co-located in tier-1 data centers that feature state of the art physical and cyber security and highly reliable designs. Umbrella data centers are third-party certified for security, using certifications that include ISO9001, SSAE16 and ISO27001, as described below:

Location	Provider	Certification
Amsterdam, Netherlands	Telecity (Equinix)	Equinix ISO 27001 Certificate (valid to 28-06-2019)
Ashburn, VA	Equinix	SOC 2 Type 2 Equinix (NA IBX) - 2015; Equinix (NA - IBX) - 2015 SOC 1 Type 2
Berlin, Germany	e-Shelter	DIN EN ISO 9001; DIN ISO/IEC 27001
Bucharest, Romania	GTT	ISO 9001; ISO 27001
Chicago, IL	Equinix	Equinix (NA - IBX) - 2015 SOC 1 Type 2; SOC 2 Type 2 Equinix (NA IBX) - 2015
Copenhagen, Denmark	GTT	Global connect_ISAE3402_General DC certification; Global Connect_ISAE3402_Cloud_DC certification
Dallas, TX	Equinix	Equinix (NA - IBX) - 2015 SOC 1 Type 2; SOC 2 Type 2 Equinix (NA IBX) - 2015
Frankfurt am Main, Hessen, Germany	Equinix	Equinix (EMEA) - 2015 SOC 1 Type 2
Hong Kong	iAdvantage	ISO27001
Johannesburg, South Africa	EOH JB1	ISO 9001; ISO 27001
London, UK	Telehouse	ISO/IEC 27001
Los Angeles, CA	Equinix	Equinix (NA - IBX) - 2015 SOC 1 Type 2; SOC 2 Type 2 Equinix (NA IBX) - 2015
Miami, FL	Terremark	Verizon 2015 SOC 2
Mumbai	TATA BKC (Bandra Kurla Complex)	ISO 27001 and ISO 20000
New York, NY	NTT-GIN	Zayo Group LLC 2015 SOC 1 Type 2 Report
Paris, France	GTT	BSI - ISO 27001; Telehouse - BSI 9001 FS 612057; Telehouse - BSI ISO 14001 EMS 612059
Prague, Czech	GTT	ISO 27001, ISO 1800, ISO 14001, ISO 9001
San Jose, CA	Equinix	Equinix (NA - IBX) - 2015 SOC 1 Type 2; SOC 2 Type 2 Equinix (NA IBX) - 2015
San Jose, CA	Equinix	Equinix (NA - IBX) - 2015 SOC 1 Type 2; SOC 2 Type 2 Equinix (NA IBX) - 2015
Seattle, WA	Equinix	Equinix (NA - IBX) - 2015 SOC 1 Type 2; SOC 2 Type 2 Equinix (NA IBX) - 2015
Singapore	Equinix	Equinix (APAC) - 2015 SOC 1 Type 2
Sydney, Australia	Equinix	Equinix (APAC) - 2015 SOC 1 Type 2
Tokyo, Japan	Equinix	Equinix (APAC) - 2015 SOC 1 Type 2
Toronto, Canada	Equinix	Equinix (NA - IBX) - 2015 SOC 1 Type 2; SOC 2 Type 2 Equinix (NA IBX) - 2015
Vancouver, BC	Cologix	Cologix 9-30-15 Multi-Site SOC 1
Warsaw, Poland	Linx Telecom	LINX WRW ISO 27001 2013 valid to Dec 2016; Cert ISO 9001 WRW LINX 2015

Privacy and Data Protection Compliance

Umbrella is committed to data protection, privacy, security, and compliance with applicable regulatory frameworks in the United States and abroad.

Cisco Systems and Umbrella are certified pursuant to the EU-U.S. Privacy Shield Framework. Cisco and its subsidiaries, including Umbrella, make available to its customers a Data Processing Agreement (DPA) that incorporates the European Commission's Standard Contractual Clauses (also known as the EU Model Clauses), so that customers may allow transfer and processing of personal data outside the Europe Economic Area (EEA) in accordance with applicable European privacy and data protection regulations and local laws.

Further information on the DPA and the safeguards we employ with respect to data transfers from the EEA can be found below in our FAQ.

.

FAQ for Customers: Compliance with European Data Protection Laws

What services does Umbrella offer?
Umbrella is a wholly owned subsidiary of Cisco Systems, Inc., that provides cloud-based security services to businesses and individuals. Umbrella technology identifies threats at the DNS layer, allowing connections to safe locations and blocking connections to malicious ones. Using this approach Umbrella is capable of pre-empting and preventing botnets, malware and phishing on or off the corporate network, over any port or protocol. As part of its services, Umbrella collects data from its users, and through big data analytical methods, identifies potential threats. Information about potential threats is accessible to users through a virtual "dashboard".

How does Umbrella deliver its services?
Umbrella provides management software to its customers over the internet, and customers access a web-based dashboard over SSL to gain visibility into their account info, configure policy and view logs generated. Customers log into the Umbrella services from an Umbrella website and access their accounts by means of unique usernames and passwords. Customers have the option to enable two-factor authentication to increase security.

Umbrella also supports Security Assertion Markup Language (SAML) authentication, so customers can add the Umbrella dashboard to their existing Single Sign On (SSO) service. This means we now integrate with services such as Okta, Ping, Onelogin, and others.

How does Umbrella comply with European data protection laws?
In addition to implementing a comprehensive privacy and data security program, Umbrella complies with applicable privacy laws and endeavors to follow best practices set out in relevant guidance, including the Directive 94/46 of the European Parliament of the Council of October 24, 1995. This regards the protection of individuals when processing personal data and the free movement of data (the "Privacy Directive"), as implemented into local laws, Switzerland's Federal Act on Data Protection of June 19, 1992, Germany's Federal Data Protection Act of December 20, 1990 as amended on September 14, 1994, and the nonbinding Opinion May, 2012 on Cloud Computing released by the Article 29 Working Party on July 1, 2012.

Umbrella has a more than 20 data centers located in various countries around the world (including non-European Economic Area countries). See the locations. Based on dynamic Anycast routing decisions, each customer's traffic can be routed to any data center facility listed on our network map, although normally this will be the closest physical location. The raw data is stored on Umbrella owned servers hosted in each third-party data center facility for no more than two hours. After that time, it is moved and aggregated at our Umbrella-owned servers hosted at the third-party data center facility in San Jose, California.

What about the U.S.-EU Privacy Shield Framework?
The EU-U.S. Privacy Shield Framework was designed by the U.S. Department of Commerce and European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce. Cisco Systems and Umbrella are certified pursuant to the EU-U.S. Privacy Shield Framework. Companies transferring and receiving personal data from the EU can also comply with applicable data protection regulations by signing standard contractual clauses, which consist of a set of contractual terms that have been approved by the European Commission. As described below, Umbrella offers a Data Processing Agreement to customers that incorporates these approved clauses. We do not require our customers to agree to the clauses but offer this option to give our customers an additional path to meeting requirements under applicable data protection laws.

Does Umbrella transfer Telemetry Data outside of the European Economic Area (EEA)?
When a customer makes a DNS request, it is resolved by a nearby data center, but then the request and associated IP address is sent to San Jose, CA for additional processing. This is necessary for the delivery of Umbrella services, as big data analytics requires the examination of worldwide data in real time. So while a customer's request may be resolved in the EU, all data is sent to the US for the delivery of services.

Does Umbrella make contractual commitments regarding compliance with European Privacy laws?
Yes. Cisco offers its customers a Data Processing Agreement (DPA) incorporating the European Commission's standard contractual clauses (commonly known as the "model clauses"), in accordance with the Privacy Directive, pursuant to the European Commission's decision of February 5, 2010. The European Commission has affirmed such contractual commitments to be a valid way that European customers may transfer personal data outside the EEA. By making these contractual terms available, Umbrella helps to ensure that European customers can continue to confidently deploy scalable, secure networks that comply with applicable regulations across the EEA.

What does the Umbrella privacy and data security program entail?
Umbrella takes a systematic approach to data protection, privacy, and security. We believe a comprehensive security and privacy program requires active involvement of stakeholders, ongoing education, internal and external assessments, and instilment of best practices within the organization. Cisco has established formal policies and supporting procedures concerning the privacy, security, review, and management of our products and services. The Cisco Chief Security and Trust Officer, Chief Privacy Officer, and Privacy Counsel maintain overall responsibility for the program, which is evaluated on a regular basis. This helps ensure it is up to date and follows modern security standards and best practices, as well as compliance with applicable privacy regulations. The Cisco Security and Trust Organization's Information Security and Data Protection and Privacy programs include technical and organizational measures designed to help ensure physical security, data integrity and privacy, and transparency. The Umbrella solution is designed for top-tier security and data privacy, and follows industry leading best practices for security and privacy. Umbrella data centers are certified by various industry recognized standards including ISO 9001:2008, ISO 27001, PCI DSS, SSAE16, and ISAE 3402 (SAS70) including Type II. These data centers feature state of the art physical and cyber security and highly reliable designs. DNS resolution is replicated across multiple independent data centers so that customer-facing services fail over rapidly in the event of a catastrophic data center failure.

How does Umbrella handle government requests for Customer Data or Telemetry Data?
Umbrella is committed to maintaining appropriate confidentiality, security, and integrity of all data stored on its servers. Our agreements with customers provide assurances that their data will be protected by our technical, physical, and procedural safeguards and will be kept confidential except in very limited circumstances. One such circumstance is when Umbrella has received a lawful, valid subpoena or court order requiring that we deliver data related to a customer (such as customer or telemetry data) in a controlled manner as part of an ongoing investigation. The Umbrella and Cisco Legal departments review each subpoena in order to determine its substantive merit and procedural validity. Unless prohibited from doing so, Umbrella will contact the customer regarding the subpoena and allow the customer to engage directly with the law enforcement agency making the request if the customer chooses to do so. For additional information regarding law enforcement requests for Customer Data, see the Cisco Transparency Report.

What if I have additional questions?
Please contact your Cloud Networking sales representative with more specific questions or concerns. He or she will involve our Security and Trust organization and/or privacy team as appropriate.

Vulnerability Notification

Our customers' security is a top priority for Umbrella. We invest heavily in tools, processes, and technologies to keep our users and their networks safe, including third party audits and features like two factor authentication. The Umbrella vulnerability program is an important component of our security strategy, encouraging external researchers to collaborate with our security team to help keep networks safe.

Reporting security issues

If you are a user and have a security issue to report regarding your account (including password problems and account abuse issues), non-security bugs, and questions about issues with your network, please contact Umbrella Support.

If you think you have discovered a vulnerability in an Umbrella product or service, email security@Umbrella.com or psirt@cisco.com. We take these reports seriously and will respond swiftly to fix verifiable security issues. When properly notified of legitimate issues, we will do our best to acknowledge your report, assign resources and fix potential problems as quickly as possible. Some of our products and services are complex and take time to update. We ask that you provide reasonable time for us to address the vulnerability before any public disclosure. For additional information please see the Cisco Security Vulnerability Policy.

Vulnerabilities

Any bug that substantially affects the confidentiality or integrity of user data is of interest to us. Common examples include:

- Cross-site scripting
- Cross-site request forgery

- Cross-site script inclusion
- Mixed scripting
- Flaws in authentication and authorization mechanisms
- Server-side code execution or command injection bugs

To help ensure availability of our services to all users, please refrain from using any tools that are likely to automatically generate significant volumes of traffic. Of course, your testing must not violate any law, or disrupt or compromise any data that is not your own. When investigating a vulnerability, please only target your own account. Never attempt to access anyone else's data and do not engage in any activity that would be disruptive or damaging to Umbrella, Umbrella customers, or Umbrella users.