CISCO
SECURE

White paper
Cisco public

U.S. FTC Safeguards Rule

Meeting the revised requirements with cloud-delivered security inspection and control

The bridge to possible

Contents

Introduction 3

Background 3

Meeting business goals while ensuring compliance 3

Mapping the FTC Safeguards Rule to Cisco Umbrella + Duo capabilities 3

Qualified individual designation 3

Risk assessment, MITRE Att@ck, and mitigation 4

Safeguards implementation 7

DNS-Layer Security 7

Secure Web Gateway (SWG) 7

Remote Browser Isolation (RBI) 8

Cloud Delivered Firewall (FWaaS) 8

Cloud Access Security Broker (CASB) 9

Data Loss Prevention (DLP) 9

Industry leading threat intelligence 10

Global Cloud Architecture Resiliency 10

Automation via APIs 11

Cisco Network integration 11

Protection off network for Macs/Windows Laptops, Chromebooks, and Android/iOS devices 12

Test + monitor safeguards effectiveness 12

Ensure personnel can enact your program 14

Service providers 14

Improve continuously 15

Incident response planning 15

Internal reporting 17

Next steps 18

Introduction

Background

In 2021, the United States Federal Trade Commission (FTC) announced changes to its Standards for Safeguarding Customer Information (the Safeguards Rule), to be implemented by June 2023. The revised Safeguards Rule applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services. The FTC's definition of "financial institution" includes many businesses that do not normally describe themselves as such. Organizations newly subject to the FTC's enforcement authority include (but are not limited to): car dealerships, check-cashing businesses, mortgage brokers, non-bank lenders, credit-reporting agencies, personal property or real estate appraisers, professional tax preparers, and courier services.[1] These businesses are required by the FTC to develop, implement, and maintain a comprehensive security program to keep their customers' information safe.[2]

Meeting business goals while ensuring compliance

The Safeguards Rule requires mitigation of "reasonably foreseeable internal and external risks" – in other words, protection against data breaches, data leakage, phishing, and ransomware.

Cisco Umbrella supports a robust set of converged cloud-native security capabilities, including DNS-layer security, to begin demonstrating compliance in as little as 24 hours. With Umbrella, you can comprehensively address both compliance and security needs with additional capabilities, like data loss prevention, cloud access security broker, remote browser isolation, malware inspection, and web security.

Umbrella meets business needs for compliance, security, and productivity. In environments where compliance is a cost of doing business, there is no time to lose. Implement Umbrella and begin checking off critical items for demonstrating FTC Safeguards Rule compliance in days — not weeks or months.

Mapping the FTC Safeguards Rule to Cisco Umbrella + Duo capabilities

This document maps Umbrella features and functionality to the requirements contained in FTC Safeguards Rule: 3.14.4 Elements[3] so you can make informed decisions on your compliance investment. For clarity, text below that is directly from the revised Safeguards Rule is presented in ***bold italic*** text.

Qualified individual designation

a) ***Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program.***

Umbrella is simple to deploy and easy to manage by either a covered business directly, or via a Managed Security Services Provider, or Managed Detection and Response provider, who would be designated as a Qualified Individual. Umbrella delivers robust security protection that helps enhance their security practices, providing covered companies with protection on and off network from cyberthreats, mitigating them before they reach your networks and endpoints. Real-time security activity reports rapidly identify compromised

1 Part 314 – Standards for Safeguarding Customer Information: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314
2 National Archives Code of Federal Regulations, Title 16 / Chapter 1 / Subchapter C / Part 314: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314
3 FTC Safeguards Rule https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314/section-314.4

systems at covered businesses, manage and control cloud application usage, and enforce acceptable usage policies.
As a cloud-delivered service, with no hardware to install or software to manually update, Umbrella reduces complexity with robust APIs and a centralized console with logging and reporting.

Cisco Umbrella: critical to your compliance journey

Risk assessment, MITRE Att@ck, and mitigation

b) Base your information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks.

As you are developing the risk mitigation plan that the FTC Safeguards Rule requires, use the below table to identify the critical risks that apply to the threat model for your environment, and note how Umbrella capabilities can help mitigate these risks. Also noted below are references to the MITRE ATT@CK Framework. The MITRE ATT&CK Framework is a comprehensive organization and knowledge base of adversary tactics and techniques, based upon real-world observations. Security practitioners use MITRE ATT@CK to improve threat detection, incident response, and cyber defense strategies by understanding and simulating attackers' behaviors.

Table 1. Common Risks and Mitigations

RISK	MITRE ATT@CK REFERENCES	UMBRELLA + DUO MITIGATIONS
Mixed mode workstations - Systems with consumer financial data also used for other activities.	• Command and Control – DNS https://attack.mitre.org/techniques/T1071/004/ • Command and Control – Web protocols https://attack.mitre.org/techniques/T1071/001/ • Drive-by compromise: https://attack.mitre.org/techniques/T1189/ • Browser Session Hijacking https://attack.mitre.org/techniques/T1185/	• Umbrella DNS-layer security can detect and mitigate ransomware, command and control callbacks, and phishing attacks • Umbrella Remote Browser Isolation (RBI) protects against browser-based security threats when users visit sites with vulnerabilities or malware. Umbrella RBI enables users to web browse safely, enabling productive website access with security by isolation. • Umbrella Secure Web Gateway (SWG) automates logging Web activity, analyzing content via malware sandboxing, and blocking access to risky sites. • Umbrella's SNORT IPS detects malware.

		• Cloud access security broker (CASB) – controls web application access, enables cloud malware discovery, and provides tenant controls to secure resources on shared domains like Microsoft Office 365.
Insider threats – Users may attempt to exfiltrate sensitive consumer financial data for financial gain or business sabotage.	• MITRE has recognized, outside of the ATT@CK Framework, the uniqueness and importance of insider threats; see https://insiderthreat.mitre.org/insider-threat-framework-initiative/	• Umbrella Data Loss Prevention (DLP) analyzes outbound web traffic and performs out-of-band cloud-based inspection, for the industry's only unified DLP policy control and logging. Pre-built and customizable data identifiers enable fast deployment and identification of leaking customer personally identifiable information (PII). • Cloud access security broker (CASB) can limit the availability of web applications that serve as conduits for exfiltration.
Valid account attacks – Attempt to masquerade as an authorized user to access sensitive systems with customer information. Compromised credentials may be used to bypass access controls	• Valid accounts - https://attack.mitre.org/techniques/T1078/	• Duo directly meets the Safeguards Rule requirement for multifactor authentication. Additionally, Umbrella can leverage Active Directory to enforce granular user and group access policies for additional access control. • Cisco Duo multi factor authentication (MFA) integrates with Cisco Umbrella for both identity provider data and Umbrella dashboard access and strengthens access security by requiring multiple methods to verify user identity and validate that users are who they say they are.
Phishing attacks – Attempts to trick users into clicking links that download malware, or directs them to a malicious website where their identity may be compromised	• Phishing attacks- https://attack.mitre.org/techniques/T1566/	• Umbrella DNS mitigates phishing attempts, protecting users from accessing known malicious domains and websites – before connections are made. • Umbrella Secure Internet Gateway (SIG) adds additional security; its Secure Web Gateway functionality can block access to compromised websites designed to steal personal information.
Lateral Threat Movement and Adversary Tool Transfer – Adversaries may transfer tools or other files between systems in a compromised environment.	• Command and control - https://attack.mitre.org/tactics/TA0011/	• Umbrella DNS mitigates lateral threat movement by blocking communication with known malicious IP addresses (Command Control Callbacks) to prevent compromised devices from communicating with command-and-control servers through any application, protocol, or port. • Additionally, Umbrella DNS helps identify potentially infected machines on your network with this detection.
Compromise of Cloud Storage Data – Adversaries may access data from improperly secured cloud storage	• Data from cloud storage - https://attack.mitre.org/techniques/T1530/	• Umbrella DLP helps identify sensitive data in cloud data stores. • Umbrella CASB functionality can help ensure that access to risky cloud applications is disabled, adding additional risk mitigation.

Browser Hijacking - Leveraging browser vulnerabilities to change content, modify user-behaviors, and intercept information	• Browser Session Hijacking https://attack.mitre.org/techniques/T1185/	• Umbrella remote browser isolation (RBI) isolates web traffic between the user device and browser-based malware. It creates a surrogate browser in the cloud that visits a website on behalf of the host systems, rendering all content safely and seamlessly. • Users can browse potentially risky sites safely and maintain productivity. • IT teams spend less time granting exceptions and responding to attacks. • Umbrella RBI is cloud-delivered, scales on demand, and works with all common devices, browsers, and operating systems.
Data Exfiltration - Adversaries may use techniques to steal data from your network. Once the data is collected, adversaries often package it to avoid detection during removal	• Exfiltration - https://attack.mitre.org/tactics/TA0010/	• Umbrella has developed a new proprietary cache within our DNS resolvers to work alongside our machine learning modules, tuned to detect data exfiltration and DNS tunneling events. • Additionally, Umbrella DLP capabilities provide a unified experience for configuring, controlling, and monitoring sensitive data in motion leaving your business and across your cloud applications. You can discover and block sensitive data being transmitted to unwanted destinations or exposed in sanctioned applications to prevent data exfiltration events from taking place.
Ransomware and Data Destruction – Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. This is a true targeted attack where your business is the target of choice versus the target of opportunity.	• Data destruction - https://attack.mitre.org/techniques/T1485/	• Umbrella proactively protects against early stages of the Cyber Kill Chain[4]. • Umbrella blocks access to malicious websites, protecting users from accessing malicious domains - before a connection is ever made at the DNS layer, and over every port and protocol. Umbrella CASB capabilities block unauthorized access to cloud applications and the data within them. • Umbrella protection for command and control callbacks prevents compromised devices from communicating with maliciously controlled servers through any application, protocol, or port; and helps identify potentially infected machines on your network.

[4] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Safeguards implementation

c) Design and implement safeguards to control the risks you identify through risk assessment.

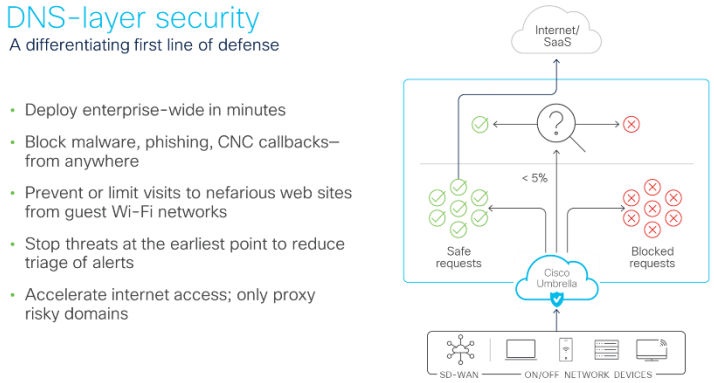
Umbrella offers flexible, cloud-delivered security. It combines multiple security functions into one solution, so you can extend data protection to distributed locations, remote users, and devices anywhere. Its feature-rich DNS security, secure web gateway, cloud-delivered firewall, CASB, and DLP functionality demonstrate FTC compliance and secure your environment:

- Visibility across all remote and on-site devices, ports, and cloud services
- Prevention against phishing, malware, and ransomware attacks
- Threat intelligence to uncover and defend against current and emerging threats

DNS-Layer Security

Umbrella DNS provides the visibility needed to protect internet access across all devices on your network, all office locations, and roaming users. By enforcing security at the DNS and IP layers, Umbrella blocks requests to malicious and unwanted destinations before a connection is established – stopping threats over any port or protocol before they reach your network, endpoints, or users.

Umbrella DNS is the fastest and easiest way to protect users in minutes with a 2-click process to get activated – signup, point DNS, and you are done. Because it is cloud-delivered, there is no hardware or software to install or update. Provision Umbrella on-network devices –including BYOD and IoT – in minutes and use your existing Cisco footprint to quickly provision thousands of network egresses and roaming laptops, plus managed Chromebooks, and managed/unmanaged iOS and Android devices.

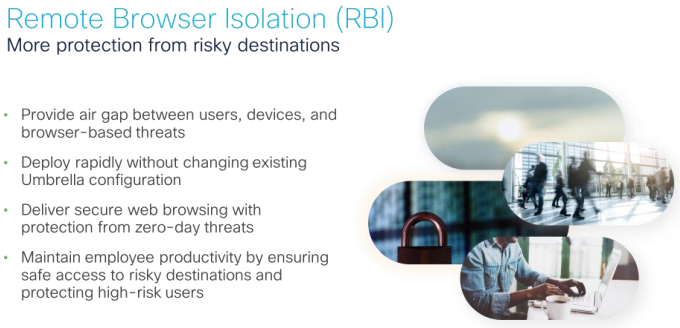


Secure Web Gateway (SWG)

Umbrella SWG functionality provides cloud native, full proxy capabilities to improve performance and reduce risk by efficiently logging, inspecting, and controlling web traffic. It offers full visibility of all web traffic with URL logging and real time reporting, advanced malware protection with file inspection, sandboxing, and blocking, SSL traffic decryption and inspection, content, and granular app activity controls, in one easy to use interface.

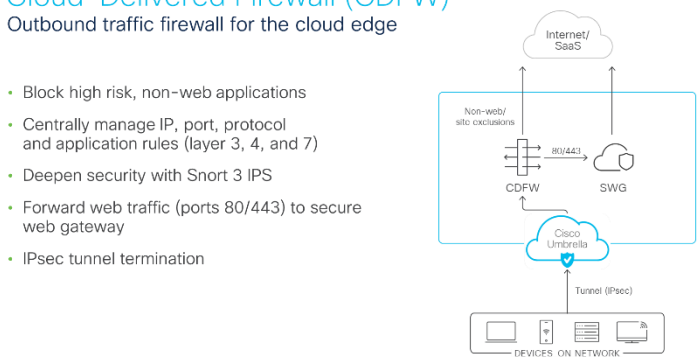
Remote Browser Isolation (RBI)

Umbrella RBI provides an added layer of protection against web browser-based threats. RBI moves the most dangerous part of browsing the internet away from users' devices and into the cloud, allowing a balance of productivity and security. This makes it possible for users to visit risky web destinations safely, enabling users to be productive and access the web destinations they need without negative impacts.



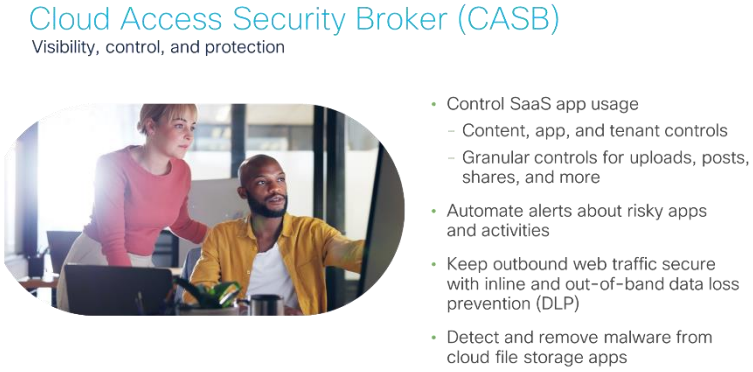
Cloud Delivered Firewall (FWaaS)

Umbrella cloud-delivered firewall provides visibility and control for traffic that originated from requests going to the internet, across all ports and protocols. It logs all activity and blocks unwanted traffic with layer 3/4 firewall rules (IP, port, and protocol), and Layer 7 application visibility and control rules to block insecure applications, shadow IT, unsanctioned traffic, and intrusion prevention system (IPS) rules based on Snort 3, the industry standard for deep packet inspection to rapidly detect and block indicators of compromise (IOCs).



Cloud Access Security Broker (CASB)

Umbrella helps expose shadow IT by detecting and reporting on cloud applications in use across your environment. These insights can help manage cloud adoption, reduce risk, and block the use of offensive or inappropriate cloud applications which violate your business acceptable usage policies and may introduce cyber risks into your environment.



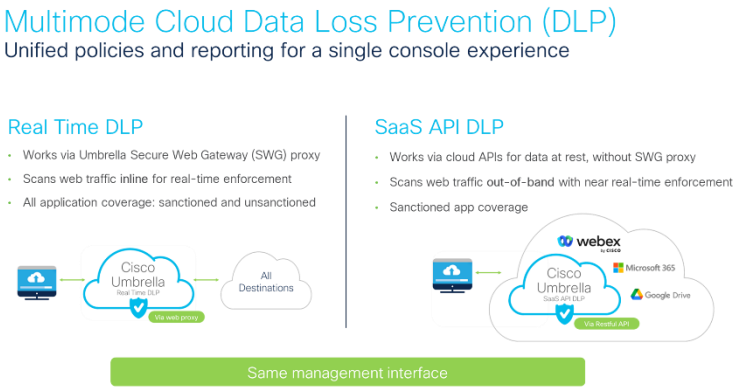
Data Loss Prevention (DLP)

Umbrella multimode DLP analyzes data both inline (data in motion) and out-of-band (data at rest) in your cloud applications to provide visibility and protection over sensitive data leaving your organization or exposed in the cloud. Only Umbrella DLP includes common policies and logs for both in-line and cloud based methods. Pre-built data identifiers are available to match personal identifiable information (PII) types from global country, government, and industry types, such as healthcare. Umbrella also supports the creation of custom-built data identifiers.

For covered companies under the FTC Safeguards Rule, the United States pre-built identifiers that Umbrella DLP supports include:

- ABA Routing Number (US)
- Bank Account Number (US)
- Driver's License (US)
- Individual Taxpayer Identification Number – ITIN (US)
- Date of Birth and Person Name (US)

- Multiple Personal Identifiers – PII (US)
- Passport (US)
- Social Security Number (US)

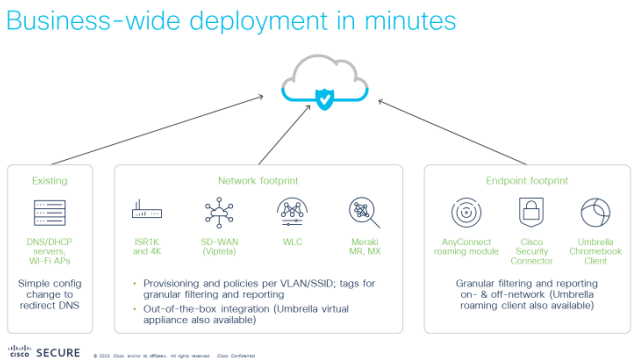


Industry leading threat intelligence

Cisco Talos is one of the largest commercial threat intelligence teams in the world; comprised of world-class researchers, analysts, engineers, and incident responders. They provide actionable intelligence for known and emerging threats, protecting Cisco customers and the open-source community at large against the latest threats and attack vectors; to see more, stop more, and act faster. Umbrella gains statistical models, machine learning algorithms, and enormous volumes of threat data through Cisco Talos to map a holistic view of the threat landscape to better detect nefarious activity and anticipate future attacks.

Global Cloud Architecture Resiliency

Umbrella's agile global cloud architecture delivers network resiliency and reliability to keep your performance fast and your connections secure. In addition to a growing global data center network, Anycast augmented routing, and over 1000 peering relationships, Umbrella delivers the best security protection and performance to deliver the performance your business requires all day and every day. Since 2006, Umbrella DNS services have provided 100% business uptime.



Automation via APIs

Umbrella enables you to complete the last necessary step to operationalize your threat intelligence and leverage your disparate products into a cohesive level of protection. By leveraging Umbrella APIs, organizations can easily generate integration and orchestration workflows to enforce the intelligence gathered from your various security tools. The rich collection of APIs makes it simple to aggregate Umbrella's industry leading visibility and control with cross product intelligence to enhance your overall security posture. The sum is greater than the individual parts due to shared context and intelligence across products and platforms.

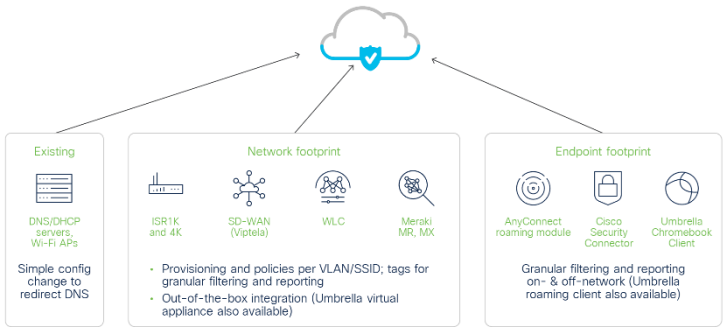
Reduce number of alerts and gain context on threats by leveraging the Umbrella Investigate API to programmatically pull contextual threat intelligence resulting in global context with each alert to allow your team to focus on critical incidents versus noise.

Cisco Network integration

Enhance and extend security to your existing Cisco networking footprint to quickly provision thousands of network egresses and roaming laptops — protecting your off-network users, branch locations, and Wi-Fi users in minutes. Umbrella offers simple integrations with many Cisco network devices, enabling you to easily deploy powerful protection without operational complexity.

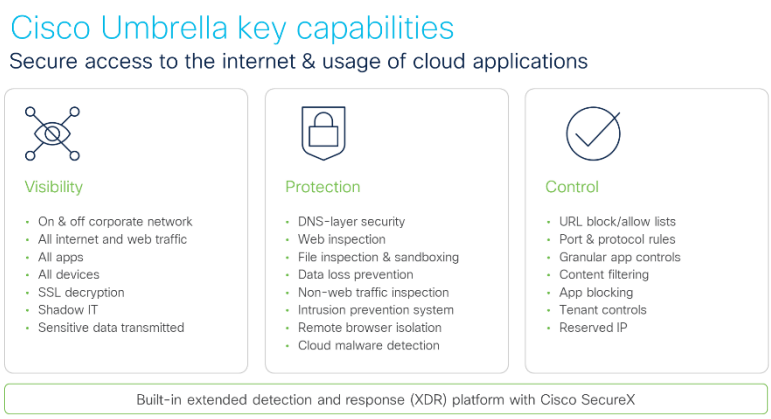
Cisco Integrations include:

- SD-WAN
- Meraki
- Integrated Services Routers (ISR)
- Wireless Lan Controller (WLC)
- Mobility Express
- Cisco Secure Firewall
- Small Business RV Series Routers
- Catalyst 8000 Series Edge Platforms



Protection off network for Macs/Windows Laptops, Chromebooks, and Android/iOS devices

Easily extend protection beyond the corporate network. Protect laptops, and managed or unmanaged Chromebooks, Android and iOS devices, no matter where they are through integrations with Secure Client (formerly AnyConnect roaming module), Cisco Security Connector, and Umbrella Chromebook clients.



Test + monitor safeguards effectiveness

d) Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems. For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments.

Umbrella provides visibility across all remote and on-site devices, ports, and cloud services to protect against phishing, malware, and ransomware attacks, with the security intelligence to uncover and defend against current and emerging threats. Leveraging threat intelligence from Cisco Talos, one of the largest commercial threat intelligence teams in the world, Umbrella uncovers and blocks a broad spectrum of malicious domains, URLs, and files actively used in attacks. Umbrella threat analysis sees the relationships between malware, domains, and networks across the internet and learns from internet activity patterns to automatically identify attacker infrastructure being staged for the next threat.

An example of Umbrella real time monitoring is the DNS Monitoring Package. It offers real-time reporting and categorization of all internet activity. It provides valuable insights into critical events on the network, including the occurrence of malware, ransomware, and phishing threats for quick detection/blocking and enforcement of content filtering rules. In real-time, all internet activity over any port or protocol is logged and categorized by 8 types of security threats, as well as 80+ types of web content. Administrators can search, filter, and export 14-days of activity. Simple to deploy – change one setting on network devices - no hardware installation or software to manually update.

Continuous reporting is an important consideration to better monitor and understand the threat environment and Umbrella usage. Reports help build actionable intelligence in addressing security threats including changes in usage trends over time to demonstrate compliance by protecting customer data. Examples of available reports include:

- Security Activity – Security-related activity in your environment, including malware, phishing, and all other security categories over the selected time period. Filterable by identity, destination, source IP, and security category.
- Activity Search – Activity from the identities in your environment over a selected time period. Filterable by identity name, destination, source IP, response, content category, and security category.
- App Discovery – Information about the cloud apps in use in your environment.
- Top Threats Report – Highlights blocked and allowed threats your organization may have been exposed to over a selected period of time.
- Total Requests – Total requests for destinations from your organization over the selected time period. Filterable by identity.
- Activity Volume – Total queries within your organization broken down by security categories and results over the selected time period.
- Top Destinations – A list of the top traffic-generating identities over the selected time period. Filterable by identity and destination.
- Top Categories – A list of the top content categories for your organization over the selected time period. Filterable by identity and response.
- Top Identities – Lists your identities in the order of which is most active, then allowing you to drill down to find out more about that specific identity and what destinations they have visited, whether those destinations are malicious or not, and a trend of their overall traffic.
- Admin Audit Log – A record of any configuration changes made to Umbrella settings by any of the Umbrella administrators.
- Cloud Malware Report – Provides an overview of malicious files within your environment and details the potential risk and exposure these files present
- Data Loss Prevention Report – Data violations detected through the Real Time and SaaS API rules are logged as part of the unified Events view of the Data Loss Prevention Report.

In addition to Umbrella specific capabilities, there are Umbrella integrations with Cisco SecureX XDR and 3rd party security platforms to provide additional context and insight. Cisco SecureX XDR is a cloud-native incident and threat response solution that aggregates Umbrella monitoring insights with the rest of the Cisco Security

portfolio and 3rd party security products. With Umbrella and SecureX, you can respond to integrated threat information, and view global threat intelligence with Umbrella specific product insights.

Third party orchestration, automation, incident response and SIEM products that support Umbrella include IBM, Google, Splunk, Exabeam, LogRhythm, NetWitness, Rapid7, Menlo Security, Cofense, Defense Storm, Digital Shadows, Efficient iP, Elastica, NS1, Perch Security, Sumo Logic, Swimlane, Threat Connect, Threat Quotient, UncommonX, Zerofox.[5]

Ensure personnel can enact your program

Implement policies and procedures to ensure that personnel are able to enact your information security program.

As a trusted partner to over 26,000 organizations, Umbrella, with its DNS-layer security capabilities, provides the quickest, most effective way to improve your security stack. Gain a new layer of breach protection in minutes, with internet-wide visibility on and off the network, no matter your company size.

The easy-to-use, cloud-delivered administration console enables the quick set up, management, and testing of different acceptable use policies per network, group, user, device, or IP address, providing greater control of the businesses' internet usage. Flexible policies can be set up depending on whether users are on or off the corporate network to support compliance efforts and provide effective threat protection when users are remote.

Service providers

e) Oversee service providers

As an MSSP acting as a qualified individual for a covered business, it is important to demonstrate to the covered business how you supported their compliance efforts. Umbrella provides a variety of reports to demonstrate critical security measures are in place, such as

- Prevention of malware, ransomware, and phishing attempts from malicious websites
- Enforcement of acceptable usage policies of the business
- Identified compromised systems by using real time security reports
- Managed and controlled cloud application usage
- Managed access control policies of the business so only authorized users could access customer data
- Demonstrated business compliance via DLP reporting

[5] Cisco Security Technology Alliance partners: https://www.cisco.com/c/en/us/products/security/technical-alliance-partners.html?selectedFilter:cisco-products-umbrella&selectedFilter:cisco-products-umbrella-investigate

Improve continuously

f) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

Umbrella real time and historical monitoring and reporting capabilities are important tools for continuous analysis and policy enhancements to strengthen customer data protection for FTC Safeguards Rule compliance.

Umbrella provides administrators both at the covered business or at the MSSP real-time information to quickly review, respond, and remediate against an attack. And continuous analysis is key to protecting the business from future attacks by helping refine its security posture to ensure preventative action has been put in place.

Several reports support the export of the results to the CSV format to allow for the creation of new reports and graphics and the integration with other reporting tools. Reports may be shared with coworkers and/or by MSSP's with their customers for additional analysis and discussion. The reports contain a rich amount of data and can be customized to provide the specific level of context and insight required.

For example, the Activity Search report shows the result of every DNS, URL, and IP request from the identities reporting to Umbrella for the selected date/time. It lists all security (and non-security) related activity and allows for search refinement using filters to see the activity most important to you. This helps rapidly identify high priority security issues within your organization that require attention. By clicking an identity or destination, you can quickly pivot from the Activity Search report to the Top Identities and the Top Destinations reports for additional clarification. Additional insight is available in the Identity Details and Destination Details reports for further information on individual identities and destinations.

Incident response planning

g) Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control.

Security incidents occur in every organization. A well-designed incident response plan can be the crucial factor that helps a business quickly contain the damage from an incident and rapidly recover normal business operations. Several incident response frameworks have been developed by thought leaders in the field, such as the NIST Computer Security Incident Handling Guide. It outlines the following four-step incident response cycle: Preparation, Detection and Analysis, Containment, Eradication and Recovery, Post-Incident Activity.

Preparation

The first step is to understand the Cisco Umbrella product capabilities and use that to develop a security profile for your business. Join a Cisco Umbrella Studio workshop to learn how Umbrella can help businesses

address different security use cases. No prior knowledge of Cisco Umbrella or other security products is necessary. The lab content is provided in an easy to follow step-by-step format with self-contained lab resources for each participant to deploy Cisco Umbrella in their own self-contained virtual environment.[6]

Detection and Analysis

Leverage the roust reporting capabilities within Umbrella to customize reports based on threat activity and identified risk factors in the covered business environment. Identify an individual to run and review Umbrella reports so malicious threats are identified to be tracked and mitigated. Deploy configuration and changes to employee access to critical applications containing customer data based on that analysis. Continuously monitor and adjust as needed based on business requirements.

Umbrella handles device and cloud security protection for egress traffic. Because Umbrella deploys in the cloud, it can also handle traffic for devices connected directly to the Internet without using VPN. This protection is accomplished using Umbrella's DNS and Secure Web Gateway based filtering, which blocks a myriad of threats including malware, ransomware, command-and-control (C2) installations and calls to attacker-controlled services, phishing, and exfiltration of data from already compromised systems.

Containment

Umbrella sees the relationships between malware, domains, and networks across the internet, leveraging Cisco Talos threat intelligence, the largest private threat research organization to block suspicious activity. Its threat analysis learns from internet activity patterns to automatically identify attacker infrastructure being staged for the next threat and mitigate it.

One of the most notable features in Umbrella is DNS-based web content filtering. For every web-based request, a user's browser queries DNS servers for an IP address that matches a fully qualified domain name (FQDN). Umbrella acts as a layer between this request to identify if the domain is identified as malicious. Users are blocked immediately at this point and cannot open any malicious content on the hosted domain. It's an effective way to block malicious content instead of relying on basic domain filtering.

DNS-based web filtering works well with Umbrella's Secure Web Gateway (SWG). The SWG proxies web traffic for inspection, including inspection of HTTPS (SSL/TLS) traffic to greatly reduce the risks from users browsing malicious websites, pages, and domains.

Eradication and Discovery

Protecting the environment with Cisco Talos by safeguarding user devices/endpoints is just one of several benefits of adopting Cisco Umbrella.

1. Content-based browsing policies – Domains are divided into 80 different categories, and administrators can use various user properties to set up browsing permissions. Administrators can use network, IP address, group, user account, or device to configure domain category policies.

2. Discover shadow IT applications– Rapidly growing businesses often provision cloud resources without any documentation, leaving applications unmanaged but active in the corporate environment. Without administration, these shadow IT applications could be a target of a compromise from unpatched vulnerabilities.

[6] https://umbrella.cisco.com/info/cisco-umbrella-studio

3. Cloud-based firewalls – Gain better visibility and control for internet traffic originating from client requests. Layer 7 application visibility and control, intrusion prevention system (IPS), and layer 3/4 firewall features protect traffic across all ports and protocols without performance degradation.t.

4. Traffic inspection in transit–Umbrella will inspect traffic (including SSL/TLS traffic) for any anomalies or possible data exfiltration to support the latest data loss prevention (DLP) strategies.

5. Threat intelligence for future detection of zero-days – The cybersecurity landscape is always evolving, and any defenses must be able to rapidly change to detect the latest threats. Umbrella integration with Cisco SecureX XDR provides tracking threats of the latest threats across an entire environment, resulting in a more robust defense solution.

Post Incident Activity

Umbrella provides predictive intelligence so your teams can research a given incident and stay ahead of future attacks. Umbrella identifies millions of security events happening in real-time across more than 100 million daily-active users. It uses big data analytics and machine learning to predict where related attacks will emerge on the internet, to provide customers real time threat intelligence to get more out of their existing network security investments and become more proactive at combating the next cyber-attack.

By adding Umbrella's global threat intelligence data as a layer in your security stack, your business can be more proactive in their approach to security. Use the Umbrella Investigate API, to view real-time data and predictive models alongside data from your other security devices and services. Umbrella delivers value by finding attacks that slip through the cracks of other security solutions.

Internal reporting

h) Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your information security program.

Umbrella is designed to provide businesses with robust customer protection, helping MSSPs and MDRs grow their security practice. It provides covered businesses with on and off network protection from cyberattacks, stopping threats before they ever reach their networks or devices. Umbrella is simple to deploy and easy to manage, relieving the business or the MSSP or MDR from complex management of the product. Since its a cloud-delivered security service there is no hardware or software to maintain.

Comprehensive reporting capabilities provide custom details based on the needs of the business or the MSSP supporting them, allowing them to show the security incident information that is most critical. For MSSPs, those reports can be shared directly with covered customers to identify incidents within the customer's environment and the security policies in place to mitigate the threats.

Next steps

Learn More about the FTC Safeguards Rule and Cisco Umbrella

Learn more about how to be compliant with the FTC Safeguards Rule by visiting the Cisco Umbrella dedicated webpage to gain additional insights to help you with your compliance journey.

Read more: https://umbrella.cisco.com/solutions/ftc-safeguards-rule-compliance-2023

Register for a Product Demo – See Umbrella in action

Join us for an online demo. Learn how Umbrella can help you cut complexity, reduce risk exposure, and improve performance by simplifying and streamlining cloud-delivered security.

Register here: https://umbrella.cisco.com/info/cisco-umbrella-live-demo-webinar?utm_content=cisco-umbrella-live-demo

Sign up for a Free Umbrella DNS trial

Secure your users, anywhere they work today with a free 14-day trial of Umbrella DNS-layer security.

Get started in minutes, not months with a few quick steps. Complete a short form on the Umbrella website. Activate your trial from the confirmation email we will send you. Name your network and point your DNS to the Umbrella global network. Any device or roaming user that joins your network is instantly protected

Signup here: https://signup.umbrella.com/?utm_content=automated-free-trial&_ga=2.131947595.513208595.1679318407-1483179553.1678812826

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.