Cisco global cloud architecture sets the stage for powerful cloud security

Built-in flexibility, resilience, performance, and agility set Cisco Umbrella apart.

Table of Contents

1

Today's new normal and the necessary evolution to SASE

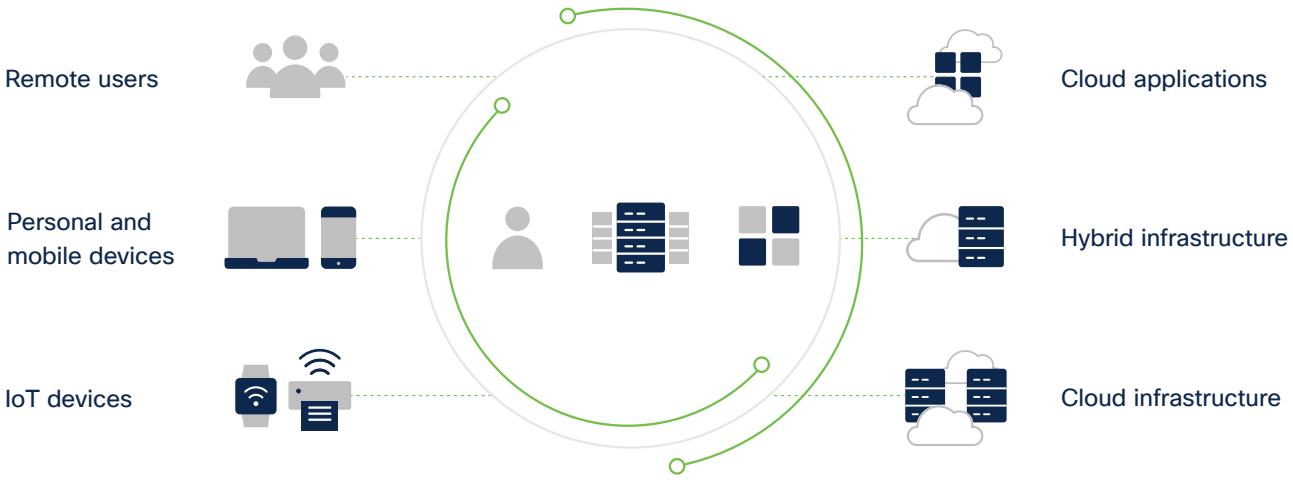
The new normal: decentralized networks

Exploding SaaS usage. Proliferating remote locations. Swelling ranks of roaming workers. The wide-scale adoption of cloud applications is fundamental to successful business operations. It's the new way of operating, and it's transforming enterprise security and networking.

In the wake of the COVID-19 pandemic, these trends have skyrocketed. As a result, IT and cybersecurity teams continue to wrestle with securing their cloud perimeter while providing the access, reliability, and speed users expect. The good news is that it is possible to decrease complexity, reduce risk, and move toward a coordinated, secure cloud approach at the cloud perimeter—without compromising performance.

Shift in IT landscape

Users, devices, and apps are everywhere



Branches of one expand the threat landscape

Your employees work from everywhere – at home, in coffee shops, the car, the airport, and even back in the office. They're working on a range of devices, which may or may not be company issued, approved, or secured. And, they're accessing data and applications not only in the data center but also in multiple public and private clouds.

Your data center is no longer your hub – your users are. To provide each user with secure access to work resources and applications, organizations must see each individual as a "branch of one." Protecting this expanded perimeter – consisting of many branches of one – requires the flexibility, capability, and scalability of cloud-based security.

Although helpful, this can add complexity to the formerly straightforward task of connecting users to applications in the data center. How users connect to business applications can differ daily. And users aren't concerned with what goes on behind the scenes. They just want easy access to what they need.

To ensure users have high performance as well as secure, reliable access, network and security organizations must consider a number of factors, including:

App location

User location

User connection

Using multi-cloud technologies and apps to support today's distributed work is also increasing our exposure to threats.

93%

of enterprises embrace a multi-cloud strategy.[1]

82%

of workers will work in a hybrid model.[2]

40%

increase in phishing in the past year.[3]

The necessary evolution to SASE

The traditional perimeter-based security model can't keep up with the continued shift to decentralized work and security's shift to the cloud. To be successful, IT teams need a new approach to control and secure their users, applications, devices, and data — wherever they are.

Enter secure access service edge (SASE), which Gartner defines as "an emerging offering combining comprehensive wide area network (SD-WAN) capabilities with comprehensive network security functions (such as secure web gateway (SWG), cloud access security broker (CASB), firewall as a service, and zero trust network access) to support the dynamic secure access needs of digital enterprises." Other analysts speak to the same concept albeit using different terms.

SASE is not a product. It is an architecture. And because everyone starts from a different place and has different goals and needs, transitioning networking and security to the cloud is an on-going journey, not a one-time event.

SASE helps you regain control of your security and your perimeter

As a cloud-edge service that helps organizations scale and simplify amidst fluctuating worker distribution, SASE allows IT and security teams to better leverage the cloud for secure networking. With SASE, they can:

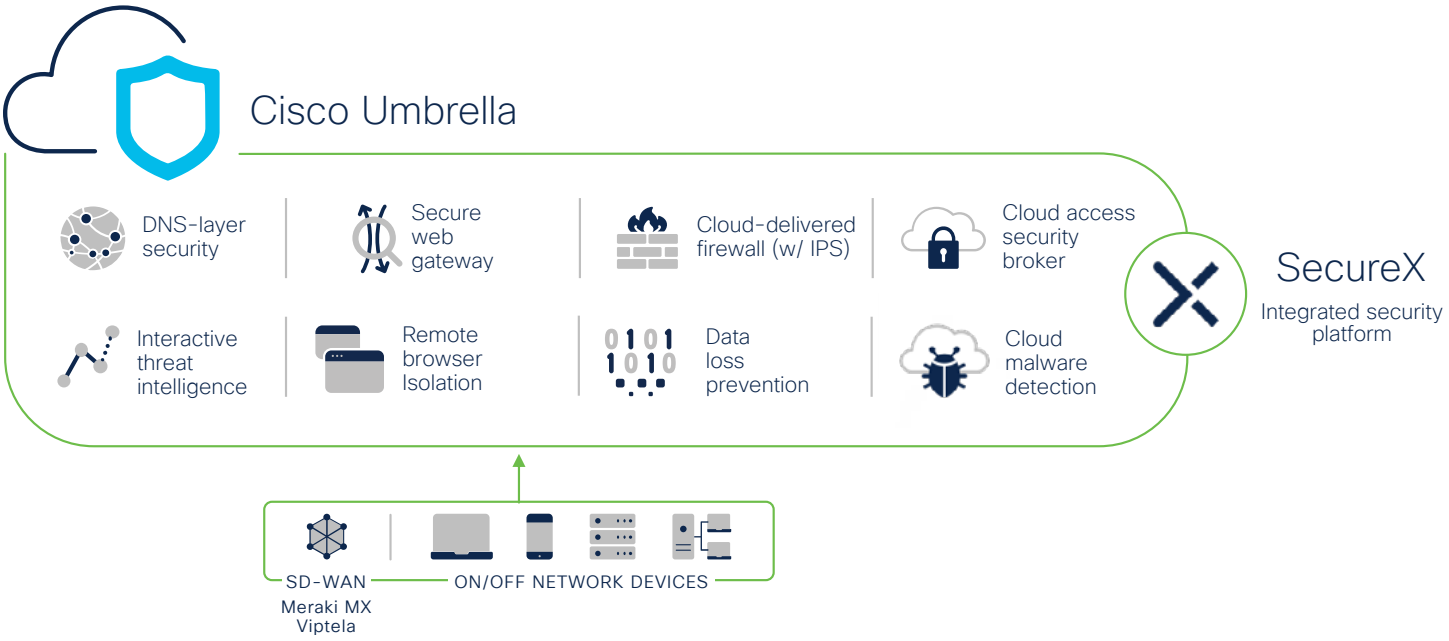
- Deliver a seamless secure connection to any application, from any device, at any time
- Lower complexity and more flexibly scale up and down
- Converge resources for greater efficiency through a secure networking-as-a-service model
- Safely move access control closer to where it's needed – to the user and the cloud edge

2

Cisco Umbrella: Core security in the Cisco SASE architecture

Umbrella is a highly elastic, cloud-native security service that forms the core security of Cisco's SASE strategy. Umbrella offers a broad set of security functions that previously required separate firewall, secure web gateway, cloud access security broker capabilities, threat intelligence, and more.

By enabling all these capabilities from a single, cloud-delivered service and dashboard, Umbrella significantly reduces the time, money, and resources previously required for network and security deployment, configuration, and integration tasks.

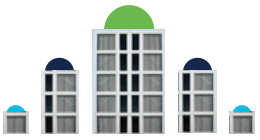


3

Global cloud architecture powers Umbrella

Powerful, reliable, secure cloud architecture is essential to successful cloud security. The right cloud architecture solution is rooted in a robust, global, and battle-hardened cloud architecture; how that solution is designed, architected, built, and enhanced directly impacts the success of the architecture, and ultimately your business and your bottom line.

The Umbrella global cloud architecture was meticulously researched and thoughtfully built to support innovative cloud security services. Using micro services with huge capacity, the global cloud architecture delivers:



Flexibility:

Infrastructure that rapidly scales up and down

Resilience:

Strong network reliability

Performance:

High performance, network capacity, and throughput

Agility:

Adaptive infrastructure means continuous innovation without downtime

Lightning-fast performance. Rock-solid reliability. Umbrella's global cloud architecture delivers network resiliency and reliability to keep performance fast, and connections secure.

Flexibility to adapt and respond to unceasing risks and changes

Today's business feels like a constant flow of business shifts and technical challenges, interspersed with disruptions, rounded out by unceasing risks and threats. Operations, IT, and cybersecurity teams must be ready for anything, nimbly averting potential disasters while building a flexible and scalable network security environment.

The Umbrella global data center network is up to the challenge

The Umbrella global network includes 37 data centers in 37 cities, across 23 countries (as of January 2022), and new data centers are continuously coming on-line across Asia, Europe, and the Americas.

Massive, diverse data sets

Our extensive global footprint allows us to resolve over 620 billion DNS requests daily from more than 24,000 enterprise customers, from over 190 countries, and it provides us with a vast amount of highly diverse, highly usable data. From multiple geographies and protocols, this data enables unrivaled insight into launched attacks as well as attacks that have been staged and not yet launched. Using it, we can effectively analyze and pinpoint where threats are coming from, who's launching them, their intended destination, the (potential) extent of the attack, and more.

10x daily traffic capacity

Umbrella's multi-terabit network, comprised of many high-capacity internet links, can sustain traffic load orders of magnitudes greater than daily peak usage. By continuously expanding capacity – adding circuits, termination equipment, and everything in between – our network remains at approximately ten times our current usage. This gives Umbrella the flexibility to handle surges, mitigate contention, manage transit, and fend off attacks on our network.

Micro services create cloud-native functions

We disaggregate functions of traditional appliances into micro services that we recreate into truly cloud-native functions. This bolsters Umbrella's ability to flexibly change functionality, rapidly scale up or down, and continuously optimize performance.

Automation allows us to see problems before they happen

Leading-edge automation spots potential problems, such as performance degradation, often before a customer would ever notice. Using a wide variety of data sources and a plethora of internal insights, we rigorously monitor our environment to inform path optimization and peering relationships, all to proactively defend and secure our customers.

Internet intelligence at scale

ThousandEyes, a recent Cisco acquisition, adds a personalized monitoring viewpoint capability and the flexibility to correlate multiple telemetry sources. This deepens our knowledge of global cloud architecture status at any time, warning when a user's experience is less than ideal and pinpointing where a failure occurs.

Resilience and reliability to ensure continued operations

When your business runs in the cloud, the infrastructure supporting that business must be reliable and resilient, regardless of what's going on at 3 am.

Optimizing our hybrid multi-cloud infrastructure

We own, actively manage, and tune our own equipment, enabling us to maximize performance and resilience by adjusting the controls necessary to maintain consistent high performance. Additionally, we selectively use public cloud providers and build our services as multi-region for the greatest resilience. By doing both, we can granularly manage to rigorous performance standards, architect for high reliability, and rapidly scale up or down as required.

Meet or exceed security & uptime standards

Cisco Umbrella data centers meet or exceed industry standards for security and uptime, such as Uptime Institute Tier III standards, ISO27001, and SOC2. They also adhere to Cisco's stringent requirements for network connectivity, security, quality, and effective risk controls, all of which help Umbrella satisfy the General Data Protection Regulation (GDPR) requirements.

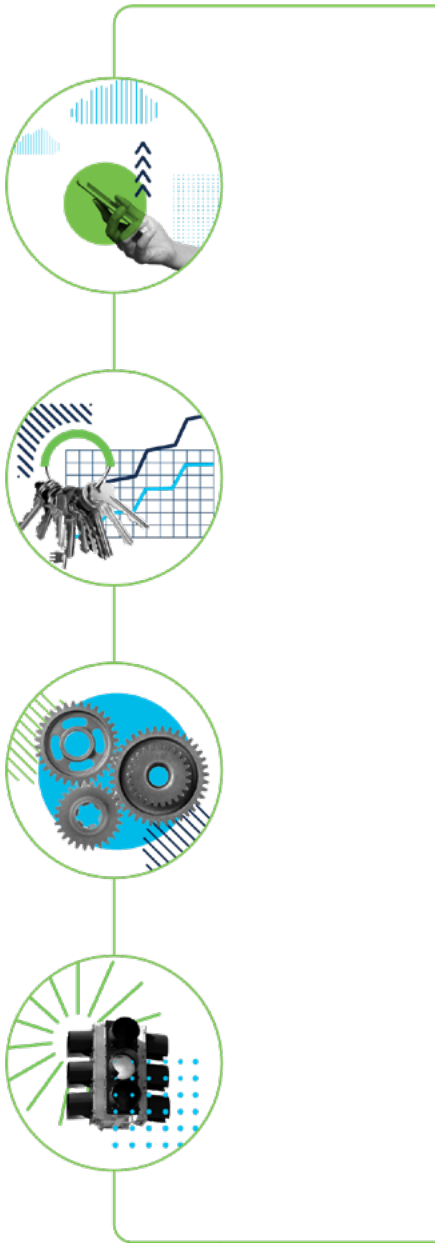
Complete transparency

Cisco is committed to providing our customers with complete transparency. We regularly publish a snapshot of our current cloud security service status and operational notices.

Augmented routing: our innovative use of Anycast

Anycast routing is like an automated assistant, providing the best possible availability, reliability, and quality, without the need to manage load balancers, configuration files, or routing policies. Augmented routing allows us to automatically route traffic via the shortest path for every connection, circumventing degraded or unavailable links without customer intervention. Umbrella announces the same IP address ranges from all data center locations globally and uses the internet routing system to connect users to the closest data center via the fewest network hops.

Automation built into the transit management function continuously monitors connections, watching for potential quality degradation and facilitating rapid response if anything unusual is detected. This happens in the background at all times, typically without customer knowledge or involvement.



Automatic data center failover

As with routing, data center failover happens without customer intervention. Whether due to planned maintenance or unplanned interruptions, failover is seamless and transparent, and redundancy is maintained.

Umbrella has delivered 100% business uptime in its DNS security service since its 2006 inception by leveraging Anycast routing (and innovative extensions). And because Umbrella SIG Essentials/Advantage run on this foundation, it possesses the same qualities and benefits.

The following scenario (figure1) illustrates Umbrella's use of Anycast routing. A customer request to an IP address in the Umbrella cloud can be responded to by any Umbrella data center – not just one. If a customer's Umbrella data center (Atlanta) goes off-line for maintenance or an unexpected failure, the customer is connected to the next nearest Umbrella data center, as measured by the fewest network hops. This failover happens automatically, without customer intervention.

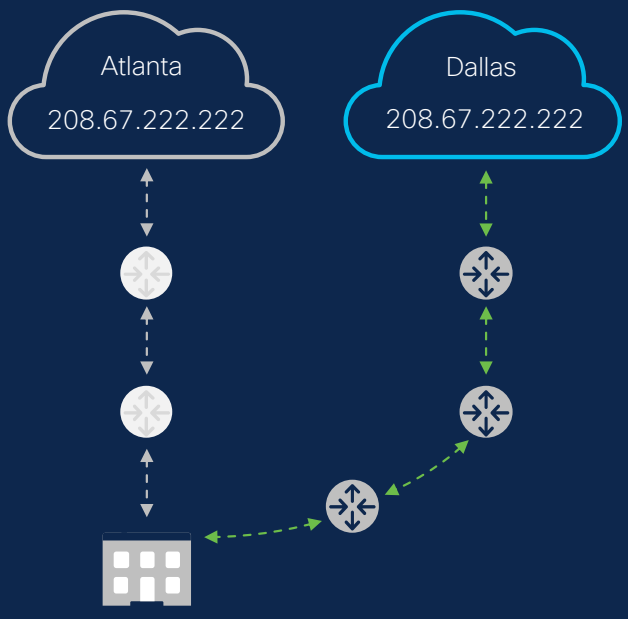


Figure 1

Multiple peering relationships improve resilience and routing

Umbrella's 1000+ peering relationships play a vital role in our ability to maintain resilience and augmented routing (through Anycast). Learn more about Umbrella's extensive peering relationships in the section, "High performance through Umbrella's global peering relationships."

Example

Augmented routing in action

Let's explore how Umbrella's combination of peering and Anycast create a resilient architecture. The customer is in Miami, served by a regional Internet Service Provider (ISP) that has a peering relationship with Umbrella and connections to two tier 1 transit providers, Provider A and Provider B (see figure 2).

User traffic flows to the Umbrella Miami data center, routed over the peered path between the ISP and Umbrella (the green line in figure 2). This peered connection delivers a shorter autonomous system path, saving the customer and the ISP money and typically resulting in a faster round trip for the data.

Umbrella maintains peering with local regional ISPs and connections with two or three transit providers at each location, providing multiple paths for traffic to get to Umbrella. If something disables the peering connection, traffic automatically moves to an alternative transit path. Like an effective highway detour, traffic continues to the destination, and the user's experience is unaffected.

What happens if the disruption isn't temporary?

Let's say a hurricane knocks out power in Miami. Backup generators in Umbrella data centers prevent sudden failures but prolonged power outages may necessitate data center shutdowns to protect from power spikes. In this situation, Umbrella's infrastructure automatically disconnects from the Miami route, and border gateway protocol (BGP) re-routes traffic to the closest alternative Umbrella data center, Dallas.

This is not a theoretical scenario. A large North American service provider suffered a major outage in the third quarter of 2020. Umbrella's infrastructure automatically alerted network operations teams, stopped using the affected links, and rerouted traffic via other service providers. This adjustment significantly reduced the impact to Umbrella customers, compared with organizations that were not using Umbrella.

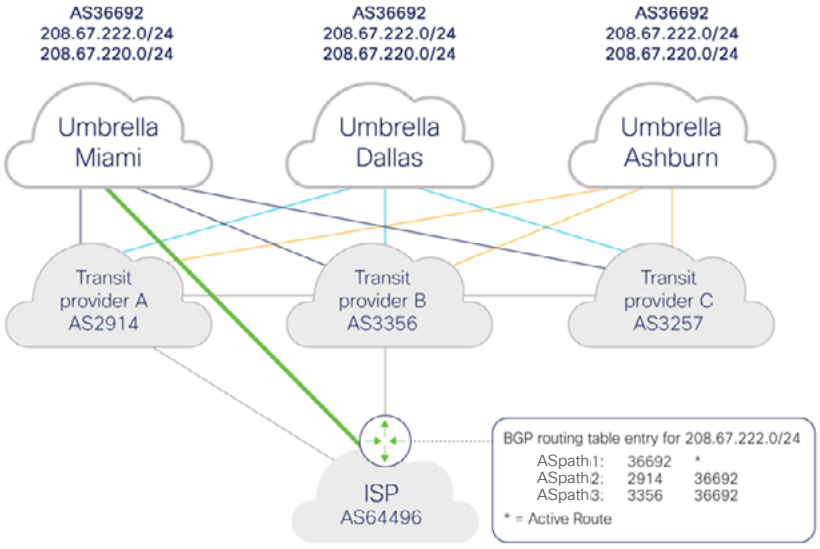


Figure 2

High performance through Umbrella's global peering relationships

Often, cloud security providers show customers a map with the quantity and distribution of their data centers. Based on that map, some customers incorrectly assume latency decreases when their security provider's data center is physically located near the ISP data center that serves the customer's network and devices. However, due to inadequate peering or transit relationships, the shortest path between the ISP and the vendor may actually require a large number of intermediate stops, resulting in a slower path between points, regardless of distance.

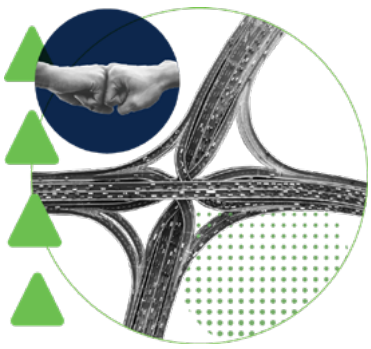
Peering matters. A lot.

Peering relationships between providers shorten the path that traffic travels between them, reducing the number of routing hops and improving performance. Umbrella's robust peering contributed to recent strong, positive performance results. In 2021, an independent performance testing company conducted a rigorous global performance evaluation. Traffic to key SaaS applications going through Umbrella with security protection was often faster than traffic going direct to internet without security protection (33%, 22%, and 21% faster for Box, AWS Console, and Salesforce, respectively). Factors include:

- 1000+ (and growing) high-quality peering connections and 6000+ peering sessions
- Peering with leading ISPs, cloud delivery networks, and SaaS and IaaS providers (see list below for examples)
- Locating data centers near Internet Exchange Points (IXP)
- Peering with Microsoft (customers expect fast Office 365 performance)

Umbrella establishes peering relationships to enhance performance and customer experience, not for cost savings to Cisco (as some security vendors do). By using settlement-free peering, where two networks agree to exchange traffic directly without compensation, we can better reinforce neutrality and ensure both parties act in their customers' best interests.

Examples of peering partnerships



Highlights

- AT&T (Global)
- Bell
- Bharti Airtel Limited
- BT
- Charter
- China Mobile
- Google Fiber
- KDDI
- Rogers
- Swisscom
- Telkom
- Verizon
- Vodafone

IaaS

- Alibaba
- Amazon
- Dell Services
- Digital Ocean
- Equinix
- Fastly
- Go Daddy
- Google
- Huawei Cloud
- Microsoft
- Rackspace

SaaS

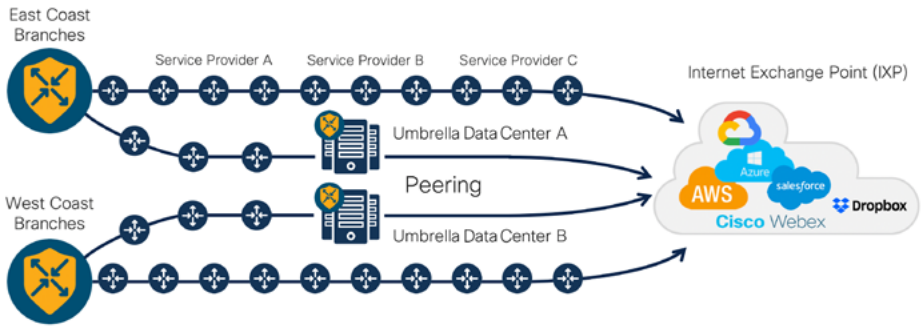
- Adobe
- Apple
- Baidu
- Box
- DocuSign
- Dropbox
- Microsoft
- NS1
- Oracle
- Salesforce
- Square
- Webex

*link to the report here

Co-location near top IXPs

Internet Exchange Points (IXPs) are physical locations where ISPs, CDNs, and other service providers connect with each other. By intentionally locating our data centers near IXPs, we easily expand the quantity and quality of our peering relationships. Using the sophisticated intelligence built into our global cloud architecture, Umbrella orchestrates connections that accelerate performance, monitor operation quality, and ultimately create an ecosystem of peered cloud service providers that brings Umbrella as close as possible to our customers.

Using settlement-free peering allows us to better enforce neutrality and ensure both parties act in the customers' best interests.



Peering with Microsoft improves Office 365 traffic

Umbrella maintains robust peering with Microsoft to ensure that an organization's Office 365 traffic remains lightning-fast. This partnership is managed from every Umbrella data center where Microsoft and Umbrella are both present at the IXP. If a customer chooses, they can run "compatibility mode" so that Office 365 traffic transparently passes through Umbrella without inspection but still benefits from the Umbrella global cloud architecture performance improvements.

Performance put to the test

An independent digital experience monitoring company evaluated the performance of worldwide traffic going through Cisco Umbrella as compared to traffic going directly through the internet, without security protection.

Cybersecurity services, by definition, inspect traffic for potential security threats and apply policy-based controls to identify and block harmful traffic. As such, it is generally expected that the performance of security-inspected traffic may be less favorable than if no inspection were done.

However, the evaluation showed that in many cases, the anticipated performance trade-off was not apparent with Cisco Umbrella.

Performance with Umbrella – even with secure web gateway (with decryption of HTTPS) and DNS policies applied – was often improved over direct to internet.

Highlights

- Traffic to Box was 33% faster through Umbrella than going direct to internet
- Traffic to the AWS console was 22% faster through Umbrella than going direct to internet
- Traffic to Salesforce was 21% faster through Umbrella than going direct to internet
- Umbrella was markedly more consistent, which denotes a more even and predictable customer experience

Agile infrastructure improves functionality without business downtime

The pace of change shows no signs of slowing in our 24/7 world. Umbrella's global cloud architecture helps our customers safely and reliably keep up with that change while continuing to eliminate customer disruptions.

Self-healing, highly automated, agile infrastructure

Our self-healing, highly automated, agile infrastructure is at the heart of our global cloud architecture. For more than 6 years — longer than any cloud security vendor — Umbrella has used containers to improve agility and enable rapid deployment of security capabilities.

With 30,000 worldwide production containers carrying security traffic at scale, our compute and network uses capabilities like global load balancer and auto scale to transparently resolve issues and devise work-arounds. This agile architecture enables us to continuously deliver new capabilities seamlessly to our customers, without business downtime. Servers, networks, and whole data centers can come in and out of rotation, with no effect on our customers' performance, network, or security.

Example

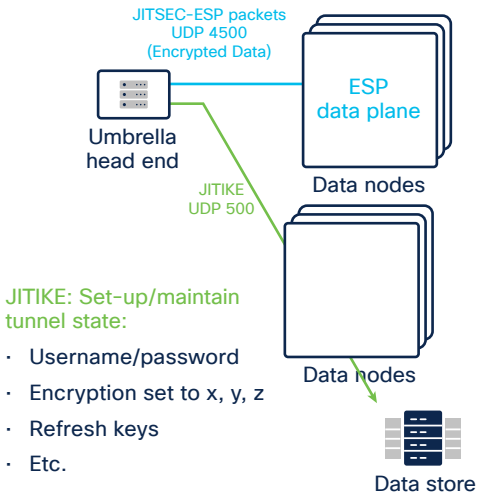
An Umbrella customer experience improvement

We've developed a way to simplify customer deployment and improve how we update Umbrella – at any time – without disrupting customer traffic.

Drawing from strongSwan open-source technology, we built something entirely new, decoupling the tunnel state internet key exchange (IKE) from the data flowing over the tunnel in encapsulating security protocol (ESP). To highlight the improvement, we created new terms: JITSEC and JITIKE (JIT is for "just in time").

This change enables us to use a single IP per data center. Storing the tunnel state separately means we can easily move the tunnel set up and its state definition within our data center while doing maintenance/upgrades to our infrastructure, as it is not tied to any specific hardware or data node.

This enables Umbrella to add new features/capabilities, perform maintenance, simplify customers' device configuration, and more – without disrupting customer traffic.



There's much more to Umbrella than meets the eye

As business moves to the cloud, pressure intensifies for the cloud architecture – the foundation upon which businesses running in the cloud operate – to continue to expand and provide capabilities never before seen.

Cisco's global cloud architecture is the essential unseen ingredient that provides Umbrella customers globally with industry-leading security protection as well as extraordinary flexibility, resilience, performance, and agility.

If you are not yet using Cisco Umbrella, why not discover what more than 24,000 enterprise customers have already learned – that the proven performance of Cisco's global cloud architecture ensures your business stays in business, secure and connected?

To learn more about Cisco Umbrella, join a live webinar.

Sources

1. *2021 State of the Cloud Report*, Flexera, 2021.
2. *Gartner Survey Reveals 82% of Employees to Work Remotely Some of the Time*, Gartner, 2020.
3. *The modern cybersecurity landscape: scaling for threats in motion*, Cisco, 2020.

Instead of buying point solutions or looking for a security vendor to meet your current needs, Gartner recommends finding a partner based on their:

Long-term vision

Ability to grow with your needs

Capability to accelerate your move to the cloud