Discover Unified Communications and Collaboration as a Service.

Maintaining security, availability, and reliability in the private cloud.

verizon

White Paper

The proven power of private and dedicated cloud services.

More and more, enterprise organizations around the world are turning to managed network and cloud servies. They can reduce capital expenses and control operational expenses (CAPEX and OPEX), enhance workforce productivity, increase agility, make costs more predictable, and simplify operations throughout the application life cycle. Today's managed cloud-based services deliver high reliability, availability, and security—which are all traditional, core attributes of carrier-class service provider infrastructures. But not all cloud services are alike. Public cloud services can be vulnerable to Internet intrusions.

Private and dedicated cloud services are available from service providers to individual organizations, and they're secure and reliable due to a variety of factors:

- A defense-in-depth security strategy with overlapping layers of protection
- The use of a customer-specific virtual routing and forwarding (VRF) environment, allowing each customer to have their own unique instance of an application that is not shared
- Firewalls to control traffic as it travels to and from private cloud services and to protect against threats from inside or outside an enterprise
- Use of purpose-built management systems, as well as syslogs for system monitoring and management, security auditing, and generalized informational analysis, debugging, and troubleshooting, to remediate failures and help reduce downtime
- The ability for customers to assign addresses utilized behind the cloud-based firewall to create a "demilitarized zone" (DMZ) for the service

More businesses are using cloud services.

The popularity of cloud services is driving massive increases in data center and network traffic, with global data center traffic expected to grow three-fold from 2012 to 2017. It will reach 7.7 zettabytes a year in 2017 according to the *Cisco® Global Cloud Index: Forecast and Methodology, 2012–2017*.

The same study predicts that by 2017, nearly two out of three data center workloads will be processed in the cloud (See Figure 1, Page 3), resulting in a compound annual growth rate (CAGR) of 30 percent.

The *IDC Worldwide Managed Network Services 2012–2017 Forecast*[1] predicts global cloud services revenue will grow at a CAGR of 9.5 percent, expanding from $64.8 billion in 2012 to $101.8 billion by 2017. A May 2012 IDC Black Book study forecasts that cloud infrastructure and services will comprise nearly 30 percent of all IT expenditures by 2020 and the total addressable market will grow to $777 billion by that time, as compared to $81 billion in 2011.

In 2013, Cisco averaged cloud market forecasts for 2015 from Forrester, IDC, Ovum, Gartner, and Mason, and the result was $66 billion spent on cloud services by 2015 (compared to $22 billion in 2011).[2] This underscores the confidence most organizations now have in the integrity of cloud services.

> **Analysts estimate that $66 billion will be spent on cloud services in 2015 (compared to $22 billion in 2011).**

The combination of private, hosted, and managed cloud services with unified communications and collaboration services can reduce or eliminate the need to install, maintain, and upgrade on-site PBX equipment and applications. Each customer is provided with dedicated, virtual instances of each application, including software and hardware redundancy and availability.

Beyond the cost and operational benefits, private, hosted, and managed unified communications help organizations increase teamwork and productivity, improve speed to market, enhance business process flexibility, increase customer satisfaction, and reduce travel expenses. The overall value is further increased by the ability to deliver unified communications applications (including presence, IP voice, instant messaging, desktop and web conferencing, and collaboration workspaces) to both fixed and mobile clients.

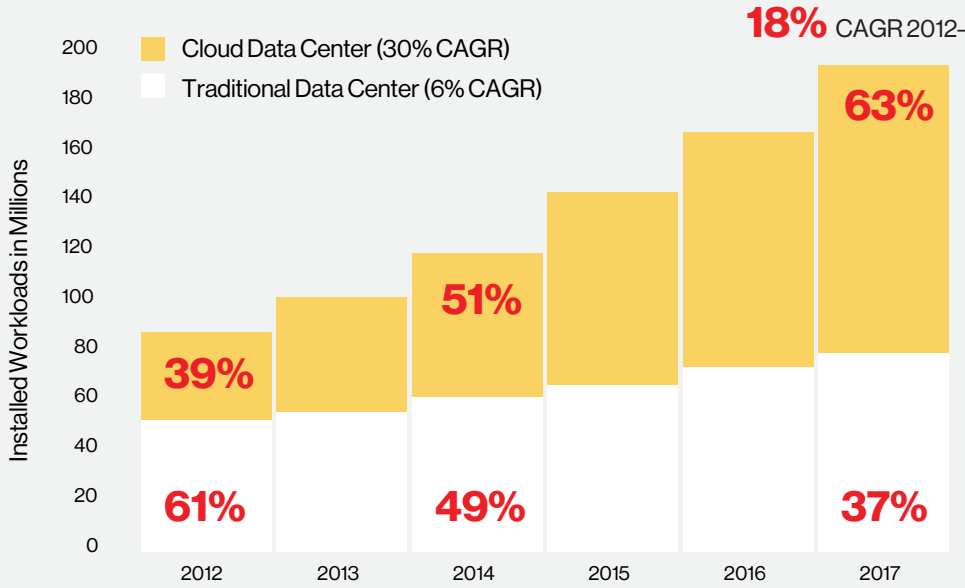
When it comes to private, hosted, and managed cloud environments, there are various approaches to security, reliability, and availability—some far superior to others. This is especially true for unified communications, where information confidentiality may be required and where the absence of reliable, available services may lead to the failure of business operations.

Challenges in maximizing security, availability, and reliability.

In an era when business happens in an instant, the confidentiality of trade secrets, sales, and customer information is especially vital—as are communications between employees, customers, partners, and suppliers. Strategic advantage can be won or lost based on the availability and security of information. And reliable unified communications and collaboration services and information can often form the basis of entirely new business models.

Services provided over the Internet and public clouds, moving from large colocation data centers to insecure fixed and mobile devices, generally lack the rigid security and reliability of enterprise network and private cloud services. For enterprise unified communications and collaboration, these shortcomings are simply unacceptable.

By contrast, world-class, private, hosted, and managed cloud services incorporate proven industry best practices, architectures, platforms, and technologies—and they adhere to enterprise data center standards. These services also enable many new features based on virtualization and other more recent innovations.



Source: *Cisco Global Cloud Index: Forecast and Methodology, 2012–2017*

Figure 1. Growth of cloud workloads

Private IP and UCCaaS.

Verizon's Global Private IP Service infrastructure is a private, hosted, and managed cloud-services environment that offers a carrier-class approach to the most mission-critical enterprise business services. Customers obtain services via a Layer 3 MultiProtocol Label Switching (MPLS) VPN. They get the security and quality of service (QoS) of older ATM and frame relay, the flexibility and scalability of IP, and the convergence of voice, data, and video applications over an integrated network infrastructure (See Figure 2, Page 4).

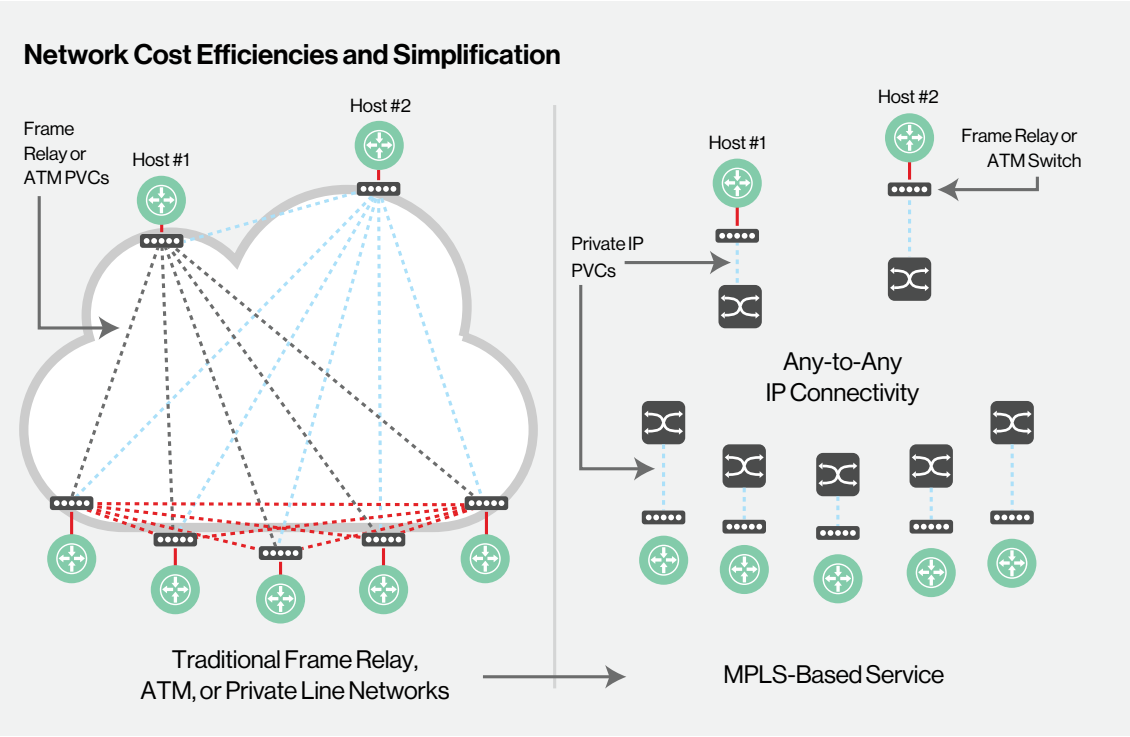


Figure 2. Verizon Private IP service: converged services over IP

Verizon Unified Communications and Collaboration as a Service (UCCaaS) provides an extensive roster of unified communications and collaboration applications to users in varied work environments and scenarios, packaging the entire suite of Cisco Hosted Collaboration Solution applications into a single user license. The package includes client and server software access rights, service and support, and software upgrades. The solution is based on Cisco Unified Communications Manager and VMware vSphere Hypervisor for virtualization.

Applications.

Cisco Unified Communications Manager: Delivers call control, voice services, and plug-and-play provisioning of IP phone features.

Cisco Unity Connection: Provides voice messaging features and services. These include web voicemail and Internet Message Access Protocol (IMAP) integration for Microsoft® Outlook® and Cisco Jabber.® Cisco Jabber provides a single interface across presence, instant messaging (IM), voice, video, voice messaging, desktop sharing, and conferencing.

Cisco Jabber Desktop Client: Allows customers to bring together all their communication applications in a single, easy-to-use interface for PC or Apple® Mac.® Users can stay connected virtually anywhere they are and can quickly find people they need to reach. Jabber brings secure soft-phone capabilities, presence, IM, visual voicemail, video, and web conferencing to the desktop.

Cisco Jabber Mobile Client: Extends communication and collaboration capabilities to the smartphone or tablet, providing remote or mobile workers the ability to connect and collaborate across any network and via preferred devices.

Verizon Audio and Net Conferencing: Offers users a virtual meeting room, allowing them to collaborate instantly or schedule events in advance.

Key differentiators.

Multi-customer versus multi-tenant computing infrastructure: Multi-tenant computing infrastructures feature a single set of applications in one IP address space on a server, which then supports multiple different customers. By contrast, the multi-customer infrastructure behind UCCaaS provides each

customer with dedicated, virtual instances of each individual application through the use of virtualization technology.

This completely isolates each instance of software from every other instance. Applications run in their own address spaces, with dedicated server processing provided to each customer. There is no routing between VRFs and individual instances of firewalls at the edge of the network, which enables customers to set up their own filter rules. Data stores on the storage area network (SAN) feature a logical unit number (LUN) dedicated to each separate customer. The multi-customer environment allows customers to enjoy the benefits of dedicated software while taking advantage of shared hardware, with carrier-class security, flexibility, and resiliency.

Defense-in-depth security model: This industry-proven best practice features multiple layers of security and different security techniques that provide overlap protection in the event that one layer, technique, or component fails (Figure 3). UCCaaS utilizes a variety of technologies and techniques to protect the core network and customer networks. This includes the use of stateful and redundant firewalls, Deep Packet Inspection (DPI), individual server and component hardening, and physical security at Verizon data centers.

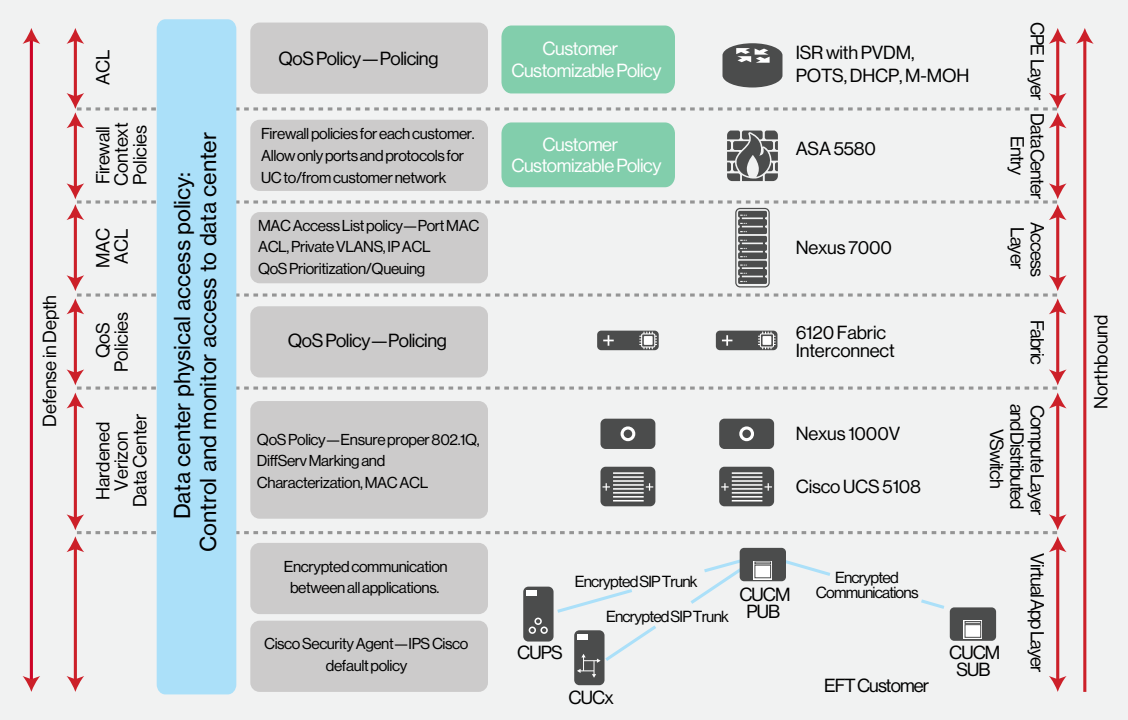


Figure 3. Defense-in-depth security layers and corresponding Cisco platforms

Security, availability, and reliability features at each network layer.

Customer premises equipment (CPE) and access security: This focuses on the PCs, phones, media players, gateways, routers, and other devices that connect to the network. The devices themselves have the ability to encrypt data, voice, or video traffic, but this can become resource-intensive.

Instead, separate virtual LANs (VLANs) for voice and data with QoS and the use of access control lists (ACLs) help ensure that only endpoints are permitted to communicate to on-premises service routers and media routers. Security features help protect Voice over IP (VoIP) devices that must interconnect with the public switched telephone network (PSTN).

Switch ports must be protected from Media Access Control (MAC) content-addressable memory flooding attacks, where the switch is flooded with so many MAC addresses that it

cannot determine which port an end station or device is attached to. In this case, it broadcasts the traffic to the entire VLAN and the attacker is able to see all traffic coming to all the users in the VLAN. Security tools limit the number of MAC addresses allowed to access individual ports, based on the connectivity requirements for those ports.

The firewall is an important best practice, protecting the unified communications services from attack from the customer's enterprise environment.

Phones on the network are also vulnerable to data attacks. Gratuitous Address Resolution Protocol (GARP) on the phones helps to prevent man-in-the-middle (MITM) attacks involving an attacker who tricks an end station into believing that he or she is the router and tricks the router into believing that he or she is the end station. This scheme makes all the traffic between the router and the end station travel through the attacker, thus enabling the attacker to log all of the traffic or inject new traffic into the data conversation. GARP on an IP phone protects against an attacker's ability to capture the signaling and RTP voice streams from the phone.

Other access security measures include:
Port security: It is important to prevent access to all switch ports. An exception is those devices allowed to connect to the port via their MAC addresses. This form of device-level security authorization enables a network administrator to authorize access to the network by using MAC addresses as device credentials.

Dynamic Host Configuration Protocol (DHCP) snooping: When enabled, this feature treats all ports in a VLAN as untrusted by default and prevents a nonapproved DHCP or rogue DHCP server from handing out IP addresses on a network by blocking all replies to a DHCP request unless that port is allowed to reply.

Dynamic ARP Inspection (DAI): This feature is used on the switch to help prevent GARP attacks on the devices plugged into the switch and on the router. Here the GARP feature prevents all devices on the LAN, not just IP phones.

IEEE 802.1X port-based authentication: Used to identify and validate the device credentials of an IP phone before granting it access to the network, the 802.1X feature is a MAC-layer protocol that interacts between an end device and a RADIUS server. It encapsulates the Extensible Authentication Protocol (EAP) over LAN to transport the authentication messages between the end devices and the switch.

Phone authentication and encryption: Cisco Unified Communications Manager can be configured to provide multiple levels of security to phones within a voice system, including device authentication plus media and signaling encryption using X.509 certificates.

A virtualized instance of a data center firewall: Deployed between the customer's VRF instance of their applications and the applications themselves, this provides an access control and monitoring point to the unified communications and collaboration applications.

Additional levels of security for network protection.

It also helps prevent denial-of-service (DoS) attacks and polices access from the voice and data VLANs based on the customer's application environment and policies. With UCCaaS, customers have access to data via syslog, which can be used in place of security log gathering. Firewall rules may be customized to meet customer security practices that may already be in place. (Note: Customers may customize their firewall policies for firewalls that extend and further harden their security posture but Verizon's baseline security policy cannot be modified.)

The fabric interconnect to the SAN: The ports and backplane used to communicate between VM instances and the SAN is segmented like the virtual LANs that carry voice and data, and

distributed switching further isolates customer traffic. While cloud services that provide infrastructure-as-a-service (IaaS), such as Amazon's Elastic Compute Cloud (EC2), are transactional, bursty services, UCCaaS carries voice and video traffic and is sensitive to even a few seconds of latency, since this will cause parties in a phone conversation to hang up. UCCaaS utilizes QoS features to protect against latency while also serving to protect against a DoS attack.

Distributed switching architecture: Isolates customer data in the Verizon data centers, with each customer VRF extended through the switched architecture. Redundant switching infrastructure helps prevent a single point of failure from disrupting service. Verizon uses extended features of Cisco Nexus 1000V switches to extend QoS features inside the virtual distributed switch environment to correctly prioritize signaling and media from end to end.

Within the servers that run the VMs: At the compute layer, CPU cores are dedicated to specific customers for the separation of applications and data. Multiple servers are supported by different processors to enable fail-over.

At the application layer: The virtual Linux environment has been hardened. All unnecessary services and ports have been disabled. The OS is not accessible to the customer. The applications are only accessible through the management applications portal. The entire application environment is also monitored and logged.

Physical security: For the UCCaaS environment at Tier 1 Verizon data centers, physical security includes multiple layers of physical isolation, requiring a combination of biometric scans, an ID card, and ticket/notification to enable access and work on data center infrastructure. All servers and network components are protected by a two-form-factor access method to restrict and actively control access to components. Additionally, the data centers do not have direct Internet access—only dedicated interconnects to the individual customers. This provides isolation of the UCCaaS core and protects customers by isolating their network from the Internet.

The UCCaaS architecture provides scalability for even the largest enterprises by utilizing a multi-customer computing infrastructure and defense-in-depth security with geo-redundancy, an application availability SLA of 100 percent, three fault-tolerance features, and a service provisioning methodology.

UCCaaS business benefits.

Solutions such as UCCaaS provide an array of measurable benefits for the enterprise user, impacting individual productivity and the organization's bottom line. These include:

Fast time-to-value through rapid deployment: UCCaaS is ready for adoption immediately, enabling collaboration in real time with a broad set of individuals across multiple locations. UCCaaS can save time over do-it-yourself PBX deployments. The service is customizable for employees and does not require a large capital investment, making it an excellent low-risk alternative to rolling out new technology solutions. Easy integration of existing services reduces the complexity and time frame required for deploying a hybrid model.

The UCCaaS architecture provides scalability for even the largest enterprises.

Extensibility: UCCaaS integrates into enterprise software fabric—enterprise resource planning (ERP), customer relationship management (CRM), and custom applications. It integrates with and delivers desktop and immersive video, and is able to grow to meet your organization's changing needs.

Better cost control through the reduction of capital outlays for communications solutions: With UCCaaS, companies can move to a predictable monthly cost that can be scaled

up or down based on business cycles. As a service instead of a product, UCCaaS helps protect companies from technology obsolescence and allows IT to focus their resources on more strategic projects.

High reliability: For more predictable business operations, based on carrier-class availability, management, monitoring, and multi-layered security.

A clear value for today's enterprises.

Service providers who use the private, hosted, and managed network cloud for their offerings are including additional benefits. They're incorporating stringent security, availability, and reliability features developed over decades in the most sophisticated enterprise environments and Tier 1 data centers.

Computing architectures utilizing virtualization and based on multi-customer instead of multi-tenant infrastructure provide software and information isolation for each enterprise deployment. The defense-in-depth security strategy protects bare metal and virtualized assets, embedding security throughout all layers of the network to maintain the confidentiality, integrity, and availability of data, applications, endpoints, and the network itself.

UCCaaS is a carrier-class offering that provides these features to enterprises through numerous individual technologies, platforms, and devices delivered through Private IP network connectivity. Beyond providing an array of CAPEX and OPEX benefits, it is easily and flexibly deployed and swiftly brings demonstrable benefits from the use of unified communications and collaboration services by fixed and mobile assets in today's enterprises.

Learn more.

For more information, including service availability at your enterprise locations, please contact your account representative or visit: **verizonenterprise.com/us/products/advanced-communications/** or **verizonciscocollaboration.com**

Verizon Private IP Service:
verizonenterprise.com/products/networking/private-ip/

Cisco Unified Communications Manager Security Guide:
cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/9_1_1/secugd/CUCM_BK_C0395F44_00_cucm-scurity-guide-91.html

Cisco Unified Communications System Solution Reference Network Design:
cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab09/clb09.html

verizonenterprise.com

1 IDC, *Worldwide Managed Network Services 2013–2017 Forecast*, May 2013.

2 *VNI Global IP Traffic Forecast, 2013 – 2018*, Cisco, 2014. http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html

3 SLA available for UCCaaS applications with geographic redundancy. Both Verizon-approved UCCaaS architectures and Private IP transport service required. SLA may not be available in all locations outside the U.S. Terms & conditions apply; see your Verizon account manager for details.