Cisco Virtualization Experience Infrastructure: Unify Virtual Desktops, Voice, and Video for the New Virtual Workspace

What You Will Learn

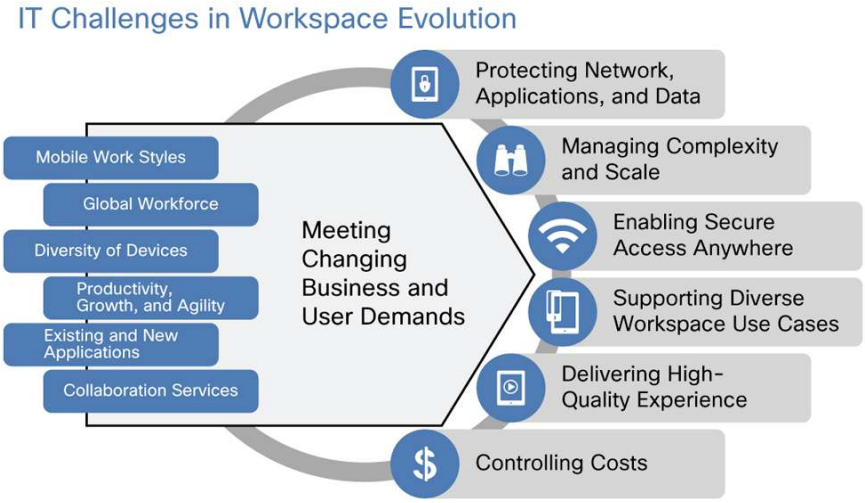
The modern workplace continues to evolve, with user mobility more prevalent than ever and still increasing; the introduction of consumer products and bring-your-own-device (BYOD) initiatives into the workforce; and the never-waning priorities of productivity, data protection, and security. To address these needs and support the initiatives of the organization, IT must consider end user computing and communications, and their supporting architectures and infrastructure, in a new and broader way. IT must provide an end-to-end solution that satisfies and balances the evolving and sometimes contradictory needs of the organization, IT, and end users. The Cisco® Unified Workspace addresses the diverse use cases that different organizations and workgroups require through either native or virtual workspace delivery and management models. This solution overview focuses on the benefits of the virtual model and describes the Cisco Virtualization Experience Infrastructure (VXI) Smart Solution that unifies virtual desktops, voice, and video to deliver the new virtual workspace.

The Evolving Workplace

Today's IT departments face a rapidly evolving workplace. The workforce is diverse and geographically dispersed, including knowledge and task workers, executives, partners, consultants, offshore contractors, and distributed call center operations, connecting from locations around the world at all times. This workforce is also increasingly mobile, conducting business in traditional offices, conference rooms, customer and partner locations, home offices, on the road, in shared workplaces, and in local coffee shops.

The modern workforce wants to use a growing array of devices that is chosen based on personal preference, location, and activity: smartphones, tablets, ultrabooks, personal laptop computers, etc. This shift increases pressure on IT to provide secure network access and a positive user experience on both company-managed and employee-owned devices while helping ensure protection of corporate data. These challenges are compounded by the many combinations of user types, existing and emerging applications, communications and collaboration needs, diverse endpoint devices, and operating systems. IT must meet these new workspace requirements while managing the associated complexity and costs (Figure 1).

Figure 1. IT Challenges in the Evolving Workplace

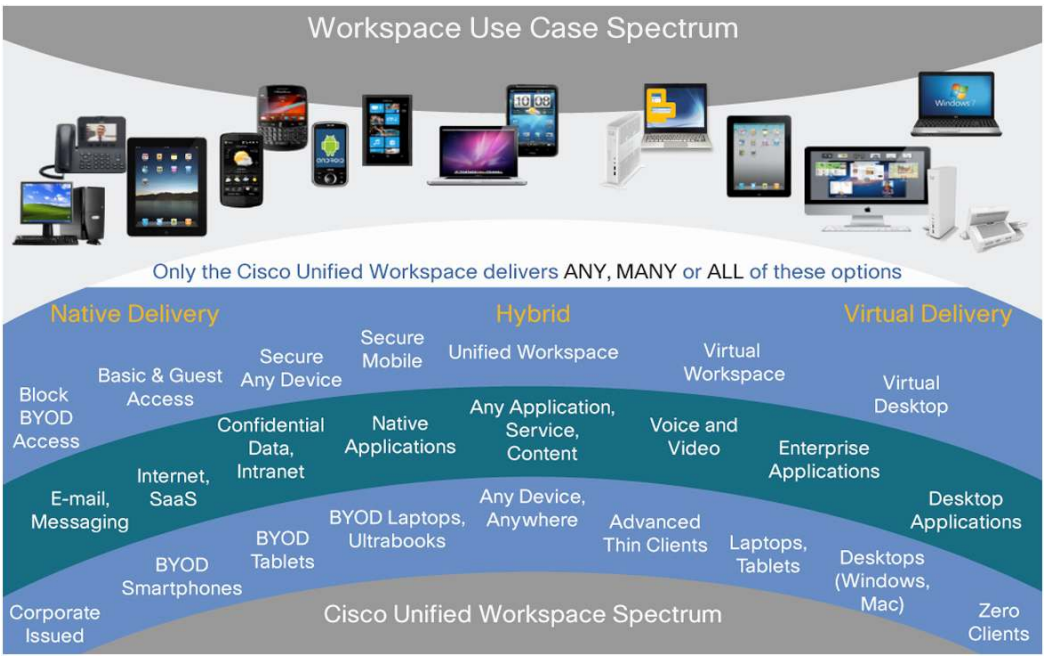


The New Unified Workspace

To manage the needs of the organization and the diverse device and work style requirements of end users, many IT departments are evolving their end user computing strategies. IT must consider security; data protection; mobility; desktop, application and communications access; and user experience. IT also must address a mix of use cases supporting corporate-owned and BYOD devices with various operating systems on fixed and mobile devices, both on and off premises. IT must look beyond the traditional desktop - applications and data tethered to an operating system and hardware - and adopt the new “unified workspace” that provides workers with appropriate access to all applications, data, and communications services, liberated from the confines of any single physical device or location.

IT can transform these challenges into an opportunity by designing a flexible unified workspace architecture that addresses the immediate use cases as well as future workspace requirements. To address diverse use cases, IT will often take a combination of virtual and native approaches to delivery of applications, content, and communications services to users. With the native delivery model applications and data reside on the devices themselves, and with the virtual delivery model, the desktop, applications, and data are centrally hosted and secured in the enterprise data center or cloud (Figure 2).

Figure 2. Unified Workspace Spectrum: Supporting a Diverse Set of Workspace Use Cases - Delivered Natively, Virtualized, or Unified

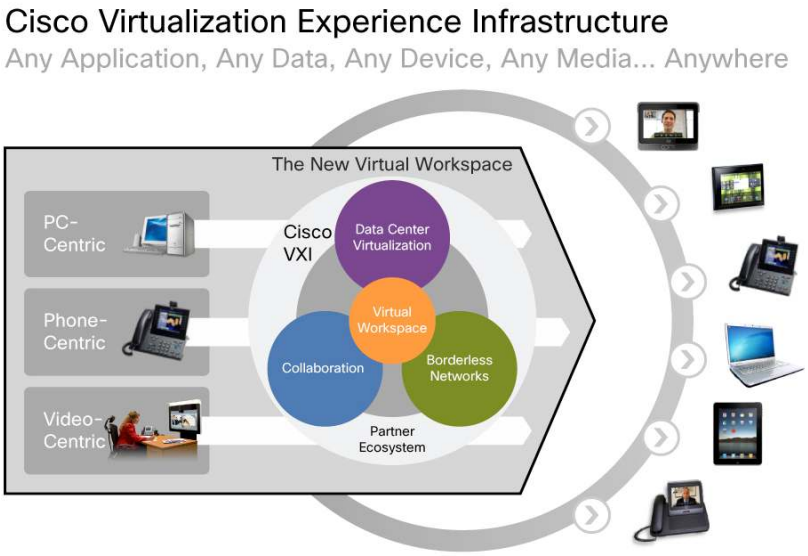


Both delivery models have complexity, cost, and capability implications. However, many organizations that need to provide a near-native user experience while tightly managing security and total cost of ownership (TCO) are considering or have already begun implementing virtual desktop and application delivery models. Desktop virtualization has been around awhile, but only recently have organizations begun to deploy it on a broad basis and across a variety of user profiles. Although desktop virtualization provides benefits on the IT side of the house, end user enthusiasm has lagged. End users have been hesitant to give up the experience and access that a fully functioning desktop or laptop provides. In addition, these same users are now demanding access to applications and data from a variety of devices, including smartphones and tablets of their own.

Fortunately for IT, end users, and the organization, desktop virtualization has come a long way and can, in some cases, provide a near-native end user experience on almost any device, while at the same time providing increased control and security, and lower TCO. But today's workforce is connected in ways beyond the traditional desktop, with mobile devices and collaborative applications, and most desktop virtualization solutions struggle to deliver a comparable end user experience. End users use the traditional desktop computing environment and integrated collaboration and multimedia applications. These users need connectivity and performance that includes not only the desktop computing environment, but also voice and video. IT must develop a strategy that helps the organization move from physical PC- and phone-centric work environments to a virtualized delivery model in which applications, content, and communications services can be delivered at anytime, anywhere, on any device.

Cisco identified this need and developed an architecture and a set of solutions that goes beyond traditional desktop virtualization, integrating virtual desktops, voice, and video into Cisco VXI. Cisco VXI combines Cisco's expertise and innovation across data center, networking, and collaboration technologies to deliver desktop virtualization, the virtual workspace, and the unified workspace (Figure 3).

Figure 3. Cisco VXI Enables Virtualized and Unified Workspaces by Integrating Virtual Desktops, Voice, and Video Across Data Center, Network, and Collaboration Architectures



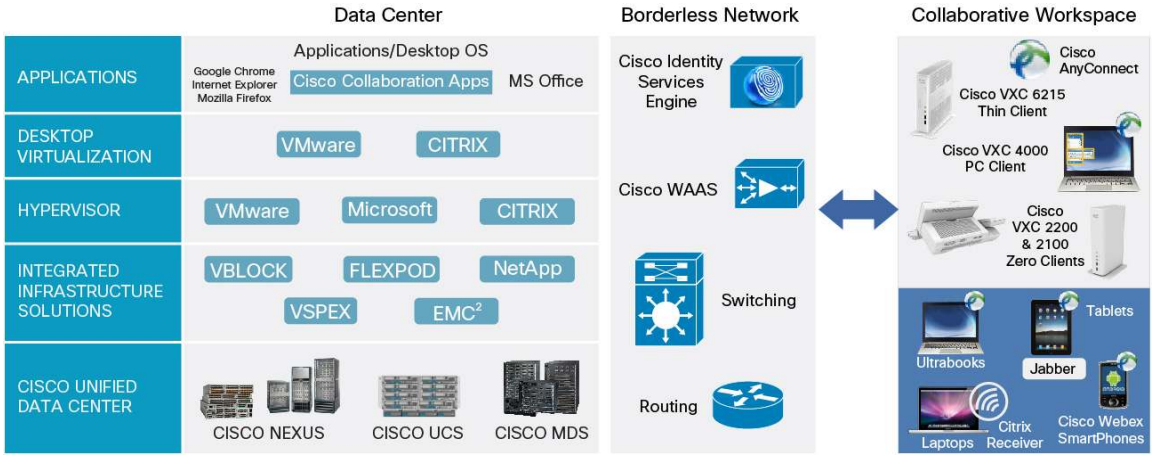
For many use cases, the solution must go beyond traditional desktop computing and desktop virtualization and consider the complete workspace. Solutions must include secure support for both corporate-owned fixed and mobile devices and BYOD endpoints, as well as integrated voice and video capabilities, including IP telephony, unified communications, collaboration platforms, and significant use of multimedia. An integrated, validated, end-to-end hardware and software architecture is required to deliver the new virtual workspace, from the data center through the network to the endpoints.

Delivering the New Virtual Workspace: The Benefits of Cisco VXI

Cisco VXI is a holistic solution, providing desktop virtualization, virtual workspaces, unified workspaces, or any combination thereof, that delivers virtual desktops, voice, and video services anywhere and on any device. Cisco VXI provides security, scalability, flexibility, and an uncompromised user and IT experience. Workspaces can be delivered to corporate-owned and user-owned devices and as part of BYOD initiatives.

The core of Cisco VXI is the highly scalable Cisco Unified Data Center, which includes the Cisco Unified Computing System™ (Cisco UCS™), Cisco Unified Management, and Cisco Unified Fabric, which centrally and securely hosts virtual desktops and applications, and dramatically simplifies deployment and management. The user workspace connects to centrally hosted virtual desktops through a secure, virtualization-aware network infrastructure optimized to deliver virtual desktop, communications, and collaboration services, based on the Cisco Borderless Network Architecture. The virtualized collaborative workspace, built on the Cisco Collaboration Architecture and portfolio, extends the reach of the virtual desktop to a diverse range of media and communications-capable endpoints, such as thin clients, zero clients, smartphones, tablets, and innovative Cisco Virtualization Experience Client (VXC) endpoints, which combine virtual desktops with voice and video capabilities (Figure 4).

Figure 4. Cisco VXI Infrastructure

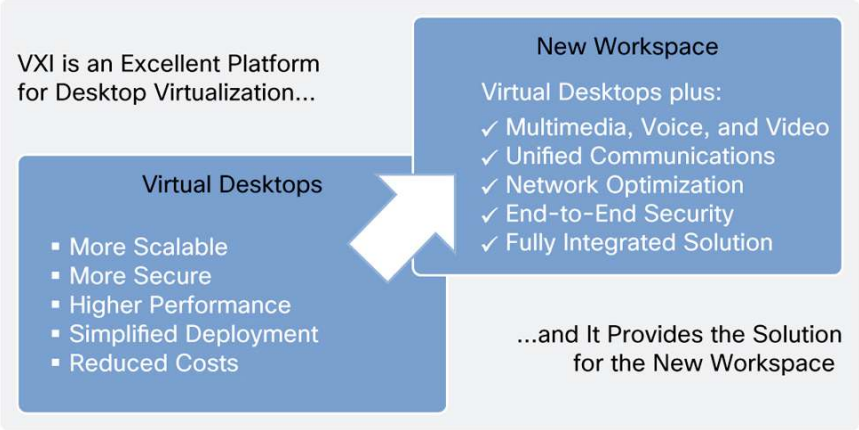


Cisco works with an industry-leading ecosystem of partners, including Citrix, VMware, NetApp, and EMC, to provide tested and validated Cisco VXI solutions that deliver:

- A validated end-to-end system and a roadmap that enables customers to evolve from virtual desktops to virtual workspaces to unified workspaces
- Advanced data center fabric and computing platforms optimized for virtualization, with the highest density of virtual machines per server blade
- Superior network optimization, providing secure virtual desktop, voice, and video delivery alongside traditional traffic types
- Multimedia capabilities and innovative endpoints that meet the productivity and collaboration needs of diverse end users: from task workers to mobile and remote knowledge workers
- Support for both company- and user-owned devices

The Cisco VXI architecture provides an excellent platform for traditional desktop virtualization as well as the new virtual workspace. Desktop virtualization on Cisco Unified Data Center and Borderless Networks architectures is more scalable and secure and delivers higher performance, simplified deployment, and reduced costs compared to other architectures. In addition, Cisco VXI goes beyond traditional desktop virtualization, providing the only integrated and optimized multimedia, voice, and video solution that considers the complete workspace: computing, communications, and collaboration (Figure 5).

Figure 5. Cisco VXI - Ideal for Desktop Virtualization and the New Virtual Workspace



Cisco VXI is a service-optimized, virtual workspace platform that offers a secure, flexible, and uncompromised solution. Cisco VXI provides benefits for the entire organization:

- For end users, with a high quality user experience on any device from anywhere
- For IT, with a scalable and secure infrastructure to deliver IT as a service (ITaaS)
- For the organization, with improved agility and productivity with lower operating costs

Cisco VXI provides benefits for a broad variety of organizations (Figure 6) and for many different user types, including:

- Field teams that need a mobile workspace with secure access to data, applications, and communications while at the office, in branch offices, engaging with customers, and on the road
- Remote and branch-office users who need access from their personal office spaces or shared flex-office spaces to the intranet, collaboration and enterprise systems, and shared resources
- Teleworkers who need the same access at home as in the office to applications, desktops, and collaboration tools
- Knowledge workers who need nonstop access to their desktops, enterprise applications, and communications from a broad set of locations
- Campus and conference-room professionals who need portable voice, video, and data; onsite mobility is important to many workgroup types
- Temporary workers, contractors, and partners who need access from campus or their own offices to many of the same systems as permanent staff

Figure 6. Cisco VXI Provides Benefits Across Many Industries and Segments

Customers such as Metro Health and Park Hill School District have seen the benefits of Cisco VXI first hand:

- Metro Health in Grand Rapids, Michigan, reduced capital expenses by 30 percent, streamlined clinical workflows, and provided physicians with ubiquitous access to dictation, follow-me desktops, and referential images.

  “We wanted to extend our systems out to a variety of form factors and locations to really advance our anytime, anywhere access to patient information.” - Bill Lewkowski, CIO and executive vice president, Metro Health.

- Park Hill School District in Kansas City, Missouri, who can now add approved desktops to servers and easily deploy specific software applications, has improved desktop management and security, and is providing faster response times to students, teachers, and faculty to help meet educational and administrative needs.

  “We are saving the District thousands of dollars by providing an alternative to purchasing a laptop for every student, teacher, and administrator. We can upload and manage an extra 100 computers on the system in minutes and without much additional work.” - Brad Sandt, director of technology, Park Hill School District.

Cisco VXI: Secure, Flexible, and Uncompromised End-to-End Solution

Cisco VXI accelerates the successful adoption of the virtual workspace by providing an open and validated virtual desktop, voice, and video solution. Cisco VXI increases business efficiency, productivity, and agility by delivering an exceptionally flexible and secure workspace solution with an uncompromised IT and user experience, anywhere and on any device.

Secure

Security for the new workspace must be delivered across each architectural element, from users and endpoints through the network to the data center. Cisco VXI improves data confidentiality and integrity by centralizing, protecting, and controlling access to critical data and intellectual property at the data center rather than across endpoints. Cisco VXI integrates policy-based identity services that enable device profiling and posture assessment and provide need-to-know access to centralized resources. This approach helps protect the organization from data loss, compliance litigation, loss of revenue, and brand damage. It also allows IT to respond quickly to security attacks and planned and unplanned disruptions: technical, natural, or human-made.

Best practices in security must be applied end to end across the Cisco VXI solution. Measures are needed to protect the data center and the infrastructure, secure remote access, and secure the traffic to and from endpoints. Additional measures must be taken to secure the virtual desktops and the communication between one virtual desktop and another as well as communication between one virtual desktop and a virtual server. Because virtual desktops are now consolidated within the data center, it is more important than ever to separate desktop and server traffic and protect mission-critical servers and applications running on the back end.

Although virtual desktops are inherently more secure than their physical counterparts, they introduce new security considerations. Mission-critical web and application servers using the same infrastructure as virtual desktops can now present a much larger attack surface for corrupted desktops. Traffic between virtual machines now pose a more important security consideration that IT managers need to address, especially in dynamic environments that have virtual machines that migrate using VMware vMotion across the infrastructure.

Desktop and workspace virtualization, therefore, significantly increases the need for virtual machine level awareness of policy and security, especially given the dynamic and fluid nature of virtual machine mobility across an extended computing infrastructure. The ease with which new virtual desktops can proliferate magnifies the importance of a virtualization-aware network and security infrastructure. Cisco Unified Data Center and Borderless Networks for workspace virtualization provide strong data center, network, and desktop security, with comprehensive security from the desktop to the hypervisor. Security is enhanced with segmentation of virtual desktops, virtual machine-aware policies and administration, and network security across the LAN and WAN infrastructure.

Cisco VXI secures the new workspace in a variety of ways:

- End user security, such as authentication, encryption, and role-based policies
- Data center security, such as firewalls, intrusion prevention systems, and email and web security
- Network security, such as consistent, context-aware security policies, security policy enforcement between virtual machines, threat defenses, secure mobility access, and content security

Cisco VXI incorporates security throughout the architecture - in the data center, across the network, and at the end user endpoint - providing security for everything from remote access to administrative errors (Table 1).

Table 1. Cisco VXI Security Portfolio

Challenge	Security for	Solution
Secure remote access	PCs, thin clients, zero clients, smartphones, tablets	Cisco AnyConnect Secure Mobility (Cisco AnyConnect 3.0 for email and web security); EasyVPN, DMVPN, and GET VPN for site-to-site VPN technologies; VXC with VPN, VXC with Cisco Virtual Office
Virtualization security	Hypervisor, virtual machines, and virtual switches	Cisco Virtual Security Gateway (VSG), Cisco Nexus 1000V Series, virtual machine LAN security, PVLAN, IP source guard, Domain Host Configuration Protocol (DHCP), snooping, Address Resolution Protocol (ARP) Inspection, and Cisco NetFlow
Threat defense	Data center defense	Cisco Adaptive Security Appliance (ASA), firewall, and Intrusion Prevention System (IPS)
Application and content security	HTTP and XML attacks	Email and web security with Cisco IronPort™ and Cisco ScanSafe appliances
Secure user virtual experience	Display protocol and interactive media	Secure integrated desktop virtualization and secure interactive media experience
Device identity and network data loss prevention (DLP)	Endpoints and network access	Cisco Identity Services Engine (ISE), Cisco AnyConnect, VXC
Enhanced authentication and seamless sign-on	Endpoints and user authentication	USB-based smartcards validated with certificates on VXC backpack and tower, Gemalto .NET card, Gemalto PC USB-TR reader, VXC 2000 Series
Rapid desktop provisioning leaves room for admin error and security loopholes	Access to and from virtual desktops	Cisco UCS Service Profiles and Cisco UCS Virtual Network Interface Card 1280 offering dedicated logical interfaces to facilitate full separation of virtual machines (VMs)
Malware and viruses in virtual desktops	Desktop users and data center	Virtual antivirus solutions from McAfee and Trend Micro

Cisco VXI helps address the security challenges from the client to the hypervisor: in campus and off campus, at remote branch offices, in small office and home office (SOHO) environments, at hotspots, and within the data center. Cisco VXI offers these security benefits:

- Cisco UCS and Cisco VN-Link technology provide visibility into, and security for, the network to the virtual machine and address complexity of security policy enforcement on the virtual ports of the server.
- The Cisco Nexus® 1000V Series Switch and Cisco Virtual Security Gateway (VSG) secures traffic between virtual machines and address the challenges of user segmentation and isolation for mission-critical applications such as enterprise resource planning (ERP), customer relationship management (CRM), and web services. Users are placed in multiple zones, and appropriate security policies are applied to the zone, even as virtual machine-based desktops migrate from one physical host to another.
- Cisco AnyConnect™ Secure Mobility and Cisco ASA Adaptive Security Appliances enable anytime, anywhere secure access to hosted virtual desktops and integrate with Cisco email and web security to deliver a secure and productive end user experience.
- Role-based access restrictions with the Cisco Identity Services Engine (ISE) address the challenge of restricting user access on the basis of the user's role, the user's device, and the device's posture compliance. An important component of an overall security policy strategy, access control is especially important for BYOD devices accessing applications either natively or through a hosted virtual desktop. Cisco ISE acts as a central policy enforcement engine for wired and wireless connectivity. Cisco ISE authenticates the workstation and, on the basis of the credentials provided, pushes the right policy to the access layer switch or wireless LAN controller. Cisco ISE provides a number of services, including authentication, authorization, device profiling, and posture assessment.

Corporate and end user data is also more secure and better protected with consistent, centralized and improved data management, backup, and retention of desktop data, leading to better corporate compliance and a safer desktop virtualization solution. Cisco VXI partners EMC and NetApp offer high-performance data storage solutions that provide centralized, managed, secure storage that greatly reduces the risks associated with end user data loss or corruption.

Flexible

Cisco VXI supports user choice to accommodate different work styles and combinations of virtual desktop, voice, and video endpoint devices, while enhancing the user experience for improved productivity and user satisfaction. It also provides a flexible, open virtual workspace solution that enables agility for varied deployment scenarios and rapid responses to changing business needs. It allows IT to achieve faster, more efficient provisioning and management of end user services through centralized control of end-to-end virtual desktop and collaboration infrastructure and services. Cisco VXI is also very scalable, allowing IT to rapidly provision new workspaces whenever needed.

The Cisco VXI architecture can support a variety of use cases, from traditional desktop virtualization to the unified workspace, providing flexibility for the organization to migrate as needed or to maintain mixed-use models over time. This single architecture delivers near linear scalability, providing tremendous investment protection and stability as usage models change and evolve (Table 2).

Table 2. Cisco VXI Smart Solutions Cover a Wide Range of Use Cases with a Single Architecture

Use Case	Desktop Virtualization	Workspace Virtualization with Unified Communications and Video	Self-Provisioned Private Cloud Workspace	Unified Workspace
IT Requirements and Business Policy	· Controlled data · Virtual application access	· Controlled data · Virtual application access · Voice and video collaboratioan	· Controlled data · Virtual application access · Voice and video collaboration · Intelligent automation for workspace deployment	· Any application · Any device · Full mobility · Uncompromised collaboration experience
User Scenario (Example)	Bank delivers desktop environment from the data center to branch offices	Call center employee accesses call queue on virtual desktop and takes customer calls using Cisco Jabber	Customer service adds 200 new call center seats to deal with high seasonal demand	Hospital administrator uses tablet to access HR applicant software on virtual desktop and uses Cisco Jabber to call applicant
Cisco VXI Smart Solution				
Workspace Productivity	Collaboration Applications (Cisco Unified Communications Manager, Cisco Jabber™, Cisco WebEx®, and Cisco Quad™)			
	All Desktop and Enterprise Applications, Internet, Intranet, Messaging ,and Software as a Service (SaaS)			
Workspace Management			Third Party MDM	
			Intelligent Automation for Virtual Workspaces	
	Desktop Virtualization Software (Citrix or VMware), Cisco VXC Manager, and Cisco UCS Manager			
Secure Mobility: Security, Remote Access			Cisco ESA and WSA and ScanSafe	
	Cisco AnyConnect and Cisco Firewalls			
Policy Management Identity	Cisco Identity Services Engine (ISE)			
Core Infrastructure	Cisco Unified Computing, Cisco Unified Fabric, Hypervisors, and Storage			
	Cisco Switches, Cisco Routers, Cisco Wireless LAN Infrastructure			

Cisco VXI flexibility may be most evident in its support for any device, including zero clients, thin clients, smartphones, tablets, ultrabooks, laptops, Macs, and PCs. End users can access the virtual workspace through their devices of choice, including BYOD endpoints. Cisco VXC provides optimized performance and flexibility and gives users secure, real-time access to business applications and content, any time and anywhere, without compromising the collaborative multimedia user experience. Cisco VXC 2100 and 2200 platform endpoints simplify IT deployment, security, and scalability with an integrated form factor for Cisco Unified IP Phones 8961,

9951, and 9971 that use existing power-over-Ethernet (PoE) and desktop phones, requiring only a monitor and a keyboard; or as the first PoE desktop solution, with a standalone Cisco VXI form factor for customers without the Cisco Unified IP Phone 8900 or 9900 Series. Cisco VXC 6215 is a complete enterprise-ready voice, video, and virtual desktop solution designed for the new workspace. The Cisco VXC 4000 Series provides multimedia collaboration within a virtualized Microsoft Windows XP or Windows 7 desktop.

Cisco VXI provides more flexibility than traditional desktop virtualization solutions and supports more virtual machines per server blade than competing architectures. In the data center, Cisco UCS and Cisco Nexus products deliver outstanding scalability. Built on the Cisco Unified Data Center architecture and integrated data center partner offerings such as NetApp FlexPod and Virtual Computing Environment (VCE) coalition Vblock™ Infrastructure Packages, Cisco VXI benefits from a highly scalable infrastructure that is optimized to host virtual desktops and deliver virtualized applications. With an expansive memory footprint, the latest generation of Intel Xeon processors, and an ultra-low latency, high-bandwidth SAN and LAN fabric, Cisco UCS is well suited to the unique demands of desktop workloads. Cisco Validated Designs for both VMware and Citrix have demonstrated the capability of Cisco UCS to deliver more than 185 virtual desktops on a single server blade while maintaining a consistent user experience and application responsiveness. This linear scalability allows incremental capacity to be added to service tens of thousands of users within a single Cisco UCS domain, providing the flexibility to respond quickly as organizational needs change.

Cisco UCS dramatically simplifies the server architecture and server and virtual machine deployment and significantly reduces the number of devices that must be purchased, cabled, configured, powered, cooled, secured, and managed. Configuration of Cisco UCS is automatic, through unified, model-based management, which simplifies deployment of the virtual workspace. The main differentiators that deliver flexibility include:

- Programmable infrastructure through service profiles that abstract the personality, configuration, and connectivity of server and I/O resources.
- Unified, model-based management that applies personality and configures server and I/O resources to automate the administration process.
- Cisco Port Extender technology, which simplifies the system by condensing three network layers into one, eliminating blade chassis and hypervisor-based switches and bringing all traffic to a single point where it is efficiently and consistently managed.

Flexibility is enabled by Cisco's "wire-once" philosophy, in which the Cisco UCS platform is wired when it is installed, with bandwidth allocation and I/O configuration managed dynamically through the system's embedded management features. Since all servers are physically wired with the same 10 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE) network, they all can host the same workloads simply by changing configurations through software. With Cisco Nexus unified fabric solutions customers can adopt solutions incrementally with little disruption to existing management and operations.

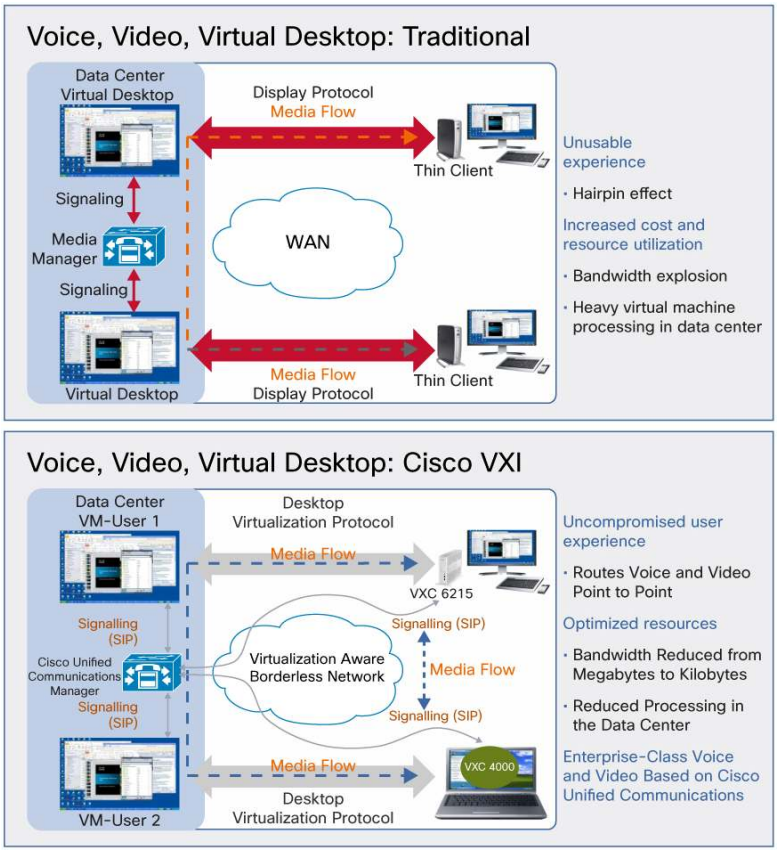
The virtual workspace network is scalable with predictable performance and provides intelligence through the network so that services are available consistently across applications and workloads, service delivery capability scales automatically, and applications are deployed faster with policy-based compliance instead of physical infrastructure changes. Cisco's wide variety of routers, switches, wireless access points and controllers, and WAN optimization products provide the networking infrastructure to meet the virtual workspace needs from headquarters to the campus to remote offices to mobile users. Cisco networks provide the right level of service to all traffic types - wired, wireless, physical desktops, virtual desktops, voice, and video - in the Cisco VXI solution.

Uncompromised

Cisco VXI helps organizations achieve competitive advantage and improved productivity without compromising on cost or resilience goals for a superior return on investment (ROI). IT benefits from reduced risk and technology investments that will serve into the future through a solution based on a validated, integrated end-to-end system and innovative roadmap with an open partner ecosystem and advanced services and support. IT can also achieve dramatic efficiencies without compromising service levels through a centrally managed infrastructure that spans the data center, network, and endpoints. Most important, Cisco VXI allows IT to deliver improved application, desktop, voice, and video services to users more efficiently across the organization while enhancing responsiveness to changing business requirements.

One of the most visible aspects of Cisco's "no compromises" approach for Cisco VXI is the intelligent routing of real-time voice and video traffic. Other desktop virtualization solutions route voice and video traffic from one user over the network to the data center and then from the data center over the network to another user. This is known as the "hairpin effect" reflecting the shape of the traffic route, and it is not only inefficient but ineffective. It puts a significant load on the data center CPUs and uses a lot of network bandwidth. The user experience in this scenario is not good, with shaky and garbled voice and video quality. Cisco VXI combines innovation in the data center, intelligence in the network, and smart Cisco VXC solutions to unify the virtual desktop with voice and video. Only a few kilobits of signaling travel to the data center so the Cisco Unified Communications Manager can recognize where the call is coming from and where it is going to optimize communications directly between the users, point-to-point (Figure 7).

Figure 7. Cisco VXI Compared to Traditional Desktop Virtualization for Voice and Video

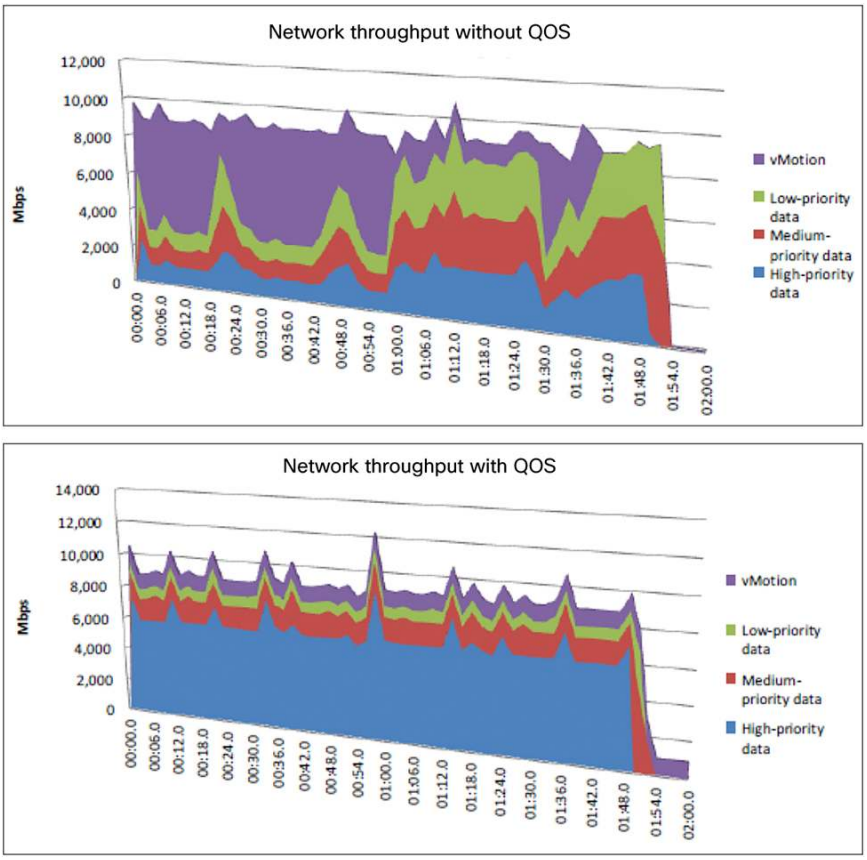


There are no performance compromises with Cisco VXI. Cisco UCS has established 63 world performance records in three years, including the highest VMware VMmark benchmarks for virtualization for any server. A single Cisco UCS blade chassis can now provide 160 Gbps of bandwidth.

Cisco works closely with its Cisco VXI partners to optimize performance wherever possible. Cisco and Citrix worked together to optimize Cisco Wide Area Application Services (WAAS) to provide high-performance delivery of Citrix XenDesktop and XenApp over the WAN. This effort allows Cisco WAAS to provide a high-quality user experience for virtual desktops by accelerating performance for applications and video delivered using Citrix XenDesktop and XenApp by up to 70 percent. Cisco WAAS also increases the number of Citrix users supported concurrently over the WAN by up to two times, through powerful optimization techniques that reduce bandwidth consumption by up to 60 percent.

Additionally, the Cisco Unified Data Center with Cisco UCS allows IT managers to help ensure high performance for individual user desktops through manageability and quality of service (QoS) features. These capabilities allow administrators to more effectively debug and analyze discrete traffic flows associated with user desktops across the computing fabric and isolate specific bottlenecks that affect an individual desktop or pool of desktops, while also implementing detailed bandwidth and prioritization control that helps ensure that IT can deliver a consistent user experience and application behavior even for congested networks and peak-demand scenarios (Figure 8).

Figure 8. Network Throughputs With and Without QoS Policies Applied: Cisco UCS Delivers Consistent Virtual Desktop Performance Even Amid Disruptive VMware vMotion Events Across the Same Infrastructure. (Greater Mbps for High-Priority Data is Better)



IT operations, organizational agility, and end user satisfaction and productivity are all improved with Cisco VXI. IT can manage more virtual machines per server, deploy them quickly, and manage them simply. IT gains control of end user data protection and security, reducing risk and enabling compliance. The organization can rapidly respond to changes in the environment with no limits on time or location and has more satisfied IT and user employees. Users can select the device of their choice, including BYOD endpoints, and have anytime, anywhere access and the additional productivity that real-time voice and video can provide.

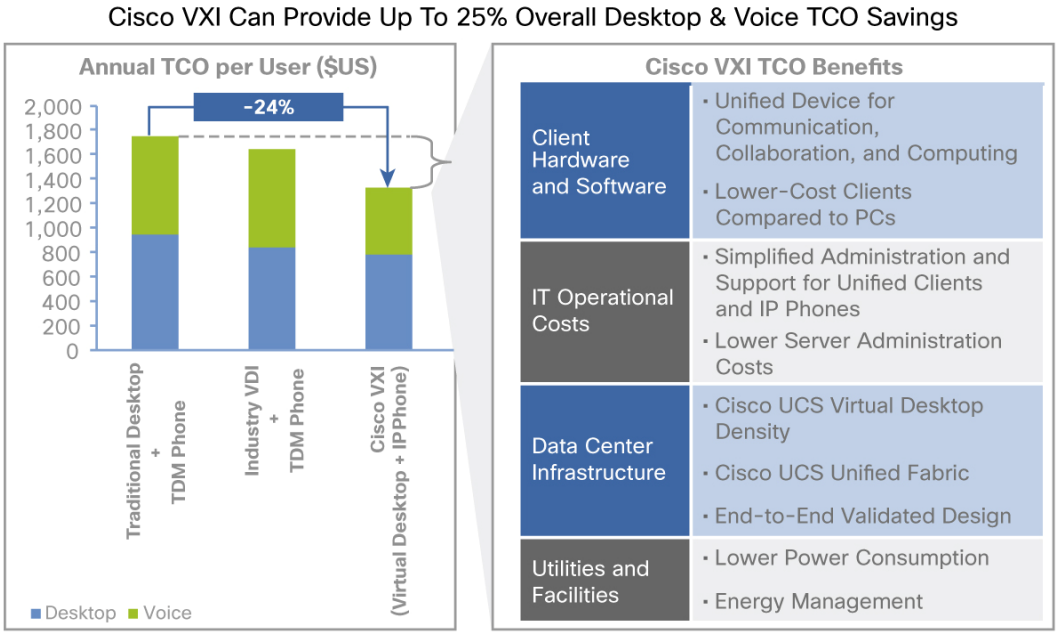
With Cisco VXI, you can empower workers to work the way they prefer without compromising organizational interests. In addition, compared to traditional desktop and telephony environments and traditional desktop virtualization and telephony environments, Cisco VXI can provide significant savings.

Success

The Cisco VXI solution saves time and money compared to alternative approaches. It offers faster payback and ongoing savings with the industry's highest virtual desktop density per server, reducing the number of servers needed and the associated capital expenditures (CapEx) and operating expenses (OpEx). It also enables lower network infrastructure costs, with fewer cables per server and fewer ports required, via the Cisco UCS architecture and unified fabric. In addition, storage costs are reduced with storage tiering and deduplication technologies, reducing desktop storage needs by up to 50 percent (Figure 9).

The newest innovations in server technology allow placement of a large, high-performance storage footprint using solid-state disks (SSDs) directly on the Cisco UCS server blade. This capability, suitable for caching read or write-intensive content that is shared across a pool of virtual desktops, delivers high rates of I/O operations per second (IOPS), critical in offloading oversubscribed shared SAN storage, delivering better performance, and dramatically reducing the cost of storage overall. In combination with an open ecosystem that supports solutions offered by Atlantis Computing, Nexenta, and others, Cisco VXI delivers a breadth of validated approaches that defray and optimize the cost of data center infrastructure.

Figure 9. Savings with Cisco VXI Compared to Traditional and Virtualized Desktops



The simplified deployment of Cisco VXI accelerates time to productivity and enhances business agility. IT staff and end users are more productive more quickly, and the business can respond to new opportunities simply by deploying virtual workspaces whenever and wherever needed. The high-performance Cisco systems and network deliver a near-native end user experience, allowing users to be productive any time, anywhere.

The ultimate measure of workspace virtualization success for any organization is its efficiency and effectiveness, both in the near and long term. The Cisco solution is very efficient, allowing rapid deployment, using minimal infrastructure components and cabling, and enabling lower costs. The solution is also very effective, providing the services that end users need on their devices of choice while improving IT operations, control, and data security along with organizational agility. Success is bolstered through Cisco's best-in-class partnerships with leaders in virtualization and storage technologies and through tested and validated designs and services to help customers throughout the process. Long-term success is enabled through Cisco's scalable, flexible, secure architecture as the platform for workspace virtualization, which is also an excellent platform for data center applications and cloud computing.

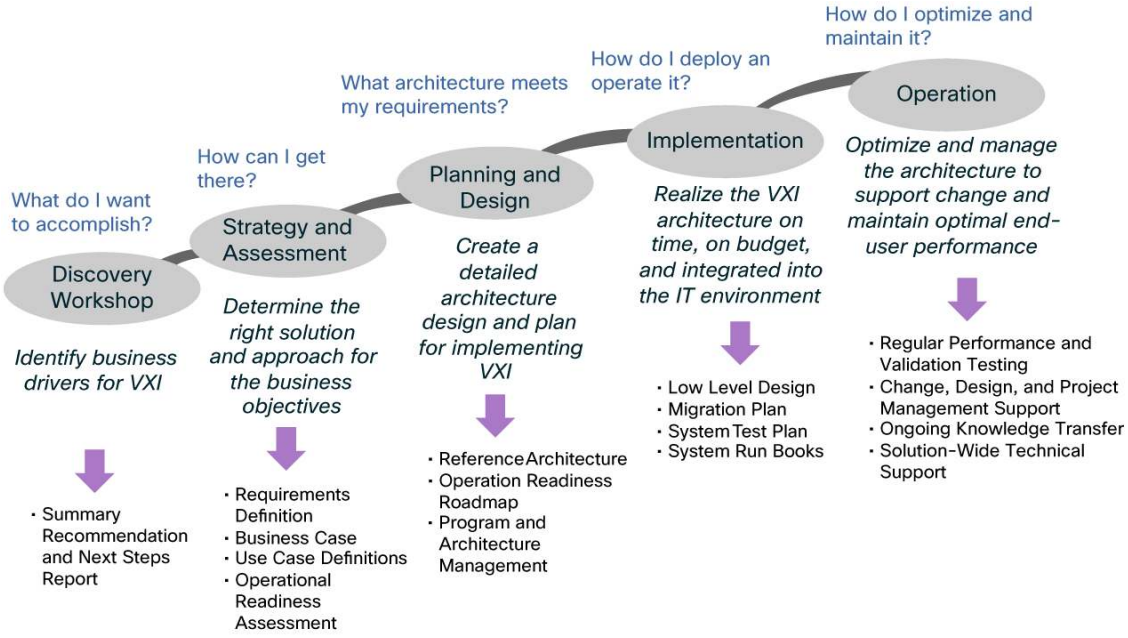
Cisco VXI Services

Cisco and its partners offer a comprehensive portfolio of services (Figure 10) to help customers successfully plan, build, and manage Cisco VXI solutions. These services help ensure effective solution design and deployment at any scale and optimize the data center, network, and collaboration architectures that support workspace virtualization to accelerate ROI. Cisco also offers technical support for the end-to-end solution, providing one point of contact to manage technical support for Cisco and third-party products included in Cisco Validated Designs. This approach helps alleviate the overhead associated with the management of complex solutions.

Customers can take advantage of these Cisco Services to navigate the potential complex system integration and operation effects associated with the adoption and evolution of their workspace virtualization solutions:

- Desktop Virtualization Strategy
- Desktop Virtualization Planning, Design, and Implementation
- Desktop Virtualization Optimization
- Cisco Allied Service for VXI (providing solution-wide technical support across Cisco and third-party products)

Figure 10. Cisco VXI Services, Benefits, and Deliverables



Cisco Validated Designs

Cisco Validated Designs consist of systems and solutions that are designed, tested, and documented to facilitate and improve customer deployments. These designs incorporate a wide range of technologies and products into a portfolio of solutions that have been developed together with our partners to address the needs of our customers and are refreshed periodically to support emerging requirements and incorporate the latest technology innovations.

Conclusion

The modern workplace is changing rapidly, bringing opportunities for end users, IT, and organizations that embrace and manage these changes. Workspace virtualization, which includes virtualized desktops, voice, and video, considers the entire user workspace and provides a solution that enhances agility and reduces costs for the organization; improves operations, control and security for IT; and increases access, productivity, and choice for end users. However, to be truly effective, workspace virtualization must be more secure and more flexible and require no compromises compared to the present system or other alternatives. The Cisco VXI workspace virtualization solution is grounded in these three principles and includes end-to-end, integrated, and validated data center, network, and collaboration architectures. Only Cisco provides a complete spectrum of unified workspace solutions that encompass native, virtual, and unified delivery models.

Workspace virtualization project leaders should consider the following approach in exploring the implementation of a new workspace solution:

- Define the end-state user experience strategy. What will the required services look like in the future? Be sure to engage line-of-business, IT server, data center, application, security, networking, and communications teams from the start.
- Identify the primary organizational and IT priorities and benefits, which can include user flexibility, data security, cost savings, BYOD capability, IT efficiency, availability, etc.

- Develop a workspace use case and technology roadmap, engaging application, data center, network, and security stakeholders. Make sure that your roadmap supports short- and long-term goals and initiatives.
- Engage your Cisco team and partners, who can help accelerate your success through advanced services that cover all phases of the initiative: plan, design, deploy, implement, operate, and optimize.

For More Information

For more information about Cisco VXI, the new virtual workspace, and related products and services please visit:

Cisco VXI website

Cisco VXI design guides

Cisco VXI Services

Cisco VXI with Citrix

Cisco VXI with VMware

More Reading

Cisco VXI Primer: Introduction to End to End Desktop Virtualization white paper

Cisco VXI Security white paper

Rich Media in VXI white paper

Cisco WAAS Optimized for Citrix XenDesktop white paper

Principled Technologies: Cisco UCS Virtual Desktop Scaling with VMware white paper

Principled Technologies: Cisco UCS Virtual Desktop Scaling with Citrix white paper

Product Information

Cisco UCS

Cisco Virtualization Experience Client (VXC)

Cisco WAAS

Case Studies

Case Study: Geometric

Case Study: KPIT Cummins

Case Study: Metro Health

Case Study: Seattle Children's Hospital

Case Study: Barwon Health

Case Study: Banco Azteca

Case Study: Oak Hills Local School District

Case Study: Park Hill School District

Case Study: Seattle University

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 www.cisco.com/go/offices.

Printed in USA C22-617932-01 07/12