ResearchCorp

2017 U.S. IT Services Report

Part 1 – IT Services & Planning
Part 2 – IT Platforms & Turbocharging IT
Part 3 – Infrastructure & What Keeps IT Awake at Night

Sponsored by

fidelus

TABLE OF CONTENTS

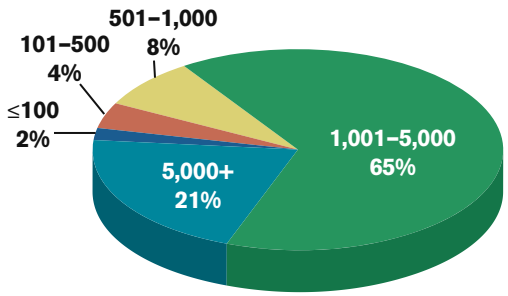
2017 U.S. IT Services Report

INTRODUCTION

Delivering IT services is an ongoing challenge for all organizations working with fixed budgets and resources. Assuring superior IT services requires consistently maintaining the perfect mix of technical skills and customer service to support the ever-changing requirements of today's dynamic IT infrastructures. With so many demands on in-house IT teams—not just in terms of new products and systems, but also for installation, integration, training, and delivery methods—many organizations utilize the specialized technical skills of IT services providers to complement the talent of their in-house teams.

The 2017 IT Services Report is based on a nationwide survey, conducted in Q4 2017. The report examines usage, approach, and preferences for IT services and products in organizations nationwide, as well as common goals and practices for engagement with IT service providers.

Company Size by Number of Employees

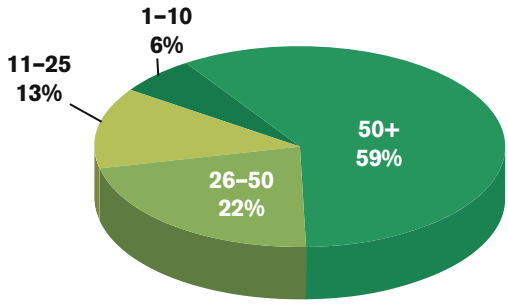


RESEARCH METHODOLOGY

Independent databases of IT professionals were invited to participate in a web survey conducted by ResearchCorp, via SurveyMonkey. The report data comprises 532 responses from organizations with 100 to 5000+ employees. Of note is that the 86% of respondents using IT services providers are in organizations with greater than 1000 employees.

This 2017 U.S. IT Services Report was sponsored by Fidelus Technologies, an IT services provider headquartered in New York City. The sponsor was not revealed to participants.

Size of IT Team



PART 1 – IT SERVICES & PLANNING

SNAPSHOT OF FINDINGS

- Organizations most often engage IT service providers for installation, setup, and ongoing management of Networks and Unified Communications.
- 50%+ of organizations engaging IT services providers for technology installation and setup projects, also engage them for Managed Services—ongoing care and maintenance.
- 54% of organizations use multiple IT service vendors in order to secure Best-in-Class technology services.
- 17% of organizations remain without a business continuity plan and/or a security breach plan despite the prevalence of natural and man-made disasters and network intrusions that lead to huge data theft—all of which adversely affect businesses every day.

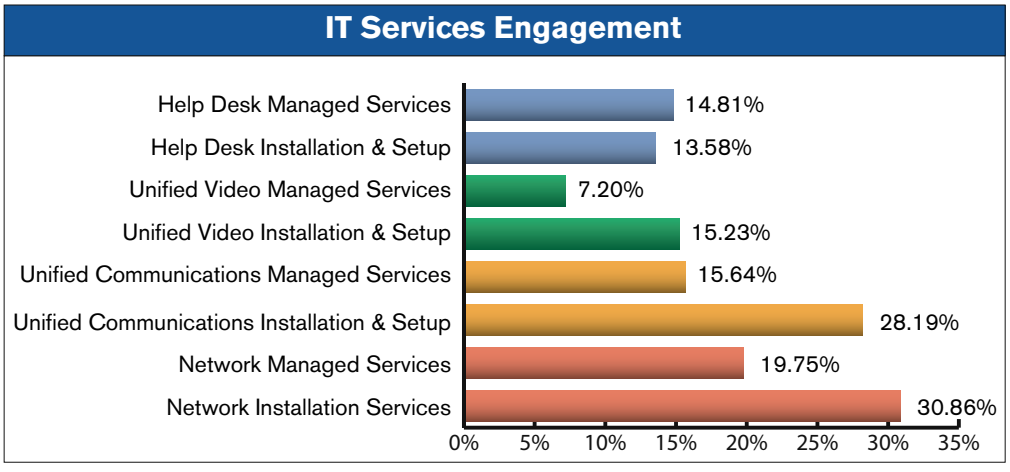
IT SERVICES ENGAGEMENT

Organizations engage IT services providers for a wide range of projects, as well as ongoing managed services. With the ever-evolving nature of technology, it is difficult, even for larger IT teams, to maintain the detailed and current expertise and certifications for new technology—especially while performing the large number of daily IT tasks required to keep an organization's infrastructure humming and employees productive.

Organizations often engage IT services providers to perform installation, setup, and training, for their in-house personnel, on network and unified communications infrastructure. 30.86% of organizations surveyed use IT services providers for network installation and setup and 28.19% for unified communications installation and setup. These two categories also dominate the managed services engagements because the technology is complex, ever-evolving, and requires specialized expertise. Figures show that 64% of the organizations who engaged IT services for network installation and setup, also chose ongoing network managed services; and, 55% of the organizations who engaged IT services for unified communications installation and setup, also chose ongoing managed services for their unified communications.

Of additional note is the fact that, while only 13.58% of organizations surveyed used IT services providers to install and setup their help desks, 14.81% of these organization engaged an IT services provider to manage their help desks.

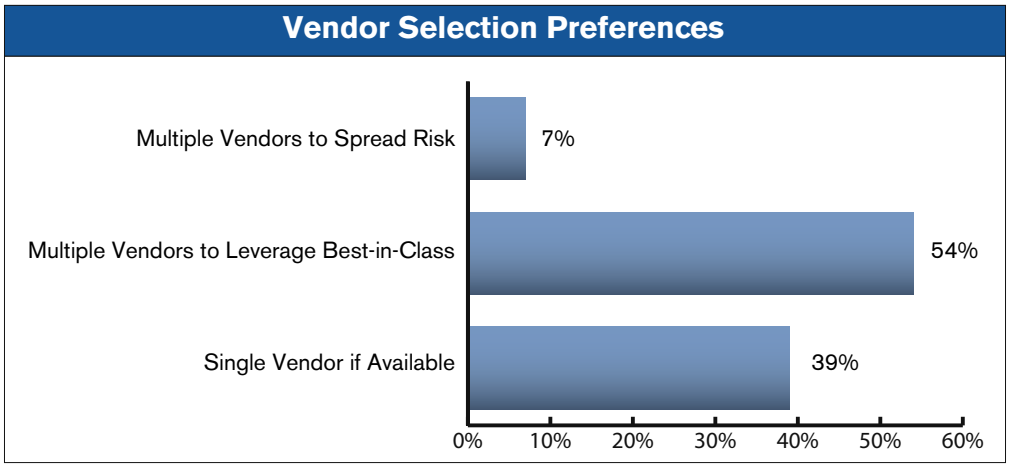
As newer technology, unified video ranked behind network and unified communications services in usage. However, 15.23% of organizations surveyed used IT services providers to setup and install their unified video systems. As with the more dominant services, nearly half of these organizations (47%) used managed services for their unified video systems.



VENDOR SELECTION

Selecting an outsourced IT services vendor to fit with both business requirements and organization culture is a non-trivial exercise and a poor selection can be costly. Furthermore, finding a single IT services vendor, with all of the expertise required by an organization, is not simple. Organizations have found that many IT services vendors claim broader technology expertise than they can actually deliver, in order to prevent potentially competitive IT services vendors from securing a foothold in their customer bases.

While 39% of the organizations surveyed desire the convenience of a single IT services vendor to handle all of their needs, the caveat is, "if available." One might suppose, since some IT service vendors overstate their capabilities and organizations have been burnt, that selecting multiple vendors could be based upon the objective to "Spread the Risk." However, with 54% of respondents selecting "Multiple Vendors" to "Leverage Best-in-Class" services, clearly quality is the driving criterion for multiple vendor engagement.



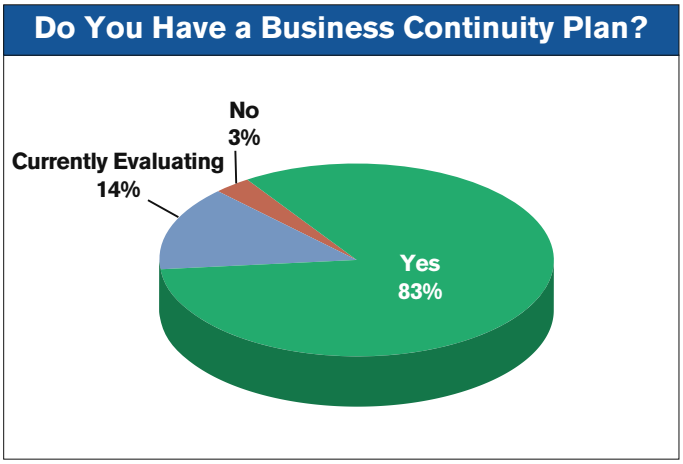
ORGANIZATIONAL STRATEGY & PLANS

Organizational IT planning to develop, roll-out, maintain, and execute continuity of operations is critical for organizations of all sizes. Engaging the assistance of an IT service provider to formulate these business-critical plans to assure IT infrastructure resilience, can be extremely helpful. The reasoning is simple. IT services providers bring an experienced and broad view of the challenges faced by, and solutions implemented across, many organizations. Such knowledge and expertise, often not held by an organization's in-house IT staff, is valuable for developing plans and avoiding pitfalls.

BUSINESS CONTINUITY PLAN

In today's world of natural and man-made disasters that continually affect and often halt business operations, it is surprising to find that some companies remain without a clearly documented business continuity plan. Yet 14% of respondents are only in the evaluation phase of such planning, and 3% have no plan, nor are they currently considering developing a business continuity plan.

Organizations develop business continuity plans to adapt operations in the event of any type of extended service interruption. These plans address maintaining the business-critical services by documenting the processes, personnel, and communications escalation for each type of event. Organizations test their business continuity plans, in advance of an event, to assure successful execution when the need arises.



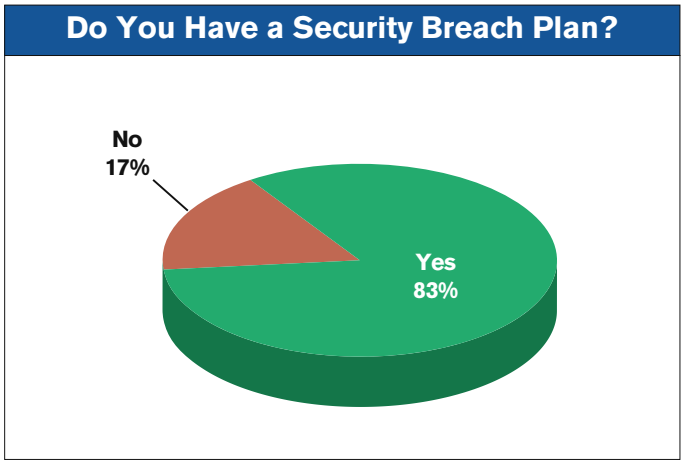
SECURITY BREACH PLAN

Front page headlines tell us horrifying stories of security breaches that continually occur across industries—and with more and more valuable data, both inside corporate networks and in the cloud, the security attacks are increasing in number and severity. According to IBM's 2017 Cost of Data Breach Study, 47% of all breaches in 2017 were caused by malicious or criminal attacks. The remaining 53% was caused by a mix of different attack vectors including ineffective or non-existent mobile device management and DLP (Data Loss Prevention) strategies, security control, system access, and/or inefficient analytics, monitoring, and processes.

On the positive side, all of the very public bad news surrounding security breaches has prompted high awareness among IT departments everywhere of the importance for an up-to-date and comprehensive security breach plan. Of the companies participating in this survey, 83% have a security breach plan in place. However, 17% of the companies surveyed remain in danger of being front-page news because they have no security breach plan at all!

To set the foundation for a top-rate security breach plan, organizations keep all systems and infrastructure up-to-date with the latest recommended patches. Organizations who delay or skip software patches—for a variety of reasons, including the lack of justification for the system downtime required to apply the patches—have paid a high price for the delays. Other organizations prudently compare the cost of a breach versus the downtime cost to do the patches and the conclusion is consistent: do the required maintenance to assure systems are up-to-date.

An additional aspect of security is user training. Social engineering is used in more than half of all attacks by hackers. Training is an effective way to reduce or eliminate the success of such attacks and is part of any comprehensive security strategy.

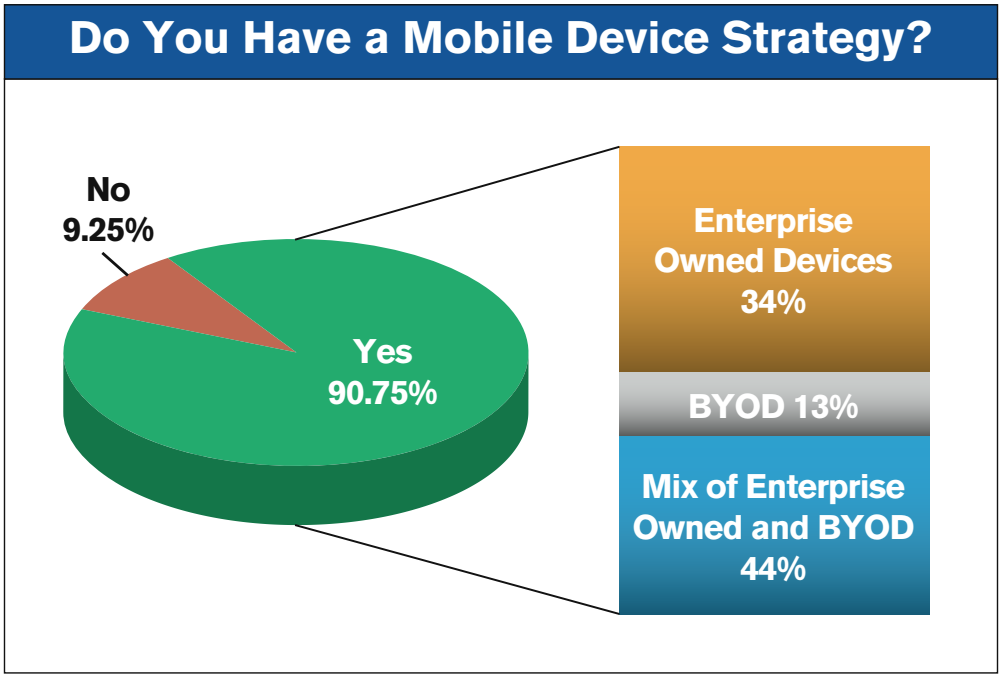


MOBILE DEVICE STRATEGY

Mobile devices are part of our daily lives, at work and at home. We use phones, tablets, laptops, and even our wrist watches to communicate and share information. From an organizational IT security perspective, the mobile devices attached to each one of us are potential pathways into an organization's network and proprietary data. As discussed later in this survey, in the Attack Vectors of Concern section, Mobile Device Compromise ranks 5th, with 32.23% of IT professionals worried about mobile device compromise. Of note is that this concern is shared among both the 9.25% of participants who do not have a Mobile Device Strategy in place, and some of the participants who do have a Mobile Device Strategy in place.

When considering a mobile device strategy, organizations considered some basic issues:

- Access control of each individual device to sensitive information.
- Ability to control or wipe a lost or stolen device.
- Enforcing basic security on each device (e.g. PIN/password to unlock).
- Mobile malware detection deployment on the devices.
- Multi-factor authentication requirements for mobile devices.



UNIFIED COMMUNICATIONS AND COLLABORATION (UCC) STRATEGY

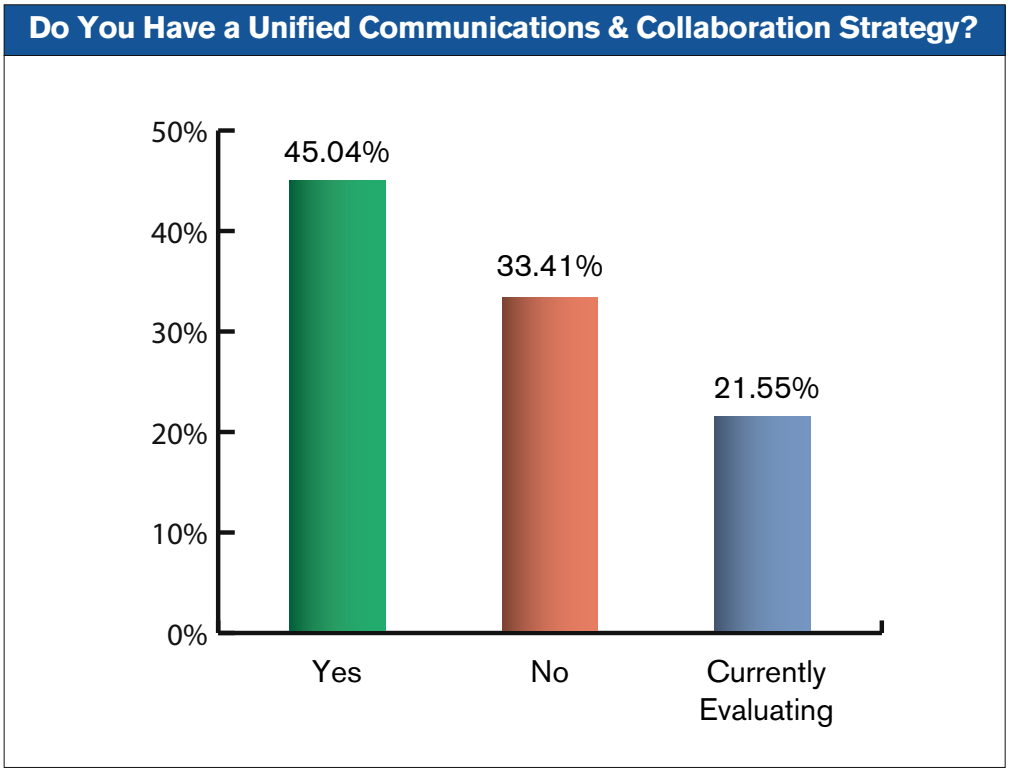
Communications and collaboration feed organizational success. The benefits of UCC are many for organizations that want to assure high-quality interactions among employees and with customers. As such, UCC is becoming a "must-have" for organizations of all sizes. Organizations have increasingly dispersed mobile workforces that require tools to facilitate effective and efficient communications. Many organizations are using UCC to increase employee productivity and reduce costs.

UCC has three components: foundation technologies such as VoIP and presence, legacy systems such as email and conferencing, and new technology like communications-enabled business processes (CEBP) and social media. It is vital for organizations to review and select the right systems and tools, specific to their communication and collaboration use cases. Based upon such an analysis, a strong UCC strategy can be developed for selection, integration, deployment, and training. The mix of these elements can be complicated, leading many organizations to bring in UCC experts.

As one might expect, considering the complicated nature of UCC strategy plan development, only 45.04% of organizations surveyed have a UCC strategy in place. Much of the complexity arises from the challenge of selecting the best business and cultural-fit solutions for the organization from the array of ever-changing technology options. However, organizations are realizing that a well-conceived UCC strategy can increase employee productivity by enabling workers to quickly and efficiently locate and interact with teammates via voice, video, instant messaging, etc. In addition, an entire team can easily collaborate on an ad hoc and/or scheduled basis.

The respondent data indicates the increasing understanding of the high-productivity value of UCC. In addition to the organizations that have a UCC strategy, another 21.55% of respondents are currently evaluating development and implementation of a UCC strategy—leaving only 33.41% of respondents without a strategy under development or a plan in place.

Strategies and plans are not a once-and-done exercise. Organizational strategy development and planning, across the technology spectrum, is a dynamic process. A process that is fed by new and improved technology availability and changing operational needs as organizations grow and mature.



PART 2 – IT PLATFORMS & TURBOCHARGING IT

SNAPSHOT OF FINDINGS

- Cisco is the highly-preferred network equipment vendor leading market usage by >80% for switches and routers, nearly 60% for wireless networks, and >60% for firewalls.
- With security as a hot button for IT teams nationwide, over 60% of organizations use either 3 or 5+ security vendors' equipment to secure their network infrastructure.
- Among the communication and collaboration platform choices, persistent group chat is used primarily for marketing and development projects and ~60% of organizations do not use this category of communications.
- It is still early in the adoption curve for Software Defined Networking (SDN) with nearly 50% of organizations neither using nor currently considering use of SDN.

When selecting new IT systems and tools, it is useful to examine the market trends across other organizations. While vendor purchasing and deployment preferences are certainly based upon an organization's use cases, categorically (i.e. network, UCC, Security, etc.), there are platforms and products that stand out among the choices as adoption and usage proliferate across the IT market as a whole.

THE MARKET SPEAKS

NETWORKING

Architecting, configuring, deploying, and maintaining a network that can optimally serve an organization today, and grow and change to suit an organization's needs in the future, requires up-to-the-minute experience in both the technologies involved and network design.

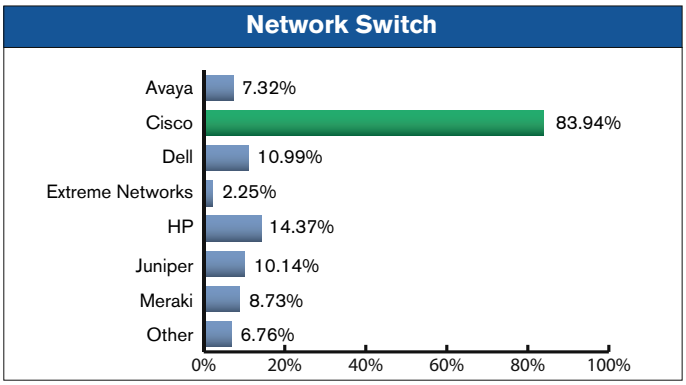
An organization's network is the backbone of the business. As such and not surprisingly, network design, implementation, and ongoing managed services are the most frequently requested IT tasks for which organizations engage IT Services providers.

NETWORK SWITCHING EQUIPMENT

A network switch connects multiple devices (i.e. computers, printers and servers) while efficiently managing the flow of data within an organization's building or campus. While switches can relieve network congestion, there are a vast array of features and functionality (i.e. physical termination type, desired level of redundancy, modularity, etc.) that organizations must review. Thus, it is important to have expertise in network design and best practices to avoid using switches unnecessarily.

The keys to adding switches to a network architecture are:

- Understanding if switches can be added to the existing network design, or if a network redesign is required.
- Determining how and where to add switches to gain optimal benefit.
- Selecting switches with appropriate functionality to address the organization's needs today and in the future, to maximize return-on-investment and assure support requirements are met.



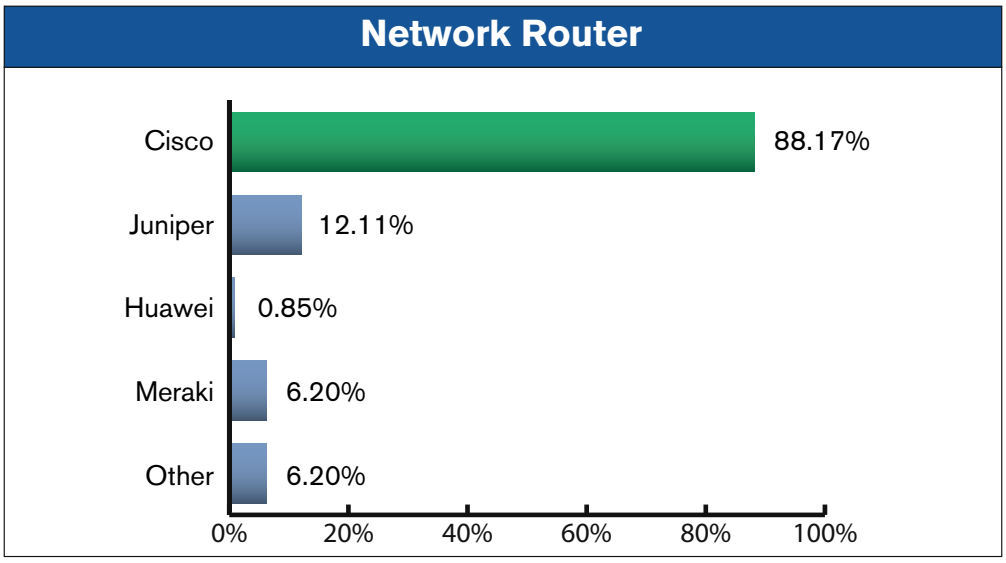
Survey participants were asked to identify switching equipment deployed in their networks, by vendor. Some organizations use multiple vendors and Cisco is the highly-preferred switch vendor at 83.94% usage.

NETWORK ROUTING EQUIPMENT

Routers were originally introduced to route traffic between network segments (subnets). However, the increased capability of switches has relegated routers to the more specialized function of edge connectivity (WAN, internet, etc.). Routers offer significant advantages with this specialization, including better per-port performance and greater flexibility in an array of functionalities which are specific to the network edge (GRE, IPsec, NAT, etc.)—resulting in increased network efficiency and increased ROI by prolonging the life of the network equipment.

When organizations choose a router, some of the factors considered are:

- **Network Design** – Routers are primarily used at the network edge (internet, provider, WAN, etc.), so it is important to understand the purpose of the router, service provider hand-off type, and throughput requirements.
- **Redundancy** – Uptime requirements for a router's functionality dictate, for example, whether dual-power supplies suffice, or complete device redundancy is required. If complete redundancy is required, then other single-points of failure (additional switches, firewalls, etc.) must be also be addressed.
- **Future Proofing** – Device lifetime is a function of a router's ability to accommodate the growth of the organization and add throughput as demand increases. To maximize device ROI, organizations sometimes choose routers that offer pay-as-you-grow options.
- **Breadth of Functionality** – Router functionality varies from performing a single function to performing multiple functions such as WAN routing, WAN optimization, SDWAN, voice capabilities, etc. Router selection depends upon the needs of the organization.



Survey participants were asked to identify router equipment deployed in their networks, by vendor. Some organizations use multiple vendors. Cisco is the highly-preferred router vendor at 88.17% usage.

WIRELESS NETWORKS

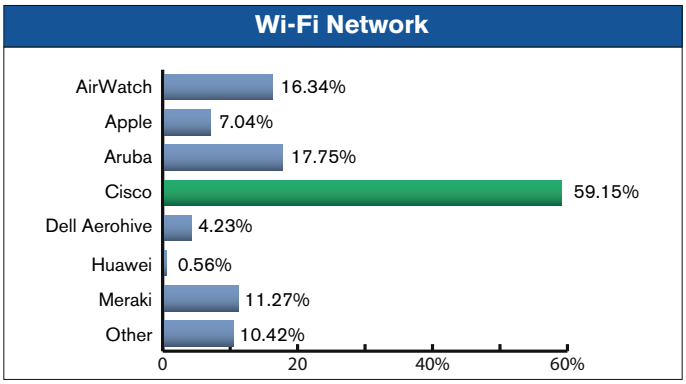
Wireless network technology is complex. Both specialized WLAN testing tools and experienced, knowledgeable, personnel are required to deploy and maintain an IEEE 802.11 wireless network that meets an organization's needs.

Avoiding congestion on a wireless network can be tricky and capacity planning is important to effectively support users as they shift between wired and wireless throughout the day. Further, workers expect the same network access rights (and limitations) when using Wi-Fi as they experience over the wired network. Elements reviewed by organizations for the deployment of a wireless network include: the number of clients it must serve, the type of traffic expected on the network, the desired amount of throughput the network should provide, and the number of access points required and where to mount them for optimal coverage.

Many unexpected things can interfere with Wi-Fi network operation. Some organizations use tools that mitigate this risk by estimating the location of access points. Other organizations believe that there is no substitution for a physical site survey and spectrum analysis. A proper site survey and spectrum analysis will help avoid poor signal propagation due to a variety of factors including walls (type and quantity) and wireless spectrum saturation in densely populated areas. Although some legacy connectivity may be required (802.11b/g/n at 2.4GHz), modern Wi-Fi network designs focus on the 5GHz wireless standards, including 802.11ac, which offer greater throughput and capacity and are not subject to the same levels of interference as the 2.4GHz wireless standards. Therefore, when selecting a WLAN vendor, organizations include an easy-to-use, centralized management platform for deployment, location and spectrum analytics, and security. When choosing the access points, organizations consider including the latest available features such as multigigabit ethernet support, multiple antennas (MIMO), and dedicated security radios. If voice is to be deployed over the wireless network, the selection of a protocol analysis tool enhanced to report the metrics specific to VoIP call quality is required.

Among the many security threats that organizations face, wireless network breaches are a particular concern due to the lack of physical security of these networks. As such, authentication, encryption, and isolation are the keys to preventing unauthorized network access. In addition, security-conscious organizations understand they must maintain the latest standards and patches. Many organizations partner with services providers who monitor vulnerabilities and quickly and efficiently apply patches and updates.

Deploying an effective wireless network, that works seamlessly with the wired network and meets employee needs and expectations, is a formidable task; and, once deployed, the wireless network must be managed on an ongoing basis to assure peak operational efficiency.



Survey participants were asked to identify Wi-Fi equipment deployed in their organizations, by vendor. Some organizations use multiple vendors. Cisco is the highly-preferred Wi-Fi vendor at 59.15% usage.

COMMMUNICATION & COLLABORATION

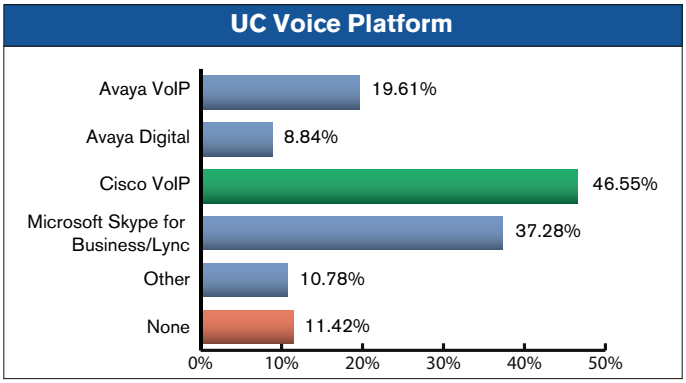
As discussed in the UCC Strategy planning section of this report, workforces are increasingly geographically dispersed and mobile. Organizations are using UCC to increase employee productivity and reduce costs. As with network infrastructure, architecting and maintaining a healthy unified communications and collaboration architecture for an organization can be complicated. Organizations frequently engage IT services providers with deep expertise in the choices and optimal design of UCC infrastructure to assist planning, development, and management of their UCC systems.

Organizations that develop a UCC strategy, consider:

- **User Experience** – This is key when developing a UCC strategy. If a user cannot use the system, it fails. Training is an important facilitator for successful deployment in an organization.
- **Handsets vs Softphones** – Softphones are an appealing option but there can be drawbacks to an all-softphone deployment, such as usability and functionality. Users' job functions are a factor in making this decision in order to assure softphone cost savings are realized.
- **Hosted vs On Premise vs Fully-Managed Solutions** – A majority of the telephony equipment often resides on site (handsets, PSTN gateways, etc.). Organizations weigh their options regarding: levels of control in a hosted model vs on premise, features available in hosted offerings, time and expertise required for maintenance, and can a fully-managed offering provide the optimal solution for the organization's needs.
- **Equipment** – Some telephony manufacturers' products are designed to be a homogenous telephony network, while others rely on third parties for various functions of the telephony environment. An additional consideration is equipment support timeliness and quality.
- **Future-Proofing** – Organizations review a manufacturer's history of introducing and/or quickly adapting to new technologies and standards. System expansion capabilities, to support both organic and inorganic growth, is also a consideration.
- **Resiliency** – Organizations review single points of failure in the UCC platform, survivability in the event of a WAN failure, and how the UCC platform fits into the business continuity plan.

UNIFIED COMMUNICATIONS & COLLABORATION (UCC)

As shown earlier in this report, currently 54.96% of organizations do not have a UCC strategy plan in place, although 39% of these organizations are currently evaluating their options and performing analysis to develop UCC plans.



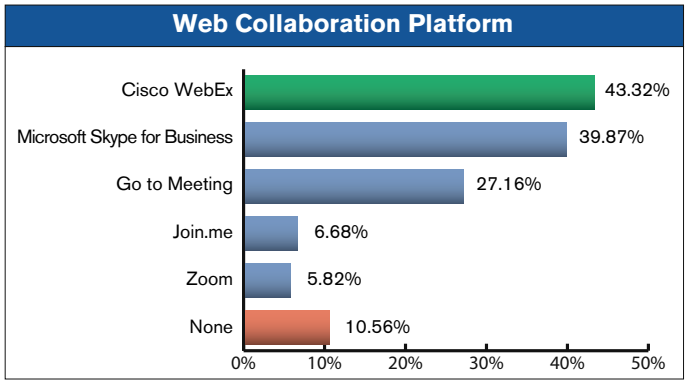
Survey participants were asked to identify the UCC platform(s) for voice, deployed in their organizations, by vendor. Some organizations use multiple vendors. Cisco is the preferred UCC voice vendor at 46.55% usage. Microsoft Skype for Business/Lync is in second place, trailing Cisco by 9.27 usage percentage points. Avaya products, with a combined usage for VoIP and Digital of 28.45%, sit in third place, 18.1 usage percentage points behind Cisco. There remain 11.42% of organizations that have no voice collaboration platform.

WEB COLLABORATION PLATFORM

A Web collaboration platform is a productivity business tool that facilitates one-to-one, one-to-many, or many-to-many employee and customer, real-time, internet-based communications. The platform is a back-end software or service and, depending upon the vendor selected, can include functionality for audio, video, screen sharing, white-boarding, advanced scheduling options, and branding.

Web collaboration is particularly convenient and cost-effective when the parties involved in the collaboration are geographically dispersed. Web collaboration platforms can be accessed via phone, tablet, computer, or recently a watch.

Cisco is the preferred Web Collaboration vendor at 43.32% usage for their WebEx platform. Microsoft Skype for Business/Lync is close behind, trailing Cisco by a narrow 3.25 usage percentage points. The third most used platform, GoToMeeting, is used in more than a quarter of organizations and trails Cisco WebEx usage by 16.16 usage percentage points. There remain 10.56% of organizations that do not use a voice collaboration platform.

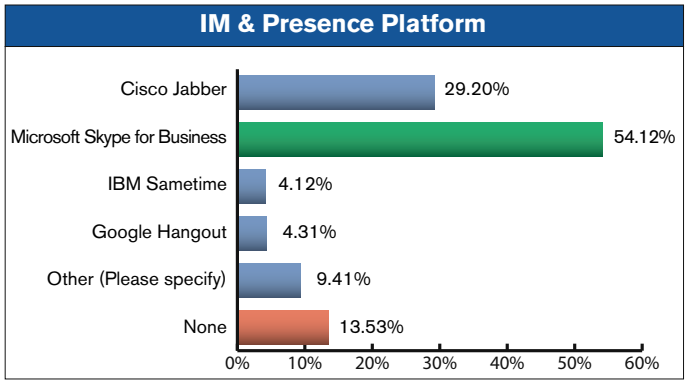


Survey participants were asked to identify the Web Collaboration platform(s), deployed in their organizations, by vendor. Some organizations use multiple vendors.

INSTANT MESSAGING & PRESENCE PLATFORM

Instant messaging (IM) is real-time, online text-based communication, through a software platform, hosted on premise or in the cloud. It is fast, simple, and private. IM is a convenient mechanism for quick exchanges, and is generally used for one-to-one communications. IM is similar to text messaging. However, a key differentiator, with regard to Enterprise security, is that texting is primarily a function of mobile phones and is often unmanaged and unsecure.

"Presence" allows people on the IM platform to see the connection status of other people on the platform i.e. which people are and are not, online and/or available. Users generally have the option to tell the IM platform that they are unavailable (not present) when they are otherwise occupied and do not want to be disturbed.



Survey participants were asked to identify the IM and Presence Platform, deployed in their organizations, by vendor. Some organizations use multiple vendors.

Organizations consider the following issues when selecting an IM platform because these are essential to user adoption and, utility and fit within the organization's IT infrastructure:

- **Security** – A locked-down platform with tightly controlled root access, encryption of all data both at rest and in transit, and secure archival of messaging for compliance reasons.
- **Ease of Use** – The amount of training required to use the platform, user familiarity with the interface, commonality of interface across all platforms, and availability on mobile devices.
- **Compatibility** – The capability to talk with other like and dissimilar systems used by companies with which the organization does business (referred to as federation).

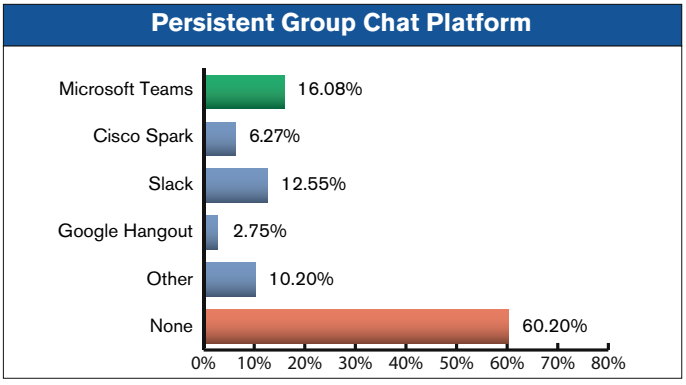
- **Hosted vs On Premise** – To match the organization's overall cloud and security strategies.
- **Integration with Existing Systems** – To support the day-to-day end-user usage, IM integration with telephony systems, productivity systems (e.g. MS Office), or other corporate systems, has varying levels of importance which are determined by the organization's examination of user use cases.
- **Licensing Structure** – Some IM platform vendors require a license upgrade to enable certain features, while others offer all capabilities with a single license type.

Survey participants were asked to identify the IM and Presence Platform deployed in their organizations, by vendor. Some organizations use multiple vendors.

Microsoft Skype for Business is the highly-preferred IM and Presence platform vendor with >50% usage among organizations surveyed—a substantial 25.92 usage percentage points ahead of the second-place Cisco Jabber. The "other" category, at 9.41%, warrants mention for two reasons. First, because it exceeds in usage size the third and fourth place products, Google Hangout and IBM Sametime. Second, because the preponderance of the products in "other" category are freeware products, or freeware versions of products, such as HipChat, Slack, and Skype. These freeware products are not under corporate control and, thus, more prone to ever-present security threats.

PERSISTENT GROUP CHAT PLATFORM

Persistent group chat is the latest iteration of written communication and it is constantly evolving. Organizations review security, customization, and guest interaction functionality when selecting a particular vendor platform. Persistent group chat allows people to create chat rooms or spaces where they can share information. The information is archived and preserved for access in the chat room log, providing the ability to see and review any conversation from start to finish.



Group chat is fast and easy to access from any device and can be set up as one-to-one or many-to-many and include: file sharing, screen sharing, video chat, and audio calls in a single platform. As with all infrastructure technology, security with persistent chat platforms is important and comes in many flavors. Two key security factors organizations examine are room moderation and encryption. Room moderation is the ability to control who has access to a particular chat room. Encryption capabilities ensure that confidential conversations remain confidential. This requires encryption at rest, and in transit, on all devices, as well as the ability to keep the encryption keys out of the hands of untrusted parties.

Teams collaborating on projects, such as development or marketing teams, find persistent group chat particularly useful. All the project information can be maintained in a single location for the entire team to access anytime, as needed, keeping everyone up-to-date—in one location. Approximately 60% of organizations surveyed do not use persistent group chat.

The products used for communication and collaboration, while generally falling into one or another category, i.e. web collaboration, IM, group chat, often have features that cross categorical lines. As the communication and collaboration products expand and mature, the categories blur and consolidate. Today, depending on the vendor selected, functionality can span multiple categories for: voice, IM, video, screen sharing, file sharing, presence, and persistence. Choice of which products to use should be made based upon an organization's use cases (communication needs and practices) and the budget of the organization.

SECURITY

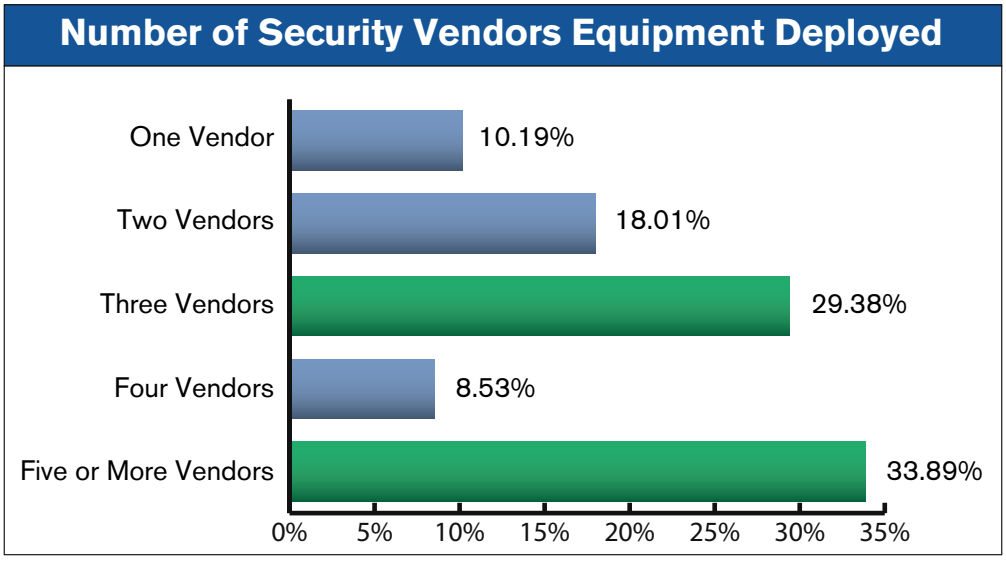
Implementing and maintaining a resilient, enterprise-quality security infrastructure is both complicated and critically important for the safety of the organization and its customers. New and improved technology is continually developed and available in response to the escalating threats to networks worldwide.

Organizations are aware, some painfully so, of the threats to their operational security, and most have implemented protection measures. The challenge to maintain focus on this particular aspect of IT, and maintain up-to-the-minute knowledge and fluency with evolving technology, is difficult to manage among all the other pressing IT tasks.

SECURITY VENDORS

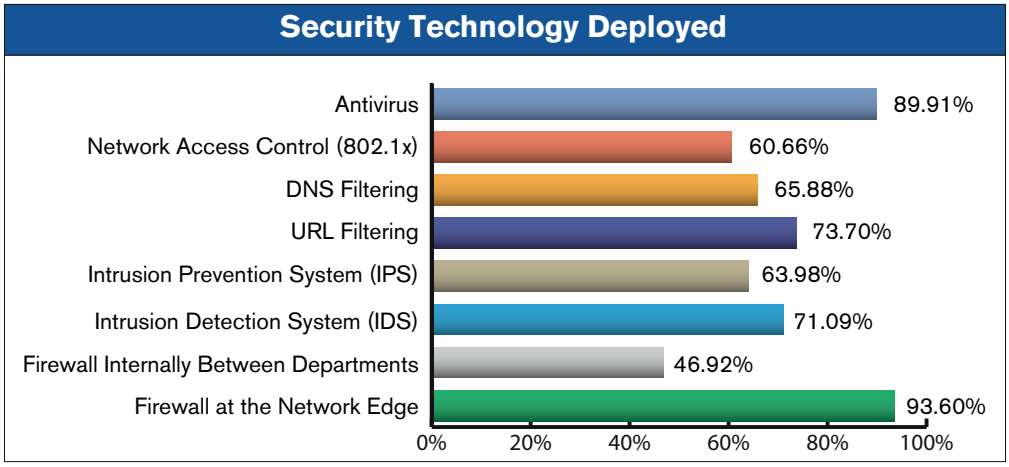
The number of security vendor's equipment deployed speaks to the complicated and continually evolving nature of security technology. In general, a single vendor cannot protect an organization against all breaches at all times. When assessing a security vendor, organizations examine response times; how quickly the vendor can respond to breaches and vulnerabilities, in addition to how well a vendor can protect the organization.

Only 10.19% of organizations surveyed found security equipment from a single vendor sufficient to meet their requirements. Two factors can be at play here. The networks may be very simple, or the in-house IT team may not be sufficiently conversant with the potential threats to determine that they may need more robust and varied technology. These conclusions are reinforced by the response data which shows that over 60% of organizations use either 3 or 5+ security vendors' equipment to secure their network infrastructure. Organizations that fall into the "One Vendor" for security equipment category may want to consider engagement of an IT services provider, with deep security expertise, to review and evaluate the security quality of their infrastructure.



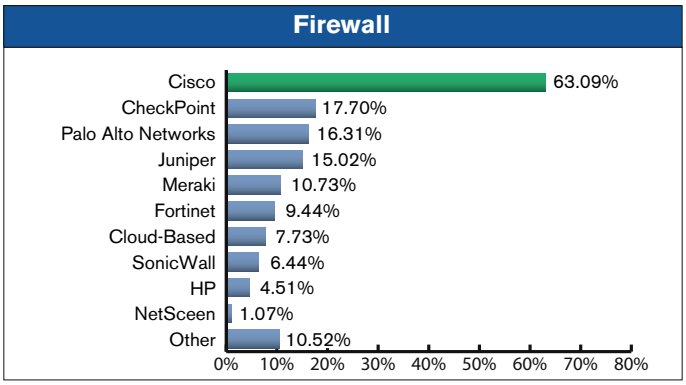
SECURITY TECHNOLOGY DEPLOYED

The breadth of security equipment available to protect organizations' networks, communications, and data can be daunting to consider. Furthermore, a firm understanding of the interactions among these devices is required to design and deploy an optimally secure infrastructure. Most organizations have implemented basic security technology. Basic being firewalls and anti-malware software. In addition, 60-73% of organizations have variously deployed Network Access Control (802.1x), DNS and URL Filtering, and Intrusion Prevention and Detection Systems. This means that 30-40% of organizations have only basic security protection and, if the firewall is breached or the anti-virus software fails, they are wide open to intrusion and malicious attack.



FIREWALL EQUIPMENT DEPLOYED

Firewalls are standard network equipment with usage approaching 100%. Not surprisingly, considering Cisco's dominance in the network equipment market, they are the highly-preferred vendor for firewall equipment, with almost 70% usage across the organizations surveyed.

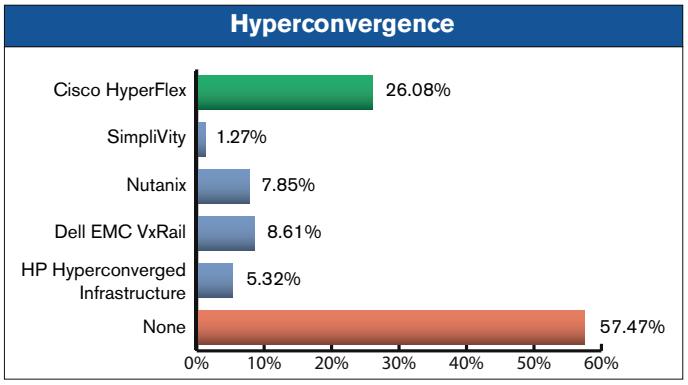


When selecting a firewall, organizations often check to ensure the firewall they choose can provide the latest capabilities available. These firewalls are sometimes called, "next generation" firewalls. IT best-practices dictate regular review of any technology choice, including a firewall, against both current and future needs of the organization for the planned life of the device. Organizations perform regular technology reviews to assure all devices are capable of protecting their infrastructure against the latest security threats.

TURBOCHARGING IT

HYPERCONVERGENCE

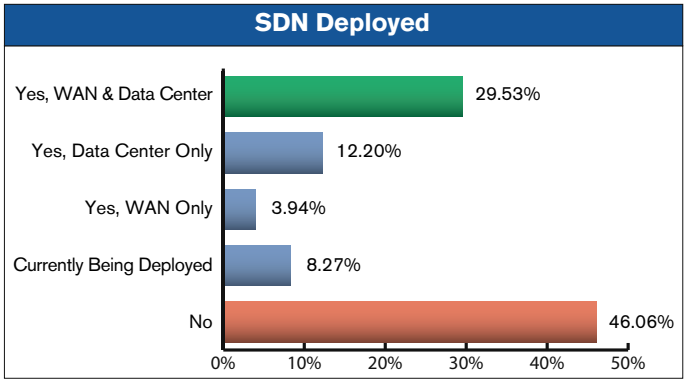
Hyperconvergence is an IT framework that combines storage, computing and networking into a single system to reduce data center complexity and increase scalability. The elements of a hyperconverged platform are: a hypervisor, to create and run virtual machines; software-defined storage for data management; and a virtual network. Multiple nodes can be combined to create convenient groups of shared storage and computing resources. In general, hyperconverged platforms use off-the-shelf servers. Using single-vendor, standard hardware provides a much more flexible and easy-to-manage infrastructure compared to a traditional enterprise storage infrastructure. IT leaders embarking on data center modernization projects, are considering and adopting hyperconvergence to provide the agility of public cloud infrastructure without relinquishing control of hardware on their own premises.



Major factors driving hyperconvergence adoption are cost/ROI, operational efficiency, high-availability functionality, ease of scalability, integrated backup and replication, global management, and single-vendor purchase and support. Hyperconvergence infrastructure is a relatively new entry into the IT market as indicated by our survey results which show over half of survey respondents are not yet using hyperconvergence technologies.

SOFTWARE DEFINED NETWORKING (SDN)

Prior to virtualization, the physical locations of servers and other network devices were static and seldom required network changes to maintain functionality. Those days are gone. With the advent of virtualization, network resources (servers) are increasingly mobile—they can move between data centers and, between private and public clouds. In addition to resource mobility, server virtualization also allows fast provisioning of new resources whenever and wherever they are needed. As with network resources, users are also increasingly mobile. These changes to the information landscape have increased network complexity and the effort required to deliver expected levels of service. SDN reduces the time required to effectively support today's more complex and ever-changing networks.



Many conventional networks are hierarchical, built with tiers of ethernet switches arranged in a tree structure. This design made sense in static client-server computing environments. However, it is not a good fit for the dynamic computing and storage needs of today's organizations.

SDN comprises multiple types of network technologies designed to make a network more flexible and agile. Network administrators can, dynamically and programmatically, initialize, control, change, and manage network behavior, via open interfaces. SDN supports the dynamic, scalable computing and storage needs of more modern computing environments.

A recent Gartner report estimates that 60% of enterprises will phase out network VPNs in favor of software-defined perimeters by 2021 (Source: It's Time to Isolate Your Services from the Internet Cesspool). Our new survey results indicate SDN implementation traction with: WAN and data center SDN deployment in nearly 30% of respondent organizations, partial deployment in another ~16% of organizations, and 8.27% of organizations with SDN implementation projects underway.

SDN design and implementation is an area where many organizations seek the expertise and experience of outside IT services providers because the design and technologies involved can be complex.

SDWAN/WAN OPTIMIZATION

The rapid escalation in the number of devices connecting to organizations' networks—plus other trends including bring-your-own-device (BYOD) environments, guest access, and the Internet of Things (IoT)—add to the bandwidth demands that IT teams manage.

IT must optimize application traffic to efficiently handle the high-bandwidth software that has reached the critical stage—fed by remote workers, branch offices, and geographically dispersed customers. IT teams require application optimization to allow them to intelligently manage WAN capacity with real-time network status, as well as accelerate and prioritize the most critical applications to meet user expectations.

WAN optimization and intelligent path selection, also known as Software Defined WAN (SDWAN), is a category of technologies and techniques used to maximize the efficiency of data flow across a wide-area network (WAN). In an enterprise WAN, the goal of optimization is to reduce the bandwidth required for critical applications and information.

An organizational goal of SDWAN deployment is to maximize the high cost of dedicated, private, high-quality networks such as MPLS or VPLS, while making better use of low-cost circuits such as internet or broadband. SDWAN helps organizations achieve both cost reduction and improved performance with a single strategy.

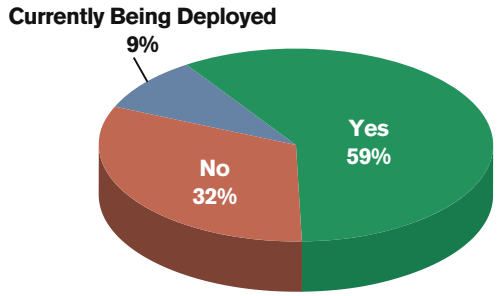
When choosing an SDWAN/WAN optimization vendor, organizations examine the vendors' abilities to provide the base operations (optimization and path selection), the flexibility to choose which data receives what treatment, and the analytics of the system. Analytics allow organizations to monitor the ever-changing network, provide the ability to demonstrate the ROI, and to better anticipate the WAN needs of a growing company.

59% of survey respondents have deployed WAN optimizations, and another 9% are in the process of deploying WAN optimization to reap the benefits of fast access to applications and data. However, despite the obvious high value of WAN optimization, 32% of organizations surveyed have not adopted the technology.

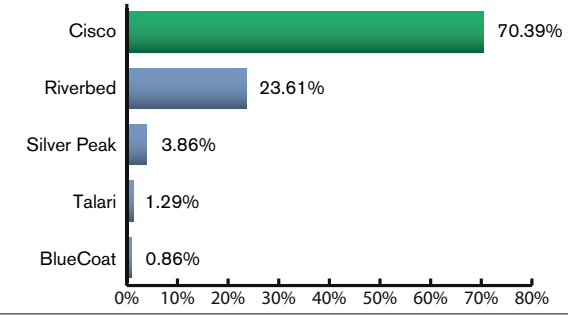
WAN OPTIMIZATION EQUIPMENT DEPLOYED

Of the 59% of respondents who are currently using WAN optimization to facilitate application and data access in their organizations, approximately 70% are using Cisco equipment.

WAN Optimization Deployment



WAN Optimization



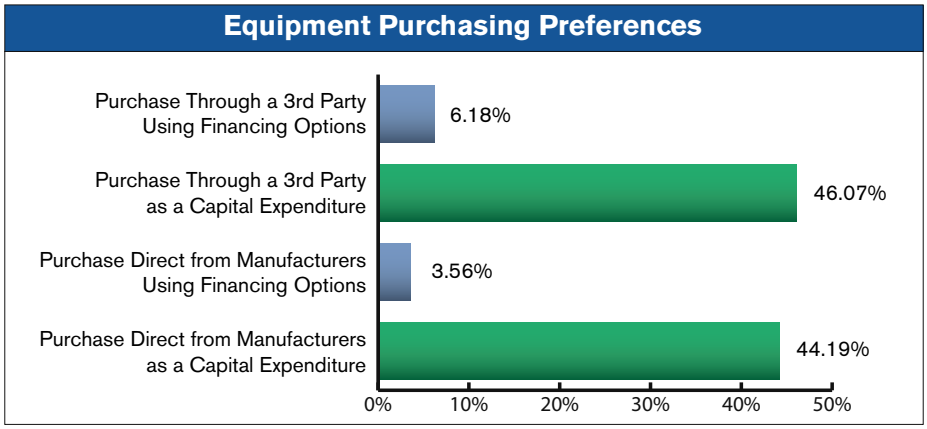
PART 3 – INFRASTRUCTURE & WHAT KEEPS IT AWAKE AT NIGHT

SNAPSHOT OF FINDINGS

- 48.69% of organizations have no application infrastructure in the cloud.
- 64% of organizations deploy virtualized desktop infrastructure to reduce total-cost-of-ownership (TCO).
- Security is the #1 focus of 44.84% of organizations nationwide.
- Email and web browsing are the highest concern network attack vectors for organizations' IT teams.

EQUIPMENT PURCHASING PREFERENCES

Across the categories of equipment, organizational purchasing preferences split approximately equally between using 3rd party IT services providers to manage their equipment purchases and buying direct from equipment manufacturers. Regardless of whether equipment is purchased through a 3rd party or direct, overwhelmingly, 90.26% of organizations chose to make their equipment purchases as capital expenditures.



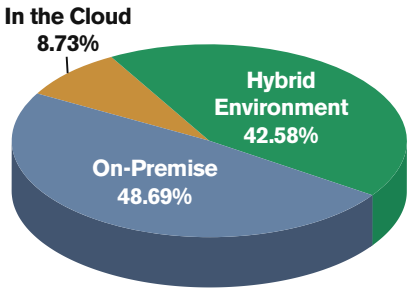
APPLICATION INFRASTRUCTURE

APPLICATIONS – ON-PREMISE OR IN THE CLOUD

Running applications in the cloud provides today's mobile, multi-device, workforce with flexible, anytime, anywhere access—whether delivered as a service, hosted and managed by a third-party IT services provider, or managed and hosted by the organization.

Organizations that choose a cloud strategy, determine which applications, and what aspects of those applications, to run in the cloud. For example, if an organization migrates LDAP to the cloud, the cloud holds all aspects of the application. By comparison, migration of organizational infrastructure to the cloud, only migrates the management of the infrastructure, as physical equipment remains on premise. Such decisions are weighed against desired functionality and organizational benefits, security implications, and cost.

Core Applications Location



Despite the cloud convenience of anytime, anywhere access for users, only a small 8.73% of organizations are running all of their core business applications in the cloud. The remainder of survey respondent organizations split between maintaining all of their core applications on premise and in hybrid environments. This for a variety of reasons, including security concerns. Generally, the hybrid environments run the common desktop applications in the cloud for mobile convenience and, the corporate business applications remain on premise for security concerns.

VIRTUALIZED DESKTOP INFRASTRUCTURE

Virtual desktop infrastructure (VDI) is technology that hosts a user's desktop environment on a centralized server. A server that can, in theory, reside anywhere and is accessible via the Internet. Desktop virtualization separates the operating systems, applications, and data from the users' hardware devices. Because applications and data are managed, stored, and secured centrally, there are many benefits.

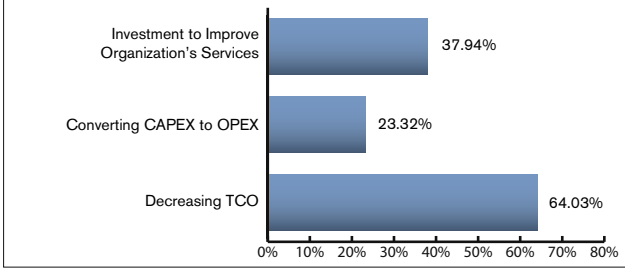
For IT, virtual desktops can help reduce the time it takes to provision new desktops, and decrease the time spent on desktop management and support. The IT tasks of managing users' devices to install, update, and patch applications, as well as back up files and scan for viruses, are reduced to management of the centralized application infrastructure.

Virtual desktops often suit the needs of the increasingly mobile and remote workforces of many organizations. Users can access their virtual desktops anytime, anywhere, across their hardware devices, increasing their productivity. With respect to cost, the devices that can access a virtual desktop are less expensive than standard laptops or desktop computers because no storage is required for the VDI-supported applications and data, and computing power can also be centralized. Security is also increased since users do not have applications and data on their devices which can be lost or stolen.

As the survey data confirms, organizations often adopt VDI technology to decrease their total-cost-of-ownership (TCO) in end-user computing equipment, convert this CAPEX to OPEX (IT services), and to improve computing services for the organization's mobile workforce.

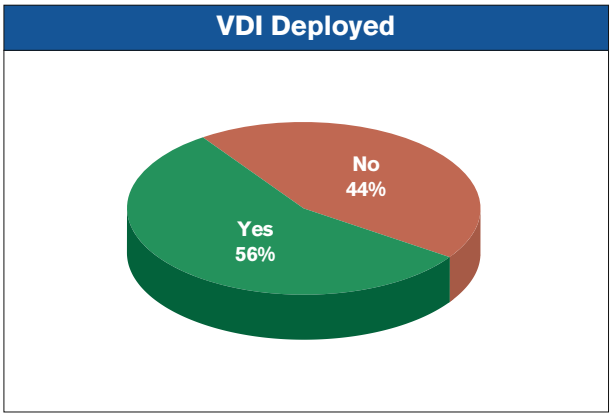
Organizations that have adopted VDI must have a good understanding of the applications used and their compatibility with VDI. For instance, real-time applications, such as voice and video, are processor intensive and often offload these capabilities to the local device (thin client) to perform optimally and reduce the burden on the centralized VDI environment.

Rationale for Using VDI

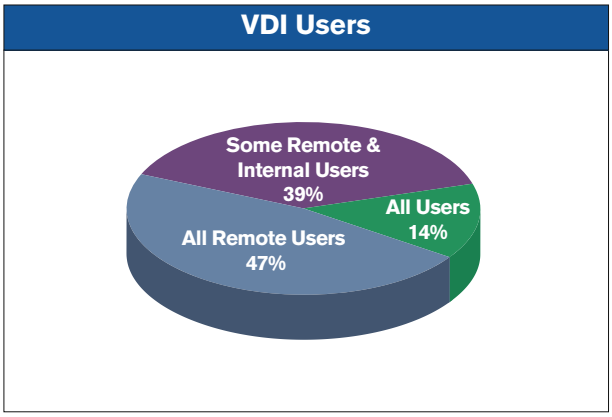


Organizations that do not have IT staff and/or expertise to maintain the VDI software and centralized servers, engage IT services providers to host and manage their VDI services.

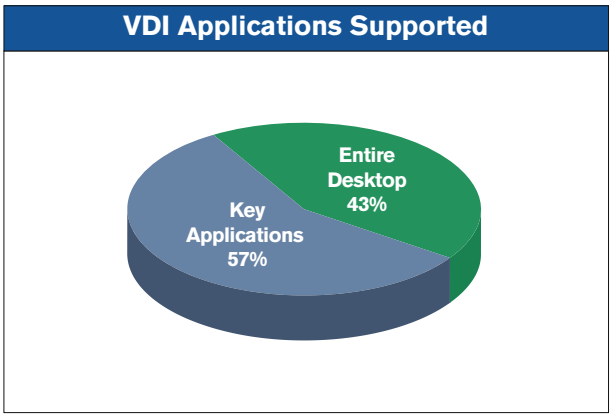
VDI deployment among the survey respondents is fairly evenly divided, with organizations using VDI, in part or in whole, 12% greater than the percentage of organizations not using VDI at all. This speaks to the broad range of organizations surveyed and the structure of their workers' locations—mobile, remote, home, and on premise.



VDI increases security because it prevents mobile and remote users from carrying devices containing valuable corporate applications and data that could be lost or stolen. The figures for remote user VDI deployment demonstrate organizations' desire to maintain tight security of their applications and data. Of the organizations using VDI, 47% have deployed it for all remote users, and 14% have deployed VDI for all users—both inside their networks and working remotely.



The applications chosen for VDI deployment divide among the key, and sometimes proprietary, organizational applications, the standard business applications, and some special purpose applications that only a few of the users require. The business and/or special purpose applications can reside on the end-user device, be added to the VDI deployment, or can be third-party SaaS applications for which access and security is managed by the third-party vendor. Of the organizations that have deployed VDI, 57% have VDI for their key corporate applications, and 43% or organizations have adopted VDI for the entire desktop.

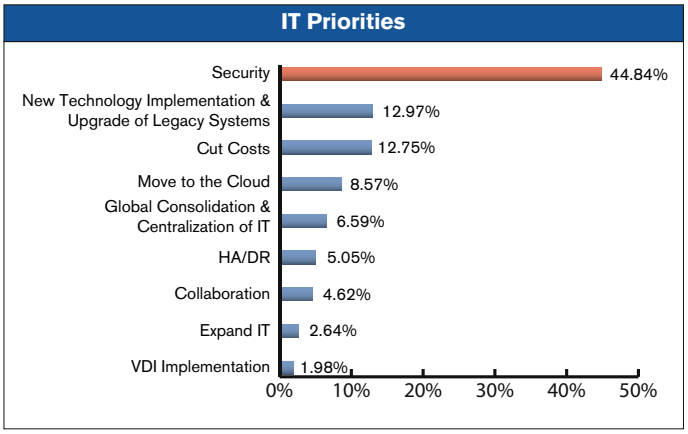


WHAT KEEPS IT TEAMS AWAKE AT NIGHT

IT teams surveyed across the United States are challenged by the planning and costs of keeping up with:

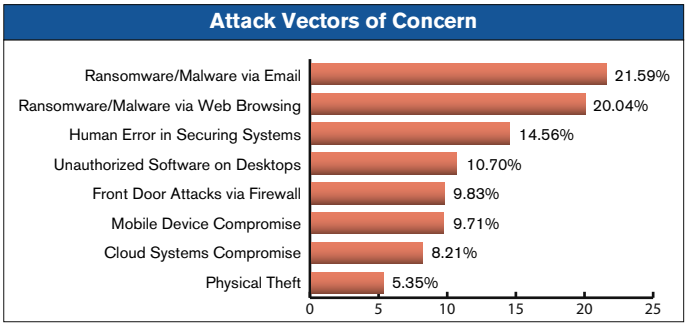
- Rapidly evolving IT technology options.
- Expanding array of user devices accessing their organizations' networks, applications, and data.
- Growing mobile and geographically dispersed workforces working around the clock.
- Escalating sophistication and frequency of security threats to their organizations data.

When considered as a whole, the challenges sum to implementing cost-effective, flexible technology solutions and the ability to keep the entire infrastructure secure. It follows that when asked for their #1 priority, 44.84% of respondents named security—followed by new technology implementation and legacy systems upgrade, cost reduction, and cloud deployments. The small percentage of organizations without proper business continuity planning are focusing on that initiative as a priority as well.



ATTACK VECTORS

With security being the runaway highest priority across organizations, the detailed data on the potential attack vectors was examined. The data reveals that the leading concerns center around employee-application usage—in particular email and web browsing—high-daily usage activities that expose organizations' networks to malicious social engineering such as phishing. Installation and use of unauthorized or unapproved software applications on the employees' desktop computers is the fourth largest challenge for organizations, because these applications can contain malware that allows infiltration of the organization's network.



SUMMARY

The 2017 U.S. IT Services Report illustrates that organizations are like small countries with valuable resources—information and people—that require services and protection. In order to service the employees, IT teams are constantly expanding the range of technology available within the organization to the employees. In order to protect those resources, IT teams endeavor to put plans and procedures in place that control usage and access to the information, while concurrently implementing new technology to support the needs of the employees. Employees are human and their goal is to accomplish their work in the most straightforward manner possible. When IT cannot service their needs, employees seek other solutions that can endanger the security of the organization. Lastly, the increasingly sophisticated and expanding range of malicious intrusions into organizations' networks keep IT teams ever vigilant—looking outward as well as inward—to maintain organizational safety and security.

PARTICIPANT PROFILE

The survey participants hold IT management positions in organizations with IT teams ranging in size from 1 to 50+ members. Over half of the respondents are managing teams on the high-end of this spectrum. The respondents have responsibility for maintaining smooth, secure, and efficient IT infrastructures for their organizations.

RESEARCH METHODOLOGY

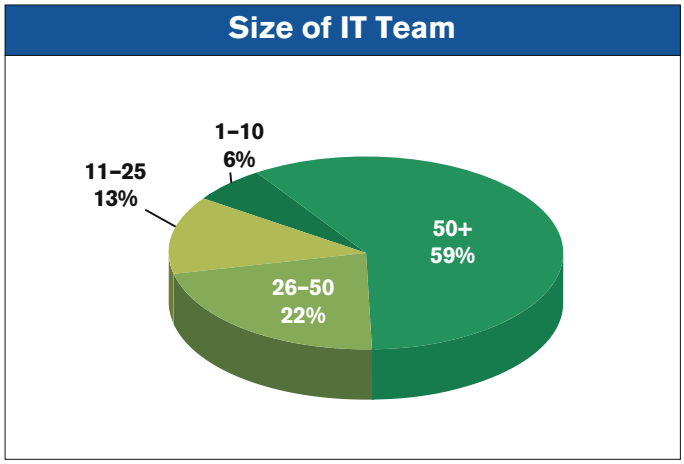
Participants were asked multiple choice and open-ended questions about their current IT infrastructure including: plans, equipment installed, platforms deployed, usage across their organizations, and priorities for IT services.

ABOUT RESEARCHCORP.ORG

ResearchCorp uses a time-tested process, ensuring we interview the people who can give us the data our clients need. Our team leverages a combination of in-person, phone and online focus group research conducted world-wide, enabling us to interpret the data, and present top-level summary and detailed reports with recommendations.

ABOUT FIDELUS TECHNOLOGIES LLC

Fidelus Technologies LLC, is a leading professional and managed IT services firm, headquartered in New York city. The company provides on-site and managed IT services across a broad range of technology solutions to organizations across the United States.



For more information contact:

Fidelus Technologies LLC
240 West 35th Street, 6th Floor
New York, NY 10001 USA
1-866-343-3587
www.fidelus.com