

Networking and Unified Communications for Government

TABLE OF CONTENTS

- 2** Introduction to Networking and Unified Communications
- 3** The Data Center
- 4** Unified Communications
- 5** Security
- 6** Key Manufacturers

Executive Summary

It doesn't take dire economic conditions to prod government agencies into finding better ways to carry out their missions. Agencies are continually seeking ways to either improve operational capabilities or decrease costs — preferably both at the same time. This holds true for network infrastructure, which is an integral part of an agency's operations and service to citizens.

As network technology has grown in sophistication, techniques and applications have been developed to make the network run more efficiently. This is done in a variety of ways. Two of the main areas of focus have been application acceleration and bandwidth optimization.

Another path to improving the network has been through the centralization of network management. Centralization is a key process for decreasing the total cost of ownership, and thus saving money, on the network. This can be realized through virtualization and server consolidation, two technologies that aim to make better use of an agency's IT resources.

Unified communications offers another path to a more centralized network. Increasing application functionality and productivity, unified communications gives staff the tools they need to increase collaboration and become more productive.

Two of the bright spots in the development of unified communications are mobile solutions and video communications, technologies that are reshaping the future of government and how it services its constituents.

.....

Introduction to Networking and Unified Communications

IT managers face a difficult task in trying to offer robust services and applications while also having to reduce operational costs. Applications continue to become more complex, and the applications' reliance on a resilient network continues to become even more pronounced. Software manufacturers increasingly create applications that utilize the resilient nature of IP and assume a high level of service availability for those applications.

IT infrastructures must provide dynamic and scalable services that not only deploy easily, but also allow agencies to add functionality as required. IT managers have an obligation to decrease the total cost of ownership (TCO) and increase return on investment (ROI), while still meeting the functional challenges of the data center.

While seeking to meet these sometimes conflicting needs, technical managers work to boost services by adding various application acceleration and bandwidth optimization devices to the network. These network devices enhance the responsiveness of critical IP-based applications.

Network Solutions Trends

Some of the network solutions available that enhance an existing network infrastructure include application control engines (ACEs) and wide area network (WAN) acceleration and application services (WAAS).

Agencies are also converging security and networking functions into one robust and easily managed solution. These initiatives, necessary to decrease TCO, nevertheless add to the complexity of the traditional IP network. Two other initiatives, virtualization and server consolidation, have similarly increased the importance of the network.

The proliferation of continuity of operations solutions has resulted in a need for redundancy via network-based storage. Agencies need network storage devices that provide a scalable solution independent of traditional distance constraints.

Many server managers have leveraged their existing server resources through virtualization, using the network to distribute applications over a larger IT landscape. This added functionality requires network solutions that are highly integrated, scalable, robust and easily managed.

To simplify management and ensure that no single solution operates without oversight, it is necessary to provide unification via an overarching management tool. Agencies now regularly depend on such network management solutions to identify outages and other network problems proactively rather than reactively.

Unified Communications Trends

Having laid network foundations with local area and wide area solutions, application functionality and productivity for the staff become primary concerns. With unified communications (UC), IT departments can offer

Consolidation and virtualization technologies facilitate a more efficient use of an agency's IT resources. Here are three approaches to consider:

- **SERVER AND APPLICATION VIRTUALIZATION:** This technology enables an organization to take multiple physical servers, typically underutilized, and consolidate them onto a smaller number of physical servers.
- **BLADE SERVER CONSOLIDATION:** This approach fits your servers compactly into a smaller rack space while saving on cabling, power and cooling costs.
- **APPLICATION CENTRALIZATION/OPTIMIZATION:** This technology permits an organization to migrate its remote office applications and data into the data center, while allowing fast and efficient access out to remote workers.

streamlined communications solutions and advanced productivity applications throughout the network.

Because of the facets it incorporates and combines, UC is a powerful and complete communications medium. It has unquestionably changed, for instance, the way agencies provide connectivity between staff.

Whether at a desk, a branch office, working from home or connecting via cell phone, a staffer needs access to the same services and levels of functionality. Today's combined advances in networking and UC allow the IT department to make this happen.

Advanced UC applications, for example, provide the real-time status and availability of other staff, including preferred methods of contact. With this level of presence, staff members can quickly determine which staffers are accessible and in what capacity.

Mobility solutions further extend the capabilities of the communications network beyond the confines of the agency. Regardless of location, mobility can provide presence and voice communications via smartphone technology as if the staffer were physically in the office.

Video communications and desktop collaboration have emerged as promising UC solutions. Both provide tremendous benefits. Eighty to 90 percent of human communication is based on visual queuing. So video serves as a logical extension of the UC network.

Add the functionality of desktop collaboration — the ability to share documents, presentations and any stored media — and UC becomes not only thoroughly versatile but increasingly indispensable in today's communication environment.

The Data Center

A data center is a central environment, whether physical or virtual, that houses and distributes data through various applications. Recently, bandwidth and energy cost increases, coupled with increasingly complex IT environments, have led many government agencies to consolidate their infrastructure by removing applications and data from remote offices and staff PCs and placing it all into a centralized data center.

With the onset of Voice over IP (VoIP), video conferencing and streaming media, the network has become even more critical to agency operations than ever before. It takes a highly skilled network architect to design the type of complex networks needed for a consolidated data center and a seasoned systems engineer to implement them. Agencies need to put a great deal of planning and thought into any consolidation activities.

Cloud Computing

Consolidating the data center allows agencies to provide rich applications, simplify management, build in redundancy and strengthen security. By centralizing remote office servers, virtualizing underutilized servers onto fewer physical ones and shrinking those physical servers down into blades, you can create an environment that proves far easier to manage, protect and secure.

Many IT departments now aim to achieve a “cloud computing” environment, with applications essentially “removed” from the hardware, allowing for more efficiency, easier management, better resiliency and lower overall IT costs.

Cloud computing involves separating the data center into an application cloud, a hardware cloud and a computing cloud. Rather than tying specific applications to hardware (such as servers, network ports, etc.), the applications can be separated and managed as independent clouds.

As a result of this independence, applications can move from server to server, or even data center to data center without performance degradation or data loss. Hosting applications that formerly resided on individual desktops further enables users to access necessary applications from anywhere.

Many options exist for hosting shared applications, including but not limited to application virtualization, desktop virtualization and blade PCs. Agencies can gain numerous benefits from a shared application cloud. Disaster recovery, in particular, can benefit from this arrangement.

For example, if agency staff can't get to the office because of a disaster, remote access to centralized applications allows users to securely obtain what they need from a home computer or other remote device or location.

Storage consolidation often goes hand-in-hand with server consolidation. Not only are agencies centralizing their ever-growing storage resources, but virtualization has also become a substantial driver, since virtualized servers reside on the storage area network (SAN). Until recently, this fact had little impact on the Ethernet network. But, today, a convergence of technologies has begun.

For years, storage connectivity was either direct-attached via Small Computer System Interface (SCSI) or by means of a separate Fibre Channel (FC) network. Because of the cost of FC networks, many organizations have now embraced iSCSI as an alternative connectivity method. This method encapsulates block-level SCSI traffic in IP packets for transmission across the network.

An even newer technology is Fibre Channel over Ethernet (FCoE). This protocol transmits the highly resilient and efficient FC protocol over a standard Ethernet network and allows for the use of existing FC storage arrays. This convergence puts even more demand on the network, which requires low latency, high throughput and built-in resiliency.

Designing a Resilient Network

When designing a resilient network, one must first determine the requirements to support the agency's functions and develop a network strategy accordingly. In most government agencies, an IT governance committee consisting of upper-level management helps establish the operations requirements of the network.

After establishing the requirements and developing a network strategy, the planning phase begins. This includes getting an accurate assessment of the current environment and a gap analysis to determine if the existing infrastructure, sites and production environment can scale to include a new, resilient infrastructure.

The actual design of the network is the third step in building a resilient network. The network design must incorporate all gathered information

A network assessment is a key step in rolling out a resilient network. Agency IT managers should take the following into consideration as they assess their networking needs:

- Current applications and data on the network, such as VoIP, e-mail, structured query language (SQL), common Internet file system (CIFS), Internet and video-on-demand
- Current network topology, including but not limited to: network devices, physical and logical links, external connections, frame types, routed and routing protocols, application specific protocols, IP addressing scheme, and traffic and network utilization analysis

concerning operations and technical requirements. It must also include specifications for availability, reliability, security, scalability and performance.

Network engineers commonly recommend designing a resilient network in modules. Modules allow an agency to provide the highest degree of resiliency by segmenting traffic and preventing a single point of failure. It is crucial to eliminate single points of failure. This is achieved by creating redundant links to critical servers and network devices. Redundant links can create problems, however.

For instance, in Layer 2 switched environments, redundant links can cause switches to flood packets throughout the network, effectively halting the switching of production traffic. Spanning tree protocol (STP) is a Layer 2 protocol designed to prevent such flooding by placing one of the redundant links in a blocking state.

At Layer 3, advanced routing protocols enable the highest level of network resilience when utilizing redundant links. Not only can advanced protocols load-balance traffic over redundant links, but they can converge in a matter of seconds in the event of a primary link failure.

Unified Communications

Unified communications gives agencies the ability to offer a seamless user experience to staff regardless of location. These technologies now expand further than ever from the user's desk and include such devices as the standard office telephone, mobile phones, PDAs, notebook computers, e-mail and video solutions. Integrating all of these disparate technologies has become essential for government agencies.

By bringing UC solutions to a centralized and secure environment, agencies can apply rapid changes to the entire environment as well as provide enhanced security and management. Centralization also allows an agency to add many more advanced applications to the network such as presence, instant messaging, desktop collaboration and emergency notification.

Moreover, with the advances in video conferencing from the desktop, web conferencing and desktop collaboration, agencies have the ability to place staff anywhere within the agency regardless of job function. And agencies can deliver consistent and tailored access to users based on the unique requirements and circumstances of those users.

Advanced Applications

Advanced applications are the next wave of unified communications solutions. Presence is one of the newer technologies and shows great potential. Unified presence is a standards-based platform that collects information from multiple sources about user availability and communications capabilities.

The information is used to provide rich presence status and facilitate presence-enabled communications. Presence applications allow staff to see the availability of others in the UC network instantly.

Instant messaging (IM) is another UC technology that's proving very useful at government agencies. IM facilitates real-time, text-based communication between two or more participants over the Internet or some form of intranet. What separates IM from e-mail is the perceived synchronicity of user communication.

IM services have additional features available: immediate receipt of acknowledgment or reply, group chatting, conversation logging and file transfer, and conference services such as voice and video.

Mobility

Today's work environments are increasingly mobile. By extending the UC network to devices outside the formal network (such as mobile phones,

home-office phones or two-way devices), users can establish connectivity methods based on personal convenience and preference.

UC users can now consolidate all calls with a single IP phone number and immediately connect from wherever they are working, allowing agencies to provide even more responsive service with no additional effort. Mobile workers can also manage all voicemail using a single voicemail box.

Additionally, a user answering a call on a mobile device can seamlessly transfer the call to a physical desk phone after entering the office. And a call started on a physical desk phone can equally be transferred to a mobile device.

Extending the agency's voice system for traveling staff has also become significantly enhanced in today's UC world. UC technology makes all major IP communications features available to traveling workers.

Regardless of user location, UC helps people connect via voice and video services. This kind of collaboration enables staffers for mutual engagement on critical documents in a real-time format. Whether one-on-one or in a conference call setting, collaboration permits the sharing of specific documents, computer desktops and applications.

Unified Contact Center

A unified contact center (UCC) extends the ability of a base UC solution into a true multifunctional contact center for either internal or external callers. UCC makes use of the unified communications infrastructure to deliver skills-based contact routing, voice self-service, computer telephony integration (CTI) and multichannel contact management.

By combining multichannel automatic-call-distributor (ACD) functions with IP telephony, UCC helps an agency rapidly deploy a distributed VoIP contact center infrastructure.

UCC segments callers, monitors resource availability and delivers each contact to the most appropriate resource in the agency. The software profiles each caller contact using related data such as dialed number and calling line ID, caller-entered digits, web-form submitted data and caller database information.

Simultaneously, the system monitors the resources available in the contact center to meet caller needs, including staff skills and availability, interactive-voice-response (IVR) status and queue lengths.

This combination of caller and contact center data is processed through user-defined routing scripts that graphically reflect an agency's operations rules. This processing enables the routing of each contact to the right place.

Unified Video

Current video conferencing technology has improved the user experience so that it can now be used internally among staff and externally with other departments and end users. The seamless blending of high-quality audio and video provides advantages to users on both sides of a virtual meeting, as all are privy to the nonverbal cues that further contextualize and inform dialogue.

Deploying video communications within a UC solution has now become as simple as implementing traditional voice solutions. With the addition of video-capable phones or desktop cameras, the UC control mechanism can establish a video call automatically if both parties have the capability for such service.

Along with desktop video conferencing, agencies can acquire significantly extended methods of video communications via TelePresence solutions. Offering a fully immersive video conferencing experience via the transmission of life-size, high-definition images and spatial discrete audio, TelePresence creates an innovative "in-person" meeting experience over the converged network.

Extending video communications across the agency can yield many gains:

- **EXTENSION OF UC PLATFORM:** Video telephony conferencing can become a further practical enrichment of user experience at the desktop via a unified software client.
- **INCREASED WORKGROUP COLLABORATION:** Video maximizes scheduling time during the workday by eliminating travel times between locations and incorporating access to operations-critical information and applications from the desktop. Agencies that incorporate video telephony into their UC architectures enable meeting or project participants to minimize delays that arise from participant handoffs.
- **ACCESS FOR REMOTE WORKERS AND TELEWORKERS:** Traveling and remote users often find it difficult to feel connected to colleagues. Video gives these staffers a far more palpable means of maintaining viable, productive relationships than audio-only teleconferencing.
- **REDUCTION OF TRAVEL EXPENSES AND CARBON FOOTPRINT:** Increases in gas and oil prices have made travel prohibitive for many government staff. In conjunction with financial initiatives to limit travel, many agencies are taking on a social responsibility to decrease their carbon footprints.

Security

The notion of perimeter security holds little meaning in today's computing environment, which includes flash drives, Skype (software for telephone calls over the Internet), instant messaging, IP-enabled phones, notebooks connecting to diverse networks of varying quality, virtual private network (VPN) and web portals accessible from a foreign PC and guest/contractor access to both internal-wired and wireless segments.

To address potential threats while providing access to the network and its services, agencies need to think about security in new ways. Security based purely on strong edge protection is no longer sufficient. A variety of strategies need to be implemented.

Virtual Private Network

Securing communications for agencies is done via a VPN. VPNs provide a private, encrypted network connection. This is done via Secure Sockets Layer (SSL) VPNs, which are VPNs utilizing cryptographic protocols that encrypt traffic at the transport layer of a connection.

SSL refers to all common protocols for encrypting websites, including SSL version 3 and Transport Layer Security (TLS). Both have the capacity to encrypt not just web traffic but any traffic.

SSL VPN refers to two different types of remote access experiences: a customized web portal that provides access to key network services and applications, and a full tunnel SSL client that provides like-for-like replacement of the full tunnel IP security (IPsec) client.

Network Access Control

Network access control (NAC) determines device access to a wired or wireless network. More specifically, NAC can assess the state, or posture, of a network device.

Based on device posture and user identity, NAC determines what network services the device should be granted. NAC provides both an architecture to repair unhealthy devices before they attach and prevents unauthorized ones from attaching.

There are three common deployments:

- **INLINE NAC:** For most small- and medium-size networks, inserting an inline NAC appliance into the network on one or more virtual local area networks (VLANs) represents the easiest method of deployment. The appliance then intercepts all IP/MAC layer traffic and adjusts the VLAN assignment according to the device's role (such as inside, guest or quarantine).
- **OUT-OF-BAND NAC:** For medium-to-large agencies, an out-of-band NAC appliance provides the benefits of inline NAC without the risk of network bottleneck. Only the posture assessment traffic is required to go through the NAC appliance. Upon completion of the assessment, NAC adjusts the VLAN and access lists of the switch port to which the host is connected.

- **DHCP REGISTRATION:** For large agencies, especially those that cannot use a NAC agent because of lack of workstation control, dynamic host configuration protocol (DHCP) registration systems provide a workstation- and network-agnostic solution. Rather than enforcing security through VLANs, as in the first two options, a DHCP registration system uses overlapping IP subnets to achieve the same goal.

Firewalls

The network firewall serves as the most basic defense in the network. It provides a state-aware security barrier between different network trust zones. Often, an agency deploys its first firewall at the Internet edge and uses it to separate the internal agency network (the trusted inside) from the Internet (the untrusted outside).

The firewall presents public-facing services, such as web, FTP and e-mail, to the Internet. However, it places these services in a third security zone, a demilitarized zone (DMZ). Additional security zones can be added as needed. Because firewalls separate security zones that possess varying levels of trust, agencies implement a firewall wherever a differentiation of trust occurs.

Application-layer firewalls have the ability to look beyond the TCP header and into the application protocol. This visibility allows the firewall to sense protocol violations, attacks or negotiation to a different port.

Web application firewalls will actually proxy HTTP and HTTPS traffic, effectively brokering the connection. This “man-in-the-middle” approach allows the web application firewall to comprehensively protect public-facing web servers.

Additional capabilities in newer firewalls include content inspection, malware protection and even antispam protection. Turning on additional services, however, may impact the performance of the firewall.

One final option is personal firewalls, which provide a base firewall capability at the PC level. If the PC initiates the connection, the firewall permits return traffic. It denies any other traffic, however, unless explicitly permitted.

Intrusion Prevention Systems

An intrusion prevention system (IPS) is an active security technology that can block security threats in real time and reset network connections as necessary.

Leading IPS systems have developed a few key features that dramatically improve the value of the technology:

- Inclusion of protocol engines to detect some of the more common, sophisticated attacks based on protocol violations, TCP replay and IP fragmentation
- Contextualization of fired signatures that provides more value to the event (such as: What is the value of the potential victim host? How can one trust that the fired signature is a real security threat? How severe is the attack if the fired signature denotes a real threat?)
- Alerting on statistical network traffic anomalies
- Collaboration with security event management products to collect and correlate security threats and actively alter IPS behavior based on a changing network security posture
- Incorporation of IPS features into existing networking products such as routers and firewalls, resulting in fewer appliances to manage and more straightforward, high-availability designs

In the last few years, IPS has tipped into mainstream adoption. Intrusion prevention is typically deployed first at the Internet edge, next at the data center and finally at the WAN edge or remote office as necessary.

Key Manufacturers

Government agencies have numerous options for finding the right networking and unified communications solutions for their needs. Several manufacturers offer both networking and unified communications products.

Cisco

Cisco covers the full spectrum of networking products including switches, routers, network management tools and software. Two types of switches are available from the manufacturer: modular and fixed-configuration switches.

It manufactures several different series of routers, including the ASR 1000, the Catalyst 6500, the 7600, the 7200, the 3800 integrated, the 2800 integrated, the 1800 integrated, the 800 and the SB100. Each series is designed to meet particular routing needs.

Cisco's vast array of network management tools can assist agencies in numerous areas: performance assurance, routing and switching

management, identity management, and video, cable and content delivery management. The manufacturer has an even larger array of software and operating systems solutions available that cover everything from broadband aggregation to WAN optimization, from mobile IP to VPNs.

Cisco is also a major player in the area of unified communications. It offers IP telephony software and hardware including phones, UC applications and hardware, contact center applications, communications infrastructure products and UC management tools.

One of Cisco's premiere UC products is TelePresence. This product delivers real-time, face-to-face interactions between people over a converged network utilizing advanced visual, audio and collaboration technologies. TelePresence does this by transmitting life-size, high-definition images and spatial discrete audio, allowing participants the added communication feature of discerning facial expressions that are typically lost over video.

Consider the following when evaluating IPS systems for your agency's environment:

- Take into account the performance implications when looking to add IPS as a service or module on a firewall or router. Typically, the firewall or router has a much higher throughput capacity than the IPS. Will the IPS impact throughput meaningfully?
- Identify the current monitoring strategy. Some agencies automatically protect against the most severe threats and log the remaining information without active monitoring — a low-cost, administrative approach. To get a comprehensive view of the network's security posture, though, a security event management technology is recommended.
- Ask the following questions: Where should I position the IPS? Where are the threats? Where is my most sensitive data located?

Microsoft

Microsoft has a presence in the UC world through their two server offerings: Office Communicator 2007 and Exchange Server 2007. Office Communicator 2007 assists with real-time communications, enabling several different communications options including instant messaging, voice and video. Utilizing presence features, this product allows users to share information about their availability and preferred method of communication.

Exchange Server 2007 is a sophisticated messaging system. With this product, agency computers gain the functionality of advanced IP phones. Staffers can simply click to call anyone in their address book. And simple phone calls can quickly be transformed into a conference call or a video conference. Additional functionality includes voicemail and fax delivery via e-mail, and access to e-mail and address books via a standard telephone.

The 2007 version emphasizes built-in protection technologies that keep communications available and safeguards against spam and viruses; anywhere access via a single inbox for all communications; and increasing operational efficiency by simplifying the integration of Exchange Server data with third-party solutions through the new Exchange Web Services feature.

Nortel

Nortel, like Cisco, offers a diverse range of networking and unified communication products: contact center suites, communications servers, Ethernet switches, switched firewalls, threat protection systems, VPN solutions, PBX solutions, optical network solutions, unified messaging technology, wireless network products, wireless mesh systems and WLAN products.

Nortel's Contact Center products enable government agencies to engage their public more fully and efficiently, allowing agents and supervisors to be located anywhere a secure IP connection can be enabled. Call Center Management Information System allows managers to view agent and queue statistics in real time, and assists in generating a variety of reports.

Another product, Contact Center Express, delivers skills-based call routing, allowing callers to be guided to the most appropriate staff member for their query.

Nortel makes several VPN solutions: an enterprise IPsec product, which offers end-to-end encrypted tunneling and remote access capabilities; Services Edge Router 5500 and Passport 7000, 15000 and 20000 Multiservice Switches, which provide VPN service to thousands of staffers simultaneously; Optical Ethernet solutions, which enable agencies to provide Layer 2 VPN service; and clientless SSL VPN solutions that allow agencies to offer secure remote access via SSL technology.

As government agencies face budget shortfalls, it's important to focus on lowering the total cost of delivering computer services. This can be facilitated by restructuring some key approaches to IT services:

- Designate one person responsible for data center design, construction and operations, and have all relevant departments report to that person.
- Create a simple, transparent model of total data center costs, so that people within the agency know what the most important metric is for success.
- Specify energy-efficient IT equipment compliant with the SPECpower consumption standard (www.spec.org/power_ssj2008) or the forthcoming Energy Star metric for servers, and be willing to spend a little more for IT equipment that reduces total cost in the data center.
- Settle on lower-level metrics (such as server utilization and the site infrastructure energy overhead multiplier, also known as Power Utilization Effectiveness) and start measuring everything of importance.

IBM

IBM has a presence in many areas, including networking. The manufacturer offers a variety of servers including blade servers, cluster servers, mainframes, Linux servers and UNIX servers. IBM also has several operating systems and storage systems to complement its networking offerings.

The software products offered by IBM run the gamut, from Application Workload Modeler, which serves as a performance and capacity planning tool for networks and network-based servers, to Maximo for Government, which helps agencies address regulatory requirements related to their contracting and personal property management.

IBM's BladeCenter blade servers line claims to use 50 percent less floor space and 35 percent less energy than other blade servers. This line supports a wide selection of processor technologies and operating systems including Intel and AMD processors, POWER processors, Cell/BE processors and Deep Packet Inspection.

The BladeCenter products reduce network complexity, improve systems management, increase energy efficiency and lower the total cost of ownership.

Avaya

Avaya is a top manufacturer in the unified communications world. Its product offerings include integrated web conferencing solutions, mobile solutions, voice messaging solutions, unified messaging platforms, video conferencing technology, UC suites and desktop telephony solutions.

One of Avaya's more popular products is the Unified Communications Standard Edition, a bundled suite of communications applications that cover telephony, messaging, conferencing and mobility needs to assist agencies in delivering the right applications to staff members' devices at the right time.

This product can integrate well with IBM Lotus and Microsoft's Office Communicator, allowing for both centralized and desktop deployment.

It also allows users to extend these telephony functions to their user devices. This means that staff members can set up a simultaneous ring for both their desks and mobile devices, shift calls in progress between devices, and access PBX and UC features while on the road via their mobile device. With a VPN client on their desk phone, teleworkers can get secure access to their office phone and its features.

Other features available include user access to telephony, voice messaging, audio conferencing and agency directory information — all in a single web-based client.

The following questions prove valuable when thinking through an agency's security strategy:

- Does an operational reason exist for allowing Skype and/or IM clients? If not, a security policy could prohibit their use. Firewalls and proxy-server technology at the network edge could stop such traffic.
- Do we provide network services to guests and contractors? NAC can allow a customization of available network services based on the identity of the user and the security posture of the connecting PC, thereby protecting your production network while still opening the door to foreign PCs.
- How do we protect the traveling notebook? In order to allow users to safely connect to foreign networks, the end-points must have protections in place such as: host-based intrusion prevention, personal firewall, antivirus and patches.
- How do we safeguard sensitive data? Classify your data into tiers, then locate it. If the data is centralized, then firewalls, intrusion prevention, strong access control and auditing serve as relevant tools. If sensitive data is widely distributed, either work to centralize it or look at data loss prevention (DLP) technologies.
- How do we ensure that highly sensitive data doesn't leave the organization? Different DLP technologies can prevent sensitive information from exiting the organization via e-mail, web, FTP and portable media. Some of these products work at the end-point by constraining user behavior. Others work at network egress. Multiple layers of protection are preferable.
- How do we manage insecure user behavior? The best security protections cannot defend against a user who inappropriately shares valid login information. Two principle approaches exist for counteracting this weakness. Teaching users about secure computing practices, including password protection, is an ongoing best practices campaign.

Two-factor authentication, by contrast, combines a known password with a physical key such as an RSA token. This one-time password resists replay and provides very strong protection against the threat of weak or shared passwords.