CDW PEOPLE WHO GET IT

VIRTUAL PRIVATE NETWORKS, VERY PROTECTED NOW

With demand for mobile access increasing, VPNs are ideal for securely accessing network resources remotely.

Executive Summary

The explosive growth of mobile computing technology is changing the security landscape dramatically for organizations of all shapes and sizes. It's rare to find someone today who doesn't have some type of computing device ever-present while on the job.

Most information workers (people who typically work with concepts, documents and other people) have computers provided by their employer, as well as a personal computer or tablet at home and a smartphone that is either personally owned or issued by the enterprise. With such a wide range of computing devices at their disposal, users now expect access to work resources regardless of their location or device.

Such ubiquitous access comes with security risks. For example, a teacher grading assignments on a notebook computer at a coffee shop may unwittingly expose students' grades to other users over an unsecured wireless network.

TWEET THIS!

Table of Contents

Similarly, an administrator logging in to a financial system from home to check monthly budget results may inadvertently grant an eavesdropper access to the system used to authorize purchase orders. Still, most organizations recognize that these new work patterns are here to stay and — rather than locking users out with heavy-handed security measures — they must find methods to help users easily access information while keeping it secure.

Virtual private networks (VPNs), which use encryption technology to securely extend enterprise network access to users at remote locations, can provide that level of safety. VPNs protect users from eavesdroppers on local networks (or the Internet) while providing access to important information resources. And they are an essential tool among an array of enterprise security strategies.

Knowing how and when to deploy a VPN will go a long way toward strengthening any organization's security efforts. This white paper explores VPNs in detail, including how VPN technology works, the roles they can play in enterprise networks and some best practices to stave off common VPN pitfalls.

An Answer to Today's Security Risks

Information technology has evolved dramatically over the past 10 years. A decade ago, most users had a single computing device, a home computer. Most people accessed the Internet via a low-speed, dial-up modem.

Today, many users have more than one computing device, along with many different mobile devices. And high-speed broadband Internet access is the norm, both at home and on the go. Users now expect to have work and personal information at their fingertips, whenever and wherever they need it.

Amid these technological changes, three broad trends are having a lasting effect on IT operations:

Rapid hardware and software advances: Device capabilities have ramped up significantly over the past decade. Inexpensive handheld devices now have the computing power of the sophisticated mainframe systems of years ago. Individuals routinely carry more computing power in their pockets than was needed to power the last flight of the space shuttle.

Consumerization of IT: As technology becomes more powerful, it also becomes more accessible. In the past, many individuals did not have access to a computer outside of their workplace. Of those that did, most did not possess the technical skills required to connect a home computer to an enterprise network without direct IT support.

Today, point-and-click interfaces make connecting to the workplace a breeze. Users simply provide a VPN address, username and password, and they're connected to a workplace computing environment.

Bring-your-own-device (BYOD) policies: While users have done office work on personal computers for years, some organizations are now adopting BYOD policies that actively encourage the practice. In some cases, staff who want to use mobile devices must bring their own devices to work (see the *Implementing BYOD Policies* sidebar).

As these trends converge, security professionals must rethink the strategic paradigms they've relied on in the past. At one time it sufficed to focus efforts on building a strong network perimeter to serve as a wall to protect the information within. Today it's just as likely that a valid user is now outside of that wall, seeking access to information housed inside.

Security now requires a multilayered approach, with different controls serving different purposes. Depending on the form factor, computing devices need some combination of

Implementing BYOD Policies

As employees make greater use of personally owned computers for work, organizations must decide how to address this situation. A formal BYOD policy is needed that governs how and when workers may use their devices. These policies typically fall into three categories:

Permissive: A permissive approach allows employees to use personal devices for at least a limited range of activities. The organization may decide to allow full access or may restrict devices to certain types of activity, such as web-based email access.

Dismissive: Dismissive BYOD policies severely limit both the use of personal devices on enterprise networks and access to data. While some organizations embrace this approach, workers seeking the convenience that BYOD offers almost universally reject it.

Mandatory: A small but growing number of organizations require staff to bring their own devices. One major corporation recently announced that it will no longer provide smartphones to its staff, nor will it manage their accounts. In such instances, employees are required to obtain their own device and connect it to the organization's mobile device management platform.

Enterprises that implement BYOD policies must carefully consider the elements that will be included. For instance, workers may be required to sign a statement granting IT administrators permission to wipe data from their devices if they are lost or stolen. BYOD programs are frequently limited to devices that have an operating system supported by the organization and meet minimum security requirements, such as running current antivirus software.

password protection, full-disk encryption, remote wiping capability and managed antivirus software. Networks must be protected with firewalls and intrusion detection/prevention systems. Data that passes between devices and networks should be encrypted through the use of a VPN and application-layer encryption technology.

VPNs are an essential component of a multilayered approach to information security. In addition to providing remote users with a secure gateway to the enterprise network, VPNs also can be used to establish encrypted connections between sites, replacing expensive, dedicated site-to-site communication links.

How It Works

Remote users often connect to public networks, such as those available in a hotel, coffee shop or airport, to gain access to enterprise resources. But neither the user nor the organization's IT staff have insight into the public network's security configuration. While an organization cannot extend a physical private network to those locations, encryption technology can simulate one using a VPN.

Encryption uses mathematical algorithms, known as ciphers, to render data unreadable to anyone who doesn't have access to the corresponding decryption key. VPNs use hardware and/or software to encrypt the data leaving a computer and send it to a remote location where it is decrypted and placed on another network.

The beauty of this approach is that anyone eavesdropping on the connection sees only the encrypted traffic, which will appear to be gibberish. The data is accessible only from the original computer or on the organization's network. In this way, the encryption technology of the VPN transforms a public network into a private network.

Mobile devices pose a unique challenge to VPN administrators. Standard VPN technologies depend on building a dedicated connection between two fixed IP addresses. But wireless devices such as smartphones, tablets or notebooks usually have rapidly changing IP addresses as they roam from network to network, making this straightforward approach impossible. Mobile VPNs adapt to the changing IP address of endpoints and ensure the connection remains stable in spite of those changes.

VPN Types

There are two types of VPNs in use today:

Remote connectivity VPNs: These are the most common. Remote workers use them to connect back to the enterprise network and gain privileged access to enterprise resources. The encryption also offers remote users security even when they are connected to an insecure public network.

Site-to-site VPNs: These are similar to remote connectivity VPNs, but instead of connecting a single user to a remote network, they connect two remote networks together. Site-to-site VPNs are commonly used to connect remote offices to a headquarters location.

For example, a school district might use a site-to-site VPN to connect the administrative office's network to those of all of the district's schools. From the end user's perspective, the networks appear to be physically joined.

When traffic must pass between them, VPN devices on the two networks automatically handle the encryption and decryption so that the traffic may be sent over the Internet. Site-to-site VPNs have brought major cost savings to many organizations that previously relied on expensive, dedicated network connections between sites.

VPN Protocols

There are a wide variety of VPN protocols. While they offer similar security benefits, it is important that both the client and server support a common protocol in order for them to communicate properly. These protocols could be considered the "language" being used by the VPN.

IPsec: This is actually a suite of protocols that perform three primary functions to make up IPsec. The first, Security Associations (SA), establishes the parameters of an IPsec connection by performing initial authentication and key exchange. Key exchange may be done manually in advance or via an automated protocol, such as the Internet Key Exchange (IKE, or the updated IKEv2).

The second protocol, Authentication Headers (AH), provides authentication and message integrity to ensure that data is actually coming from the purported sender and has not been modified in transit. And the third, Encapsulating Security Payload (ESP), offers encrypted data transport, providing confidentiality for data sent over an IPsec VPN connection.

Secure Sockets Layer (SSL) and Transport Layer Security (TLS): These protocols provide encryption for HTTP Secure (HTTPS) web servers. They also may be used to establish VPN connections with remote systems through standard web browsers. The advantage of this type of connection is that the end user does not need to install any specialized software in advance, but instead can visit the VPN website in a browser to establish a connection.

Datagram Transport Layer Security: DTLS is a protocol used by Cisco's AnyConnect VPN product. It is based upon SSL/TLS VPN technology but adds features that support the tunneling of connectionless traffic, such as that used by the User Datagram Protocol (UDP).

Microsoft's Point-to-Point Encryption: MPPE protocol encrypts traffic sent over the Point-to-Point Tunneling

Protocol (PPTP) to create VPN connections. MPPE is quite popular because it is supported by a wide variety of operating systems without having to install specialized software.

Secure Shell: SSH is well known as a tool for gaining secure command line access to Linux systems. While not as common, it is also possible to create a VPN by tunneling traffic over SSH.

Finally, there is a subclass of VPNs known as Trusted Delivery Networks. With TDNs, the VPN does not actually provide encryption. Instead, all sent data is routed through a single, trusted Internet service provider.

The ISP then uses routing and switching techniques, such as Multiprotocol Label Switching (MPLS) or the Layer 2 Tunneling Protocol (L2TP) to ensure traffic is viewed only by the intended sender or recipient. This technology works only with site-to-site VPNs when the same ISP connects all of the sites together, making it somewhat expensive.

Multifactor Authentication

While many VPNs rely on standard user ID and password authentication techniques to verify identity, this may be insufficient in certain circumstances and organizations may require more sophisticated proof of identity.

There are three ways in which users can prove their identity when attempting to authenticate to a system. They may provide:

- **Something they know:** This is the most common form of authentication, because it is the least expensive and simplest to configure. A user simply tells the service a secret that is known only to the two parties, such as a password.
- **Something they have:** The user provides proof that he or she has possession of an object that nobody else has. Typically, this is a numeric code displayed on a physical token retained by the user. This factor also is sometimes implemented through the use of digital certificates stored on devices.
- **Something they are:** The user uses a biometric technique to measure a unique physical characteristic. Biometric authentication techniques include fingerprint scans, retinal scans and voiceprint analysis.

The most secure scenarios call for multifactor authentication, in which a user must authenticate using two mechanisms from different categories. For example, a user might provide a password (something they know) as well as a code from a security token (something they have). Multifactor authentication is especially common in high-security VPNs that provide access to sensitive information.

One of the major benefits provided by multifactor authentication in a VPN setting is that it prevents someone who finds a lost or stolen device from directly connecting to the issuing organization's network without having the second authentication factor. The same approach can be used for standard network connections through the use of 802.1X technology.

Where VPNs Fit In

Some security professionals view VPNs as the Swiss Army knife of the information security toolkit because of the diverse roles they may play in a security program. There are four scenarios in which an organization might deploy a VPN:

Scenario 1: Protect traffic from eavesdropping and manipulation.

Employees often use mobile devices to access the Internet from public locations that deploy unencrypted wireless networks. Eavesdroppers on those networks can run freely available software to monitor users' activities, such as reading email or browsing the web, and access sensitive information.

In some cases, eavesdroppers may even be able to steal authenticated sessions, gaining access to a user's accounts. The recent release of Firesheep (an extension for the Firefox web browser that intercepted unencrypted cookies from sites such as Facebook or Twitter) illustrates this threat well. Wireless eavesdroppers enjoyed one-click access to users' social networking accounts when accessed via the same wireless network.

VPNs remedy this issue by providing the encryption an open wireless network lacks. IT administrators can deploy a remote access VPN and configure devices with a remote access profile.

When a mobile user accesses an unknown wireless network location, he or she first connects to the VPN, and then accesses Internet and intranet resources through the VPN's secure encrypted tunnel. All of the user's traffic is routed through the enterprise network, leaving eavesdroppers unable to penetrate the encrypted tunnel and view or manipulate network traffic.

Users must be cautioned, however, that if the VPN is being used to relay otherwise unencrypted traffic, that traffic will remain unencrypted when it leaves the organization's network. Users concerned about end-to-end security must also employ the use of application-layer encryption, such as that provided by the HTTPS protocol (see *Securing Applications* sidebar for more information).

Scenario 2: Provide consistent device protection, both in-network and out-of-network.

Many enterprises allow staff to take their work computers home, which introduces its own set of risks. Computers in the office are typically connected to a secure, well-controlled network populated with systems managed by the IT group.

Home networks, on the other hand, are notorious for playing host to unpatched, infected computers that may compromise a work computer's security. Work computers that become infected can carry malicious software back into an organization's secured network, posing greater risk to other systems.

Some of those risks can be mitigated by configuring take-home devices to automatically connect to the organization's VPN whenever they are powered on. The VPN client also may include a firewall that automatically blocks connections from other systems on the local network, providing employees with a secure computing environment, whether at home or at the office.

Scenario 3: Differentiate personal devices.

A growing number of organizations now enforce BYOD policies that allow workers to use personal devices to access email, calendars and other nonsensitive resources. The policies may also prohibit the use of BYOD systems in accessing sensitive data.

VPNs may be used to enforce such policies by limiting the types of access permitted to devices not issued by an organization. For example, the Cisco AnyConnect VPN client uses Extensible Authentication Protocol (EAP) chaining capability to provide an added layer of protection.

EAP chaining allows the VPN to authenticate both the user and the system, providing different levels of access based not only on an individual's identity but also on whether an enterprise-issued computer or personal device is used. A user connecting from an enterprise-issued computer might be granted access to sensitive information, while the same user connecting from a personal device might be denied that access.

Scenario 4: Protect specialized networks.

Organizations also commonly use VPNs to provide protection for highly secure, specialized networks, which might facilitate access to private information or systems that handle an organization's sensitive functions. Individuals who are authorized to access the sensitive network may use a system located anywhere on the enterprise network to establish a VPN connection to it.

One common example of this scenario is a specialized system administration VPN that allows access to servers housed in an organization's data center. The sensitivity of those servers may require prohibiting their direct access from the enterprise network.

But it would be inconvenient if administrators had to visit the data center to physically connect to the protected network to perform server maintenance and configuration tasks. Organizations often compensate for this through the use of a data center VPN that is available only to system administrators but allows connections from any location on an organization's internal network. System administrators using such a network gain the convenience of easy access to servers while shielding those servers from other network users.

Real-world VPN

VPN administrators have a variety of technologies at their disposal and may select the correct mix of services that meets their organization's security requirements. Two questions facing administrators with regard to configuration are whether to use split tunneling and what, if any, type of multifactor authentication should be required for VPN access.

Split Tunneling: Yay or Nay?

VPNs typically offer two tunneling options: full tunneling and split tunneling. With full tunneling, all network traffic leaving the host computer is sent in encrypted form over a VPN connection. Split tunneling sends only the traffic destined for the network protected by the VPN through the VPN tunnel. Traffic intended for systems on other networks is sent out through a computer's Internet connection without the protection of a VPN.

Why would a split tunneling approach be preferable? Here are a few reasons:

Privacy: Users may not want all of their network traffic sent through an organizational network, especially when they are connecting from a home computer to a work network using a VPN. Those users may want their work traffic to travel through the VPN, but personal network activity to go out directly through their Internet connection.

Efficiency: Enterprises might want to limit the amount of data sent through their VPNs to provide additional capacity

Securing Applications

IT professionals have another weapon in the security toolkit to protect sensitive information in transit over unsecured networks: encryption at the application layer. While VPNs encrypt all traffic headed to an organization's network, individual applications can also implement encryption to ensure all use of the application is protected. The most common example is the use of Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) protocols to encrypt sensitive web traffic using the HTTPS protocol.

In some cases, organizations that want to protect only a single application may find application encryption a good alternative to a VPN. The major benefit is that it's quite simple for the user to configure. He or she simply connects to a website's HTTPS address, then authenticates using a user ID and password, or whatever authentication factors the organization requires.

Keep in mind that application encryption isn't a panacea. It's great for situations in which nonemployees need to access data on an organization's web server or when employee access can be limited to specific web applications. When more complex access is needed, VPNs definitely are the way to go.

for more users. If a home computer user's streaming video request travels through the VPN tunnel, it is consuming organizational resources.

Multiple network access: Some users might need to connect to multiple networks at the same time. Using a full tunneling VPN may prevent that access from working properly.

Speed: Users may experience latency if their traffic is first routed through an enterprise network before reaching the Internet. They also will be subject to the potential bottleneck of limited bandwidth availability on an organization's network.

There also are downsides to split tunneling. Users who are unaware that it is taking place may rely on the VPN to secure traffic that actually is traveling directly onto the Internet in unencrypted form. When split tunneling is used, it is especially important that users are trained and understand exactly what traffic is — or is not — secured by the VPN.

Multifactor Authentication and VPNs

Multifactor authentication allows administrators to provide a higher level of both identity-based and context-based security. Administrators may feel confident that users actually are who they claim to be (identity-based security) and are accessing the network from an approved device (context-based security).

Two-factor authentication provides peace of mind that someone who finds a lost or stolen device will not be able to use it to gain access to the enterprise network. Nor will a user's password — perhaps compromised through a successful phishing attack — be sufficient to grant such access without an additional authentication factor.

Digital certificates are one example of the use of multifactor authentication to provide context-based security. A digital certificate may be placed on an authorized device and transmitted to the VPN server as proof of possession of the device.

This serves as a "something you have" authentication factor. Then the user may be prompted to log in with a password — a "something you know" factor. Neither the device alone nor the password alone is sufficient to gain access to the VPN.

Similarly, organizations may use biometric technology to provide a "something you are" factor for authentication purposes. The most common use of biometrics for remote access is to secure access to a mobile computing device through the use of a fingerprint reader. Successful fingerprint authentication grants access to the device, which contains a digital certificate used as a "something you have" authentication factor.

Multifactor authentication also may be used to regulate access to wired and wireless enterprise networks through the use of 802.1X technology, which provides a flexible framework for authenticating users to networks with any authentication factors that support EAP.

Networks using EAP and 802.1X operate authentication servers that process requests from supplicant software running on the user's device. After a successful authentication attempt from a device's supplicant, the authentication server instructs 802.1X-enabled network devices to grant the device access to the network.

For example, an 802.1X network might require that users attempting to gain access authenticate via a combination of the code from a one-time password token (something you have) and a personal identification number, or PIN, (something you know).

Email and VPNs

Many organizations choose split tunneling to exempt email traffic from VPN requirements that apply to other systems on their networks because email is one of the most significant traffic loads on remote access VPNs. Excluding it greatly increases the VPN capacity available to other users.

Why wouldn't an organization want to secure email access? The answer is that it is very easy to apply application-level encryption to email connections.

All of the major email protocols, including Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP) and Remote Procedure Call (RPC), support the use of SSL and TLS encryption technology. Administrators can simply configure mail servers to require encrypted connections, exclude email from the VPN tunnel, and be assured that the user's email traffic is secure whether connected to the VPN or not.

Addressing VPN Concerns

While VPNs offer a wide range of security benefits to enterprises, there are some drawbacks — both real and perceived — to using the technology. It's important that IT administrators are aware of those concerns and address them proactively.

The main concerns around the use of VPNs are related to performance. Many users have experienced VPNs that operate so slowly that the effect on network performance is noticeable. While it is true the encryption and decryption operations performed by a VPN take time, they should not degrade network performance.

Having sufficient VPN capacity to perform the encryption and decryption operations quickly is essential for a good user experience. This is where hardware-based VPNs shine: VPN concentrators and other devices dedicated to implementing cryptographic technology contain specialized processors that implement the decryption algorithm in dedicated hardware designed for that sole purpose.

These chips greatly improve the performance of VPN operations. The bottom line is that if users complain about VPN performance, the VPN device should be checked to ensure

that adequate memory and processor cycles are available. Administrators may simply be asking too much of a device.

The use of VPNs also may cause bandwidth-related performance problems. If users routinely connect to a VPN for all remote-computing needs, traffic must pass through the organization's network twice, first entering the network through the encrypted VPN tunnel, then decrypted and passed out to the intended destination.

When the destination system replies, the traffic similarly passes back through the organization's network, where it is encrypted and sent back through the VPN tunnel. Organizations deploying a remote access VPN, especially one that does not employ split tunneling, should plan carefully for such increased bandwidth requirements.

Another complaint raised by users is that they're uncomfortable with their personal communications being exposed to the organization's IT staff. While the obvious answer is to instruct users to only connect to the VPN for work-related traffic, that simply is not practical advice.

Today's mobile workers, especially those using personal devices, are accustomed to multitasking and often have work and personal email accounts open at the same time. Organizations should consider the use of split tunneling to address such privacy concerns.

The final issue comes from security administrators themselves: VPN technology can interfere with other security technologies, including data loss prevention (DLP) products.

By their nature, VPNs encrypt traffic so that it cannot be seen by anyone other than the devices participating in the communication. An improperly placed DLP device may not be able to see VPN traffic in unencrypted form.

The answer, at least for users located outside an enterprise network, is to design network topology so that the DLP device is positioned in line after the VPN device, giving it access to traffic after it is decrypted. Outbound VPN traffic is a different story. (For more on that topic, see the *Outbound VPN Access* sidebar.)

In almost every case, it should be clear that a VPN's security and privacy benefits outweigh the potential drawbacks. As long as organizations are willing to invest in the VPN hardware necessary to maintain high performance, they should be able to run a service that adequately addresses any issues.

Outlines for a Strategy

Once the IT team decides to move forward with a VPN rollout, it should take time to develop a clear strategy for use. That strategy should guide the technology selection process to ensure that products are chosen that meet or exceed functional requirements. Here are some tips for developing a solid VPN strategy:

Develop simple and clear use cases: Take the time to write out the goals of a VPN strategy in language everyone can understand. Is the goal to provide secure access for remote workers? Should administrators have access to financial systems from home? Is the goal a site-to-site VPN to connect networks at various locations within an enterprise? Write these things down so that the program may begin with its goals in mind.

Clarify BYOD policies: Is the organization planning to adopt a permissive, dismissive or mandatory approach to BYOD? If users will be permitted to use personal devices, what are the security requirements? What level of control will be exerted over those devices? Will they have the same level of access as devices issued by the organization?

Develop an access policy: What resources will be accessible via the VPN? Will a VPN connection provide full access to the network, or will it be limited to a subset of features? Does this policy differ for personal devices? The policy should clearly outline requirements for both identity and context-based security.

Outbound VPN Access

The ideas presented in this white paper have shared mainly the perspectives of IT professionals designing VPNs for use by their organization's staff members. While it's true that this is the primary concern of an internal IT team, another perspective should be considered as well.

Will outbound VPN access be allowed from the network? Can staff members connect to another organization's VPN? What if visiting vendors or contractors need to use the VPN to connect back to their "home" network?

Whether to allow outbound VPN access is a serious decision because the use of this technology can render many security mechanisms blind, and allow users to bypass the security controls put in place. A few examples:

- Outbound traffic from VPN clients installed on computers located on the network is unreadable by DLP systems, and could allow a malicious insider to use a VPN connection to remove sensitive information from the organization in an undetectable fashion.
- Users connecting to a VPN will be able to bypass all of the other outbound network controls imposed by an organization's firewall. Because all of the traffic is sent through a third-party network, the firewall simply sees it as a single (allowable) VPN connection.
- Similarly, content filtering mechanisms are unable to monitor or filter web traffic routed through a VPN, which could expose an enterprise to liability if users visit unauthorized websites, such as gambling or pornographic sites.

Always consult with legal counsel and carefully weigh the functional requirements before deciding to allow outbound VPN access from an internal network.

Create a chart: When designing a VPN strategy, it's often helpful to develop a chart that highlights the structure of the enterprise network as well as the locations where VPN traffic will exit encrypted tunnels. The chart can be referenced later to ensure that the traffic to be protected will actually be encrypted when necessary.

Be mobile friendly: It is likely that many users will access the VPN from mobile devices. Be sure that the chosen VPN technology is mobile friendly and that the selected authentication techniques actually are possible on mobile devices.

For example, a retinal scan probably is not going to work very well from a smartphone. Similarly, a password policy that requires extremely long and complex passwords is likely to frustrate users typing it on a mobile device's tiny pop-up keyboard.

Consider a technology that offers convenient mobile access, such as Cisco's AnyConnect product line. The VPN should also be tested with any mobile apps used by the organization to ensure proper functioning.

Choose a technology that meets the enterprise's requirements: Do not start looking at specific products until the policies and requirements for VPN access are developed. That set of requirements can then be used as the "shopping list" to ensure selection of products that are compatible with the existing networking and identity management infrastructure and that meet all functional requirements.

Log VPN activity: Once the VPN is up and running, be sure to log VPN use and monitor those logs for signs of suspicious activity. Watch for red flags, such as simultaneous VPN connections from the same user account, access from suspicious countries or the use of the VPN while a user is onsite. Any of those may indicate that a VPN account has been compromised and an unauthorized user is on the network.

VPNs provide a flexible, useful tool for ensuring the confidentiality and integrity of information assets in the hands of an increasingly mobile workforce. The wide variety of VPN technologies and product lines available today provide a solution that will fit the requirements and budget of any organization.

Symantec™ Mobile Security offers comprehensive protection for Android™- and Windows®-based mobile devices against malicious threats while ensuring compliance with regulatory requirements. Mobile Security provides antivirus technology, advanced firewall and SMS antispam features to ensure mobile assets and maintenance of compliance policies.

CDW.com/symantec

With the growing popularity of high-end mobile devices, many employees are opting to use their consumer-grade personal devices — such as PCs, tablets and smartphones — in the workplace. Trend Micro™ suggests you embrace consumerization and securely manage your workforce without limits. Mobile Security is a fully integrated mobile device management and security solution within a security framework that spans physical and virtual, PC and non-PC devices. It protects data by enforcing the use of passwords, encrypting data and remotely wiping data from lost or stolen devices.

CDW.com/trendmicro

The MobileIron mobile IT platform secures and manages apps, docs and devices for global organizations. It supports both corporate-liable and individual-liable devices, offering true multi-OS management across the leading mobile OS platforms. MobileIron is available as both an on-premises system through the MobileIron VSP and a cloud service through the MobileIron Connected Cloud.

CDW.com

TWEET THIS!

CDW® PEOPLE WHO GET IT™