

Inside this issue:

Top Ten Reasons to Upgrade to Exchange Server 2007 **2**

Top Five Mobile Security Threats **3**

WatchGuard Ups the Ante for Network Security **4**

Mobile Security—Preventing Data Leaks **5**

APC—Start with the right rack and you can't go wrong.**"Fits Like a Glove" NetShelter® SX Guaranteed Compatibility**

Whether you are designing a wiring closet or the largest data center, or just looking for the most flexible rack solution, APC NetShelter® SX rack enclosures provide a secure and vendor-neutral environment for your IT equipment.

APC is committed to ensuring that your rack-mount equipment will fit into NetShelter SX enclosures. APC guarantees that all 19" EIA-310-D compliant equipment will physically fit into NetShelter SX enclosures with the mounting hardware provided by the original equipment manufacturer (OEM), APC, a third party vendor, or any combination thereof or your money back.

NetShelter® SX is APC's next generation rack enclosure solution influenced by 10 years of customer feedback addressing current IT market trends for high-density server and networking applications. With a strong focus on cooling, power distribution, cable management and environmental monitoring, the NetShelter SX provides a reliable rackmounting environment for mission-critical equipment.

Download Free Rack White Papers

For full details, visit www.apc.com/promo Key Code: a481w

NetWorks, Inc. has experience installing APC racks and recommends many other APC products. Contact our service team for a consultation. They know the questions to ask to save you time and money and possibly uncover issues you would not have thought about.

WELCOME**Patrick Fagen**

On January 28 we welcomed a new engineer to our staff. Patrick has done intern work for NetWorks, Inc. during the past two years and recently graduated from the University of Iowa.



NetShelter is completely compatible with all APC award-winning InfraStruXure architecture, allowing you to add rack, power and cooling on a scalable as-needed basis.

Top Ten Reasons to Upgrade to Exchange Server 2007

Microsoft Exchange Server 2007 is designed to deliver increased protection for your business and give anywhere access for your employees, while being operationally efficient to deploy, manage and maintain. Should you upgrade? Here are ten reasons for you to consider.

1. Keep your e-mail system running at lower cost

New data replication capabilities in Exchange Server 2007 drive increased availability at a lower cost. Local Continuous Replication delivers database redundancy with rapid recovery, minimizing the frequency of full tape backups. With Cluster Continuous Replication in combination with Microsoft Cluster Service (MSCS), active/passive clusters provide both database and service redundancy without requiring expensive shared storage, even when clusters span geographic locations.

2. Access e-mail, voice mail, calendar, and contacts from virtually anywhere, anytime

In Exchange Server 2007, your employees can access their important inbox information from virtually anywhere using their desktop computer, laptop computer, a browser window from any Internet-connected computer, their mobile device, and even using a basic telephone when no Internet connectivity is available. Employees enjoy a rich and familiar experience based on Microsoft Office Outlook 2007 functionality. Best of all, it's all built in with centralized management and robust security, making rich anywhere access possible for your entire workforce instead of just a limited few.

3. Get affordable, enterprise-class mobile messaging that's better than ever

Exchange makes enterprise-class mobile messaging a reality by offering industry-leading scalability, native integration with compatible devices for lower total cost of ownership, and by providing a variety of device options to suit today's business needs. Building on the advances in Exchange Server 2003 Service Pack 2, mobility features in Exchange Server 2007 raise the bar on user experience and deliver improved manageability. Now desktop features such as support for rich HTML, quick flags, sophisticated calendaring, and fast search are available on mobile devices. In addition, Exchange Server 2007 provides more granular security policies and enables users to perform basic tasks on their own (such as perform a remote wipe from Outlook Web Access 2007).

4. Empower employees with unified messaging while saving money

With new unified messaging in Exchange Server 2007, employees can receive their e-mail, voice mail, and faxes through a single inbox that can be accessed from anywhere. Employees can manage all of their messages in one place just as they manage e-mail today. For example, voice mail can be forwarded, or if the recipient adds text notes to the voice mail, messages can be found using built-in search. With Exchange Server 2007, you can deliver these features while lowering cost and complexity through consolidation of your voice mail infrastructure.

5. Get comprehensive protection from spam, viruses and phishing attacks

Exchange Server 2007 provides integrated antivirus, anti-spam and anti-phishing technologies to stop the latest threats before they impact your business and employees. Multi-pronged message filtering in the perimeter network is available through the Edge Transport server role. For customers who prefer to use a service, similar capabilities are provided in the "cloud" (as an Internet-based service) through [Exchange Hosted Filtering](#)*. Additionally, [Forefront for Exchange Server](#)* protects Exchange servers from viruses and worms by utilizing multiple antivirus engines simultaneously. To protect from evolving threats, filters are kept up to date with frequent and automatic updates.

**Exchange Hosted Filtering and Forefront Security for Exchange Server are included with the Exchange Server 2007 Enterprise CAL license.*

6. Reduce compliance risk in a way that makes sense for your business

Exchange Server 2007 incorporates features specifically designed to help your business comply with corporate, regulatory, and legal requirements. These features enable you to apply retention rules, scan and act on messages in transport, flexibly journal, and perform rich text searches across mailboxes in your organization. Exchange Server 2007 eases the toll often placed on administrators charged with applying and enforcing compliance policies, while avoiding adverse impact on employees and their productivity.

7. Take advantage of powerful Web access

Outlook Web Access (OWA) 2007 provides a rich, Outlook 2007-like experience in a browser and is great for use at home, at an airport kiosk, at an internet café, at a friend's house, or anywhere where there is an Internet connection available. No VPN or network tunnel is required. OWA enhancements in 2007 include a new Scheduling Assistant to help employees efficiently book meetings, fast server-side search, integrated unified messaging as well as new features to access documents and attachments more easily from outside the office. With two-factor authentication support and attachment viewing in HTML format, OWA also offers enhanced security compared with previous versions.

Top Ten Reasons to Upgrade to Exchange Server 2007

Continued from page 2

8. Boost administrator productivity with new tools

Exchange Server 2007 helps administrators save time and reduce effort with advanced management tools. A new command line interface gives administrators complete, fine-grained control over Exchange objects as well as the power to easily automate all types of operations with scripts. In addition, the graphical management console has been completely updated, with a more intuitive user interface, improved discoverability and a toolbox work center that integrates diagnostics, monitoring, and troubleshooting tools including the Exchange Best Practices Analyzer and the Exchange Troubleshooting Assistant.

9. Ease deployment and management

Deploying Exchange Server has never been easier. Exchange Server 2007 has a modern, modular architecture based on server roles. The server role concept is integrated into setup and deployment, helping to eliminate potential errors resulting from manual configuration, reducing the surface area for malicious attacks, and simplifying day-to-day management. Server roles are not tied to particular hardware configurations; they can be deployed on one server machine or many**. The new Autodiscover feature further eases deployment - by creating an automatic connection between Exchange Server and Outlook 2007 clients where no special scripts or complex user intervention is required.

**The exception is the Edge Transport role that is intentionally designed to reside by itself in the perimeter network.

10. Optimize your investment for future growth

As a native 64-bit application, Exchange Server 2007 breaks through past memory and cache limitations for higher performance and increased scalability even as mailboxes sizes grow to accommodate employees' demands for more storage. The resulting reduction in input/output (I/O) increases storage utilization so you can optimize existing storage investments or consider lower cost storage options.

To learn more, visit www.microsoft.com/exchange.

Top Five Mobile Security Threats

While most employees know to steer clear of files associated with Britney or Paris, there are plenty of other parasites out there waiting to prey on a company's unsuspecting employees. Here's a look at the top five concerns currently plaguing the wireless world.

1. **Device Theft**—Many people seem to have a cell phone glued to their heads, but others often drop or leave behind their trusted pocket pal. "Mobile devices are easily left behind on a table, and a quick thief can grab and dash with your phone," says Derek Kerton, head of the wireless practice at The Kerton Group. Kerton also notes that the culprit isn't always the common thief; spies and other corporate competitors often have someone to do the dirty work as well.
2. **User Error**—Companies should know what their employees are doing with devices that are supposed to be used specifically for work. Lax Madapaty, product manager for Microsoft's Mobile Communications Business, says companies can enable and disable inapplicable applications, such as camera features on a mobile phone, as well as limit access to unsecured wireless networks. "Companies usually focus their attention on technology, but users are often the weakest link," says Khalid Kark, principal analyst at Forrester Research Inc.
3. **Phishing**—Text messaging may be a convenient way to keep in touch with the office, but it's also very easy for attacks known as phishing. In the mobile world, this is also known as SMiShing—when a user is tricked into downloading viruses or other malware via text messages. John Pescatore, a vice president and distinguished analyst at Gartner Inc., says that this technology takes advantage of people's level of trust of short messaging services, "which is way higher than it should be."
4. **Repairs**—Keys fail, screens flicker, and wear and tear may leave your mobile device in need of a tune-up. Just make sure you get back whatever you send in; users often send units for repair, only to receive a reconditioned unit in return. "The original smartphone or PDA may be repaired or, more likely, it ends up being sold on eBay—with all the customer data on it," says Pescatore.
5. **Common Platforms**—So many devices use Windows Mobile or the Symbian operating system, so how hard can it be to create an all-encompassing threat? According to Forrester's Kark, "A common platform will make it much easier for [hackers] to write viruses and worms that can propagate across many devices."

(Source: Channelpro, February 2008 issue, "Security Goes Wireless" by Rachel Cericola)

WatchGuard Ups the Ante for Network Security

Seattle, WA - January 28, 2008

Press Release



WatchGuard® Technologies, a global provider of network security solutions, today unveiled its latest version of network security software for its Firebox® X Peak™, Core™ and Edge unified threat management (UTM) appliances, positioning WatchGuard UTM devices as the leading price/performance UTM appliances, as evidenced by a panoply of new security capabilities, connectivity features, increased performance and robust network administrative tools.

For businesses that need uncompromising network security, the new WatchGuard Fireware® 10 and Edge 10 releases are highly-reliable, feature-rich UTM operating systems for the WatchGuard Firebox X Peak, Core and Edge families of appliances. Unlike other network security devices, Fireware 10 and Edge 10 are optimized for today's complex network connectivity schemes, and are designed for high-reliability, enhanced UTM functionality, hardened security and greater administrator management and ease of control.

"Businesses today face increasingly new challenges of more mobile workers, remote and branch office environments, and new technologies that stretch the limits of conventional network security appliances," said Eric Aarrestad, Vice President of Marketing at WatchGuard. "Recognizing this, WatchGuard developed version 10 to alleviate connectivity challenges, while improving security and providing administrators with new levels of network security visibility."

To see the complete article, go to <http://www.watchguard.com/press/releases/wg392.asp>

Here's a quick look at the 10 most important changes in "10".

Integrated SSL VPN—Secure remote access via an SSL VPN thin client

Single sign-on—Transparent Firebox Authentication via Active Directory

VoIP and Video conferencing support—One of the most-requested new features

New virus outbreak detection in spamBlocker—Adds another powerful layer of malware protection for the network

Enhanced IPS signature set and engine—Technology behind a Gateway AV/IPS subscription gets faster and stronger

HTTPS in WebBlocker and 54 category support—More specific surfing restrictions increase productivity and protection

SNMPv3 support—Secures device communications with fallback to SNMPv2

New reporting—Faster and more flexible, with a great new look and feel

Integration with LiveSecurity—Smoother initial setup experience

Expanded quarantine for AV—Email caught by AV engine can be quarantined for later administrator review

Mobile Security—Preventing Data Leaks

Regulating the electronic flow of information stored in a digital format has never been so hard. Most organizations have attempted to reduce the risk of data leaks from servers and networks with firewall, intrusion prevention, authentication, and access controls. The mobility trend driving widespread use of laptops for remote and mobile computing has recently spurred the use of encryption solutions for protecting data on devices that may be lost or stolen. But now, a new risk is side-stepping these controls — one that creates the opportunity for data to slip outside the protective net without detection. The culprit is any plug-and-play storage device attached to a stationary PC or laptop USB port.

The USB port enables use of many peripherals, including storage devices. Digital music players can host huge quantities of MP3 files — and hold files in any other format such as word processing, PDF, spreadsheet, database, photo, or multimedia. USB memory sticks do the same thing, albeit without the capability to play back stored multimedia. Digital cameras can store files. So can cell phones, portable hard disks, personal digital assistants, and many other mobile devices.

The danger stems from operating systems that usually recognize and authorize any USB-connected storage device the instant it is plugged into an enterprise endpoint. This Achilles heel effectively makes all endpoints susceptible to data leaks. Danger can also flow in the other direction when newly attached storage devices send virus-infected files or malicious applications onto the endpoint device — and potentially throughout the enterprise network.

When data leaks out, the resulting glare of bad publicity often triggers consumer outrage, regulatory scrutiny, and/or punishment by financial markets. Civil and criminal convictions also may occur for individuals responsible for conditions leading to a leak in organizations subject to laws such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley, and Basel II.

(Source: Check Point Software Technologies, Ltd.)

An entirely new category of threats to your most sensitive information has emerged. Many companies have developed products that address the issue of endpoint protection — Check Point Pointsec Protector, Symantec Mobile Security Suite 5.0, RSA SecurID, just to name a few. Let NetWorks, Inc. help you address these new challenges and find the right strategy to protect your data.



About Us

NetWorks, Inc. is a leading provider of computer networking and hardware procurement services for the Des Moines metropolitan area as well as for other areas of the Midwest. Our experienced staff can help you with any of your company's information processing needs. We specialize in local and wide area networking with extensive experience working with Novell and Microsoft. NetWorks, Inc. was founded in 1994 and has a staff of certified systems engineers that are available 24 hours a day. We value our client relationships and are dedicated to providing complete network solutions.

NetWorks, Inc. works with IT professionals to help support technology solutions that are critical to your organization's success. Our team is good at asking questions. It's the way we learn about the unique challenges your company faces. And because we serve a diverse group of businesses, we have experience enough to know it is rare that two companies require exactly the same solution. Our technical resources, experience, and creativity are unmatched.

Why not put us to work finding a solution for you? Let our experienced team help you solve your IT problems. We are locally owned and operated.

Did You Know?

NetWorks, Inc. can help you track your licensing renewals. We update our files frequently so that we can provide our customers with a 30-60 notice of upcoming license expirations. We appreciate your business and hope that our improvements will make doing business with us easier.

Service Offerings

24x7 Support
Consulting
Documentation
Emergency Services
Hardware/software Procurement
Installation
LAN and WAN
Monitoring Services
Network Design
Planning
Project Management
Security Assessments
Storage Solutions
Troubleshooting
VoIP and IP Telephony

Preferred Partners

Acronis	Insightix
Akonix	Juniper
Apple	LeftHand Networks
Barracuda	Microsoft
Check Point	Nortel
Cisco	Novell
Citrix	PGP
CommVault	Revinetix
Compellent	RSA
Dell	ScriptLogic
EqualLogic	SonicWall
Extreme Networks	Symantec
Fortinet	WatchGuard
HP	...plus more
IBM	

Contact Us

To request more information, please call or email us at: sales@networks-inc.com.

We would like to hear from you! Let us know your thoughts on this newsletter and what you would like to see in future newsletters.

To be removed for our mailing list, call 515-221-1290 or send an email to aliciam@networks-inc.com and type "Unsubscribe" in the subject line.

NetWorks, Inc.

2045 Grand Avenue, Suite F
West Des Moines, IA 50265

Phone: 515-221-1290
Fax: 515-221-0175
Web: www.networks-inc.com



www.buyintothecircle.com



Voted Best Computer
Consulting Company by
readers of Des Moines
Business Record!