

Inside this issue:

HP Trade-In Program 2

Free Tools from Solar-Winds 2

10 Biggest Security Threats of the Future 3

Disaster Recovery Solutions 5

Fortinet Debuts Database Vulnerability Assessment Appliance 5

WELCOME

Andy Smith joined our service team on July 28.

Adam Mead joined our sales team on October 1.

Microsoft Software + Services

The goal of the Microsoft® Software + Services strategy is to empower customers and partners with richer applications, more choices, and greater opportunity through a combination of on-premise software, partner-hosted software, and Microsoft-hosted software. How software is consumed will ultimately be decided by customers based on their IT strategies and specific needs. However, one thing is certain: Choice is always a good thing, and a Software + Services strategy will help Microsoft partners and customers realize their full potential.

Benefits of Software + Services

- Lowers the cost of supporting IT infrastructures
- Affordable access to powerful applications
- Access to a wide range of the most current Microsoft products, including servers and desktop PC applications
- No software to install on company equipment
- Ability to vary license orders each month
- 30-day evaluation licenses available on most software

NetWorks, Inc. recently joined the Microsoft Services Provider Licensing Agreement (SPLA) program. The agreement allows NetWorks, Inc. to offer licenses for many Microsoft products on a flexible, month-to-month basis. Our SPLA agreement allows us to provide a new partner-hosted solution combining software and services to deliver more value to our clients.

In the next month we will communicate more details about our new hosted solutions. Please contact Christine Penniman if you would like to start customizing a solution today.

Email: chrisp@networks-inc.com
Phone: 515-222-2281

NetWorks, Inc. Overstock Deals

NetWorks, Inc. will be offering discounts on overstock product to help reduce our inventory. We are finalizing the product list now and will have it available on our website by the end of October. Check back periodically for updated information at www.networks-inc.com.

HP Trade-In Program

The HP Trade-In Program makes HP technology more affordable, simplifies the removal of sensitive data, and helps to preserve the environment. A wide range of HP and competitive brand products are accepted for trade-in and cash back when purchasing new HP products. It's part of HP Total Care!

Learn how easy it is to get a trade-in allowance you can use toward the purchase of any new HP products, including: desktop computers, monitors, notebooks, printers, plotters, and much more.

How the program works:

1. Get a quote
2. Purchase new HP or Compaq branded products
3. Ship your product(s) for trade
4. Receive your redemption check

For complete details, visit: http://www.hp.com/united-states/tradein/home_flash.html

Tackle Daily Tasks with Free Network Monitoring Tools from SolarWinds

The old saying "you get what you pay for" holds true in just about every way possible – except with SolarWinds' free network monitoring tools.

We've been providing the networking community with free network management and free network monitoring tools since the company was founded nearly a decade ago. The word has spread over the years and now professionals worldwide use our free network monitoring tools and other network management and network discovery solutions to keep their networks up and running.

Choose from the list below to find out why network engineers use our free network monitoring tools for everyday tasks. In fact, more than a million of you now rely on these free tools to perform network monitoring and network management tasks on a daily basis!

- **SolarWinds Free TFTP Server** - upload and download executable images and configurations to network devices - our most popular free network monitoring tool!
- **NEW! SolarWinds Free Real-time NetFlow Analyzer** – capture and analyze up to one hour of NetFlow data to see what types of traffic are on your network, where it's coming from, & where it's going.
- **NEW! SolarWinds Free Exchange Monitor** – continuously monitor Exchange and get real-time insight into services, mail queue sizes, and host server health with this clever desktop dashboard.
- **SolarWinds Free NetFlow Configurator** - configure NetFlow v5 via SNMP on supported Cisco® devices - a perfect complement to Orion NetFlow Traffic Analyzer and our free Real-time NetFlow Analyzer tool!
- **SolarWinds Free Advanced Subnet Calculator** - compute addresses for IP subnets - another perennial favorite in our suite of free network monitoring tools!
- **SolarWinds Free Wake-On-LAN** - remotely power up network PCs.

To download these free tools, go to: <http://www.solarwinds.com/products/freetools/index.aspx>. SolarWinds offers network management products for every environment. More than 50,000 customers trust their solutions to discover, configure, monitor and manage the increasingly complex systems and processes that make up the network infrastructure. Please contact NetWorks, Inc. if you have any questions about solutions offered by SolarWinds.

10 Biggest Security Threats of the Future

State of Technology: Security

By VARBusiness Staff

September 19, 2008

Who knew there were so many ways to become a victim of cyber crime? No doubt, the security landscape has significantly changed as financially motivated criminals create malware, infiltrate systems and steal valuable data and assets. But as security threats grow in size, scope and sophistication, so do the opportunities for channel partners to help businesses secure their networks and reduce the risk of attack. In Everything Channel's State of Technology: Security survey, hundreds of channel partners estimated some of the biggest threats we might see on the horizon through 2009.

#1 Trojans/Info Stealing Keyloggers/Fast Flux Botnets

Attackers often hit the jackpot with information stealing bots and keyloggers that sit silently on systems and steal sensitive and financial data—all completely unbeknownst to the user. Security reports indicate that more than 700,000 pieces of new malware have already been detected since January. And if current malware trends continue, this type of data-stealing malware will more than double in 2009. One of the most notorious Trojans is Storm. Also known as Nuwar, the Storm is the most versatile malware on record. And it is thus far unstoppable. The bot's creators released thousands of variants and code-changing techniques, creating the largest peer-to-peer botnet in history.

#2 Data Loss/Breaches

No one wants to become the next TJX. Data has become a business's most important asset—and cyber criminals know it. Consequently, cyber criminals will increasingly refine their attacks to get at the heart of a businesses' data center. Malware, delivered via blended threats and social engineering, is designed to stealthily swipe data off a user's computer and send it to offshore servers, where it is collected and then used or sold to the highest bidder on the black market. While financial data, such as Social Security numbers, credit card and bank account information will continue to be attractive targets, security experts say that criminals will increasingly focus on intellectual property, passwords and other types of identifying information.

#3 Internal Threats

Whether intentional or accidental, internal threats will continue to be one of the biggest security threats over the next 12 to 18 months. If a company's security policies are unknown or unenforced, users will continue to unknowingly engage in risky behavior, such as surfing unsafe Web sites, clicking on malicious links delivered via e-mails, or failing to encrypt sensitive data. As the workforce becomes increasingly mobile, users will further increase the risk of exposure by working on open networks with unencrypted mobile devices.

#4 Organized Cyber Crime

Gray Pigeons. Honkers Union of China. They sound like teenage garage bands, but in reality they are highly organized and complex cyber crime organizations. In the last two years, groups of hackers once loosely defined with a common goal have coalesced into complex multi-layered global networks. Sophisticated organizations like the Russian Business Network are responsible for creating and distributing much of the malware that is increasingly targeting businesses that span the market segments. And unlike other types of organized crime, cyber crime hackers can rely on their anonymity and international presence in order to avoid detection and escape the law.

#5 Phishing/Social Engineering

Considered a gateway to a larger "blended attack," social engineering is becoming more creative and targeted in nature. In a phishing attack, users will generally be enticed with an alluring e-mail subject line, often touting a fake breaking news headline or a celebrity video. Once the e-mail is opened, the user is treated to a brief message, and encouraged to click on a malicious link embedded in the message claim-

10 Biggest Security Threats of the Future

Continued from page 3

ing to lead to another Web site or video. Instead, the link often links to an infected Web page, which installs malware on the unsuspecting user's computer. Social engineering has become so sophisticated, that attackers have begun to design e-mails specific to targeted individuals—usually executives and others with access to sensitive information—in what is known as a spear phishing attack.

#6 Viruses

While not posing the same threat as in years past, viruses still can wreak havoc on a company's network by infecting files and applications, costing a company thousands of dollars of lost production time. Viruses such as Parite, first detected in October 2001, infects its host file, Netsky, and drops executable malware. Other viruses, such as Virut, are polymorphic file infectors that download and run other malicious programs, meanwhile infecting all the executable files in order to replicate.

#7 Cyber Espionage

Cyber attacks aren't just for stealing credit card numbers and social security information. Following Russia's invasion of Georgia, hackers from both countries escalated what some had termed an all out cyber war by hijacking news and popular Web sites each other's countries. Attacks on Georgian Web sites rerouted visitors and left many government and news sites defaced or blocked entirely. Security experts say to expect that cyber espionage will soon become a standard means of attack during international conflict.

#8 Zero Day Exploits

Once hackers detect a security glitch in an application, it's only a matter of time before they develop malicious code to attack vulnerable systems before a patch is created. These vulnerabilities often affect Web browser and applications relegated to a specific platform. But recently, security researchers detected a variation of a cross-platform Domain Name Server vulnerability that can open the door wide open for what is known as cache poisoning attacks—tricking the DNS to accept an incorrect request which subsequently reroutes unsuspecting users to another, usually malicious, Web site. Once a user is rerouted to the malicious site, financially driven cyber criminals then have the ability to dump Trojans, keystroke loggers and an array of malicious payloads onto users' vulnerable computers. Meanwhile, attackers are working to develop malicious software that can automate Web browser vulnerability exploits, reducing the time it takes to exploit a system to seconds.

#9 Web 2.0 Threats

As more applications migrate to Web 2.0, so will the security threats. Users can expect to see more attacks on social networking sites such as Facebook and MySpace, as well as professional sites like LinkedIn. Attackers will also find more ways to inject legitimate, high trafficked Web sites with malicious code that installs malware onto users' computers or redirect traffic to another site. One recent example included an attack infecting United Nations and some UK government Web sites. Users visiting the infected sites unknowingly downloaded a malicious file that attempted to deliver a combination of eight different exploits. And users should be wary of phony "cleaner" software that dupes users into paying for an application that they believe will rid their system of viruses. In reality, most of these applications are useless at best.

#10 Vishing

Security researchers have found that Voice over Internet Protocol (VoIP) attacks comprised more than double the number of security vulnerabilities in 2007 compared to all of 2006. While VoIP threats seem to be here to stay, the defensive technology is still playing catch-up. And while many users are becoming increasingly savvy to spam, phishing and other Internet related scams, that awareness doesn't always translate to voice protocols. Security experts anticipate a 50 percent increase in VoIP-related threats by the end of this year.

Contact NetWorks, Inc. to schedule a security audit. We offer a broad range of technologies for SMB as well as Enterprise solutions—helping you maintain compliance and security.

Disaster Recovery Solutions

On September 24 we hosted a Disaster Recovery Solutions Seminar with solutions presented by Dell EqualLogic, Data Domain and CommVault. What is your first thought when you hear someone say "disaster recovery plan"? The obvious natural disaster situations in Iowa include floods, tornadoes, and winter power outages. It's easy to overlook the possible threats from inside. Here is a story shared by CommVault about an insider job.

Over a period of nine months, the number of computer malfunctions within a large company had risen from an average of two per year to critical levels. The impact was such that the business fell behind with its invoicing systems and had to buy processing and backup from third parties. As it could not deliver some of its services reliably, it started to lose the confidence of its customers. The situation began to spiral.

Eventually, the company suspected foul play may be involved and called the police. Secret surveillance equipment was installed to monitor staff. One was filmed lightly scratching circuit boards in disk units and also attaching paper clips to them. Both these actions led to a short circuit.

When confronted, he confessed everything. His motive was to earn overtime, which was required to process the overlap work which was delayed by the malfunction. He netted \$1300 over the 9 months. The company lost at least \$950,000 in that same period. (Source: Disaster Recovery Guide)

To read more true stories like this one, go to <http://www.disaster-recovery-guide.com/stories.htm>.

NetWorks, Inc. can consult with you on development of a disaster recovery plan. It's also essential to perform a regular audit of your plan to ensure you are prepared to recover from a major incident. This is not the time to take short cuts. Thorough planning now can save you thousands of dollars in the future.

Fortinet Debuts Database Vulnerability Assessment Appliance for Data Theft Detection and Prevention

On September 22, Fortinet introduced the first in a family of security appliances dedicated to database vulnerability assessment (VA). The FortiDB-1000B appliance is a mid-enterprise product designed to "harden" databases by detecting weaknesses in passwords, access privileges and configuration settings. As databases are fast becoming the next big target for cybercriminals due to the sensitive and valuable information they hold, there is an increasing need for powerful tools that can detect and help guard against data breaches. This is especially critical for vertical industries such as retail, which require compliance with the Payment Card Industry Data Security Standard (PCI-DSS) to protect customers' personal and credit card information.

For more product details, go to: http://www.fortinet.com/products/fortinet_database.html.

NetWorks, Inc. is a Gold FortiPartner and can help answer any questions you have about Fortinet solutions.

About Us

NetWorks, Inc. is a value-added reseller and systems integrator that designs, deploys, and support small, medium and large corporate networks. We started as a system integrator company in 1994, but have grown to offer advanced service and procurement solutions. We strive to find the best ways to support the goals and strategies of every client...no matter if your business is large or small, local or national.

Over the years, NetWorks, Inc. has implemented complete network solutions that grow as our clients prosper. These long-term partnerships are what our clients have depended on since 1994. Whether you have qualified IT personnel on staff or you choose a custom service package from NetWorks, Inc., we can deliver the service that suits the way you work.

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.

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 from our mailing list, send an email to aliciam@networks-inc.com and type "Unsubscribe" in the subject line.

Preferred Partners

Acronis	Insightix
APC	Juniper
Apple	Lenovo
Astaro	Linksys
Barracuda	Microsoft
Check Point	Netgear
Cisco	Nortel
Citrix	Novell
CommVault	PGP
Compellent	Revinetix
DameWare	RSA
Data Domain	ScriptLogic
Dell EqualLogic	SolarWinds
Extreme Networks	SonicWall
Fortinet	Symantec
HP	VMware
IBM	WatchGuard
Inova Solutions	Wyse

Service Offerings

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

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!