VERTEKS
CONNECTION

VERTEKS
VOICE & DATA
NETWORKS

volume 13 number 2

STAYING UP TO DATE

Verteks helps the Marion County Property Appraiser with cost-effective upgrades for its servers, security, backup and phone system.

As the pace of technology change continues to accelerate, organizations in virtually every industry are struggling to keep up. Under pressure to reduce expenses while improving the delivery of services, government agencies in particular tend to lack the budget and manpower to maintain their IT infrastructures.

Through its longtime partnership with Verteks Consulting, the Marion County Property Appraiser has been able to overcome these challenges. Verteks helps the agency take advantage of the latest technology advances to save money, reduce risk and increase efficiency.

The relationship began almost 15 years ago when the agency decided to replace its aging PBX with a voice over IP (VoIP) phone system. At that time, VoIP was still relatively new, and Verteks came highly recommended for its expertise in the technology. Verteks provided a highly competitive quote along with a working demo of a VoIP solution. The fact that Verteks had deployed similar solutions for many different government agencies across Florida made the decision easy.

Since then, the Marion County Property Appraiser has turned to

continued on page 2

VERTEKS CONNECTION

PRSRT STD
U.S. POSTAGE
PAID
Tulsa, OK
Permit No. 2146

Marion County Property Appraiser

continued from page 1

Verteks for all of its IT needs, from PCs and servers to data storage and network upgrades. The agency counts on Verteks for sound advice, responsive support and cost-effective solutions to common IT headaches.

"Everybody I've worked with at Verteks has been more than willing to help with anything we need," said Sherry Sherouse, Senior Programmer and Application Specialist, Marion County Property Appraiser. "They answer all our technology questions, and if they don't know they'll find out and get back to us. They're always very quick to respond and resolve any IT issues that arise."

Stability and Security

The Marion County Property Appraiser was using a mainframe platform as recently as 2009. At that time, the agency implemented several servers to support its applications, but those systems had also begun to show their age. In fact, one of the servers had failed recently, increasing the need to migrate to a newer platform.

Verteks helped the agency implement VMware virtualization technology to consolidate and upgrade its servers. Now all of the agency's applications are on two powerful HP servers, with one of the older servers used as a backup system to minimize the risk of downtime.

"We removed four or five servers and now just have two HP Gen 9 servers that run a total of seven virtual machines. We also have a SAN server that provides storage for the virtual machines," Sherouse said. "Everything is in one place — we only have one VMware environment to log into — and it has definitely helped as far as compacting what we have in the office and giving us more space. Plus, our old servers wouldn't support some of the newer software. With the new system, we'll be able to do some additional projects."

The agency also had an older firewall that had started to fail. Verteks replaced it with a next-generation WatchGuard firewall, improving both security and system availability.

"When your firewall fails, you lose pretty much all access. It also leaves you open for data leaks and security breaches, which of course is a big issue," said Sherouse. "Verteks was able to get everything back up and get us on the WatchGuard firewall. It's easy to manage and we haven't any problems with it."

Data Protection

Verteks has helped the agency improve its data backup and recovery processes with the Datto Total Data Protection system. Data is backed up automatically to a small onsite appliance then replicated to the Datto Cloud. Files can be recovered quickly with just a few mouse clicks.

"The Datto backup system works wonderfully," said Sherouse. "If somebody deletes a file off the network by accident, it just takes a few minutes to go into the Datto system, find the file, download it and put it back where it belongs. With our old system, it would take us hours to do that. Also, our snapshots go back several months and we have, I think, a year's worth of backups in the cloud. So you can restore files from a particular point in time if you need to.

"Recently, somebody deleted a file that I only use occasionally for customer reports. It turned out they had deleted it a couple of months earlier and I didn't realize it because I hadn't used it in that length of time. But I was able to find the correct backup on the Datto system and restore the file. It saved me from having to re-create the whole thing."

With help from Verteks, the Marion County Property Appraiser has been able to replace aging systems with new technologies that help the agency better serve its customers. Although technology continues to change rapidly, one thing remains constant — a strong relationship with a technology partner that helps the agency stay up to date.

> **"Everybody I've worked with at Verteks has been more than willing to help with anything we need ... They're always very quick to respond and resolve any IT issues that arise."**
>
> **— SHERRY SHEROUSE,**
> **Senior Programmer and Application Specialist,**
> **Marion County Property Appraiser.**

News Briefs

Companies Eye Software-Defined Storage

Traditional enterprise storage strategies are under the microscope in 70 percent of IT organizations, according to a recent study from open source infrastructure solution provider SUSE. More than 90 percent of companies surveyed reported interest in the software-defined storage due to frustrations associated with costs, performance, complexity and fragmentation of existing solutions.

FTC Says Phishing Defenses Lacking

Few businesses are taking full advantage of the latest technologies to combat phishing, according to a new study from the Federal Trade Commission (FTC) Office of Technology Research and Investigation. Fewer than 10 percent of the businesses have implemented a Domain Message Authentication Reporting and Conformance (DMARC), a supplemental security technology that would allow them to receive intelligence on potential spoofing attempts and to instruct ISPs to automatically reject any unauthenticated messages that claimed to be from the businesses' email addresses.

Video Conferencing Gains Momentum

An IHS Markit survey of 207 North American firms finds that 86 percent plan to be actively using video conferencing as part of their unified communications by February 2018. That's a slight increase over the previous year's projections.

Verteks Connection

Editorial Correspondence:
7360 E. 38th St.,
Tulsa, OK 74145
Phone (800) 726-7667
Fax (918) 270-7134

Change of Address: Send corrected address label to the above address.

Sounding the Alarm

WannaCry attack serves notice that it's time for Windows 10 migration.

Organizations that have been putting off a migration to the Windows 10 operating system got a wakeup call on May 12. On that day, hackers exploited known vulnerabilities in older versions of Windows to launch the largest cyber extortion attack ever.

The WannaCry ransomware attack was astonishing in both scale and speed, striking hundreds of thousands of computers in about 200 countries within a span of 48 hours. It is believed to be the largest cyber extortion scheme in history.

According to Kaspersky Lab, roughly 98 percent of the computers affected were running some version of Windows 7. Machines running Windows 10 apparently were not affected. Furthermore, the attack exploited a vulnerability for which a patch had been issued months earlier.

"People have always put off OS updates until absolutely necessary, both in an effort to conserve costs and to make sure all the bugs have been worked out of the new version," said Don Gulling, president, Verteks Consulting. "Ultimately, there always comes a point when it simply becomes too risky to cling to the old version. The WannaCry attack makes it clear we've reached that point with Windows 7."

Mainstream support for Windows 7 ended in January 2015, and the end-of-sales date for both 7 and the little-used Windows 8.1 is on Oct. 31. While Microsoft says security patches will be provided for Windows 7 until January 2020, it also warns customers that patches probably won't keep the OS secure.

Holding on to Windows 7 likely will drive up operating costs due to the need to remediate large numbers of malware attacks that wouldn't penetrate Windows 10 systems. Forrester analysts says new and improved security features in Windows 10 will mitigate many threats and reduce remediation costs by 33 percent.

Although users have always loved Windows 7's stability and intuitive design, it is now nearly eight years old. It wasn't built with modern security safeguards.

"Advanced security features are among the most compelling benefits of Windows 10," said Gulling. "Enterprise-grade features such as identity and information protection are built right into the core of Windows 10. Windows 10 also improves data loss prevention by using containers and data separation at the application and file level."

Other significant security features in Windows 10 include:

Virtualization-Based Security. VBS creates an isolated, hypervisor-restricted subsystem for storing, securing, transferring and operating other sensitive subsystems and data. It is essentially an architectural change that vastly reduces the attack surface area and attempts to eliminate the attack vectors themselves. As such, it makes it very difficult for attackers to tamper with core components of the operating system.

Windows Defender Antivirus. This built-in solution uses the cloud, vast optics, machine learning and behavior analysis to rapidly respond to threats. Because emerging "polymorphic" strains of malware change their appearance to evade signature-based scans, Windows Defender also uses behavioral analysis to catch things that haven't been seen before.

Windows Hello. This is biometric-authentication technology designed to help eliminate traditional password vulnerabilities. It supports facial, iris and fingerprint authentication in conjunction with a personal identification number.

Device Guard. This combination of hardware and software features can be configured to lock down a device so that it can only run trusted applications that you define.

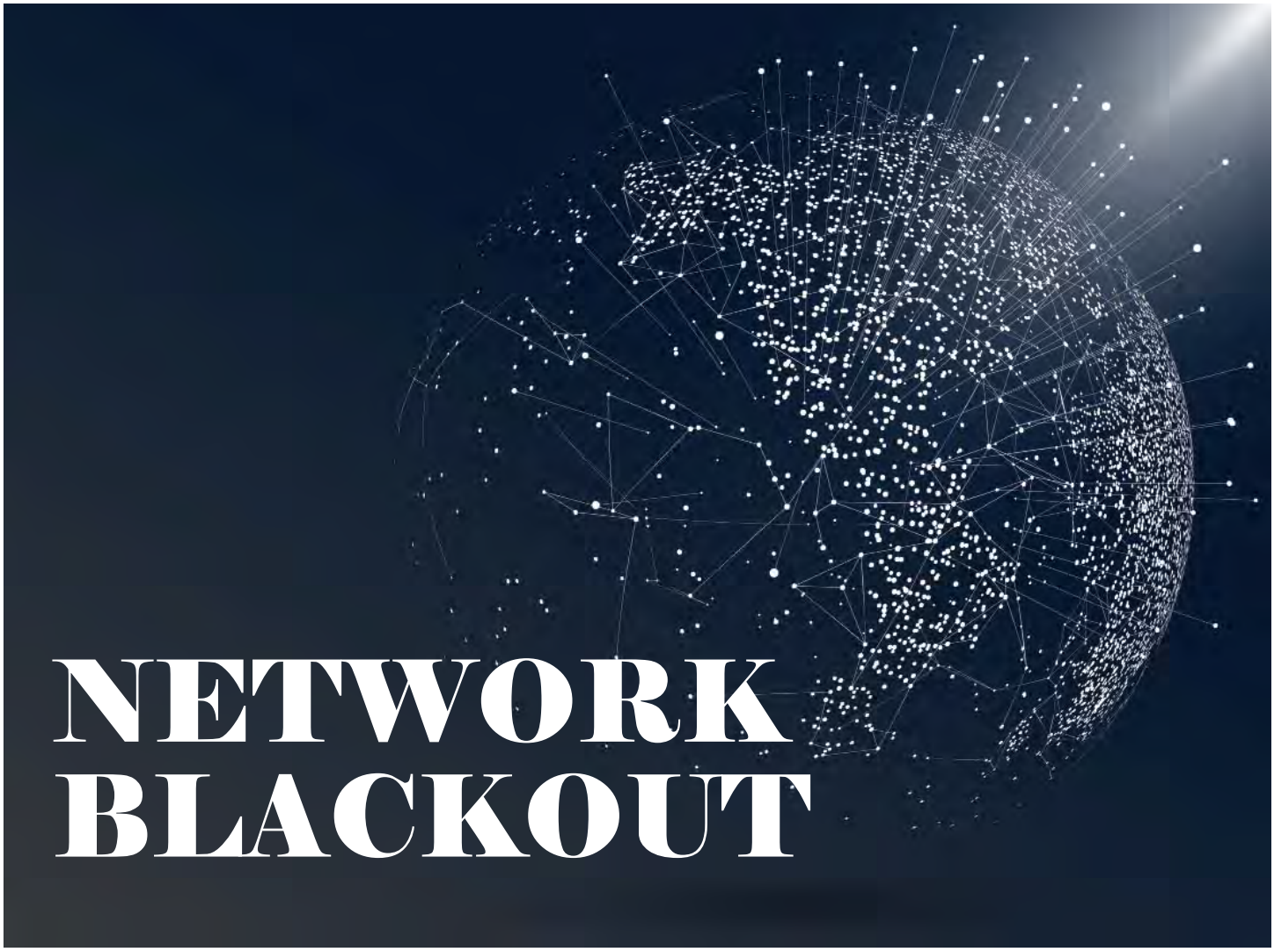
Protected Processes. This feature prevents untrusted processes from interacting or tampering with trusted processes. It makes computers less susceptible to tampering by malware that does manage to get on the system.

It's no real surprise Windows 7 remains the most popular desktop OS with nearly twice the market share of Windows 10. It's familiar, it's reliable and it works. Nevertheless, the WannaCry outbreak illustrates the security risks organizations take if they fail to upgrade.

The global financial services company Credit Suisse says the attack should prompt all organizations to accelerate their plans to upgrade to Windows 10.

"If you're not current, you're toast," analyst Michael Nemeroff wrote in a note to clients following the WannaCry attack.

A migration to Windows 10 won't be without challenges. You have to make sure your hardware meets minimum upgrade requirements and your applications don't suffer from incompatibility issues. If you don't have the time, expertise or manpower for such a project, give Verteks a call. We can simplify the process and help speed your transition to the operating system that offers the greatest protection for your critical technology assets.



NETWORK BLACKOUT

Software-defined perimeter aims to keep potential intruders in the dark.

During World War II, blackout drills were nightly rituals in cities around the world. Street lights were turned out, automobile headlights were dimmed and everyone headed indoors where they covered windows with heavy curtains, blankets or blinds to minimize all outdoor lighting. The idea was that enemy bomber planes couldn't accurately target what they couldn't see.

This simple logic is at the heart of the software-defined perimeter (SDP), a new security approach in which network segments are cryptographically "blacked out" from the rest of the infrastructure. Sensitive information simply cannot be detected by unauthorized users, which dramatically diminishes the opportunities for network attacks.

"The primary objective of the SDP is to make the application infrastructure effectively invisible or 'black' by eliminating DNS (domain name system) information or IP addresses," said Juanita Koilpillai, CEO of Waverley Labs, a cyber risk management company that was selected to develop an SDP solution for the Department of Homeland Security. "SDPs establish an undetectable application infrastructure by changing the historical paradigm and establishing communications with only authorized users rather than communicating with anyone seeking access."

Isolating Assets

The SDP approach evolved from the work done at the U.S. Defense Information Systems Agency (DISA), where network access is based on a "need-to-know" basis. Using a variety of security controls, the DISA enforces strict network segmentation once users gain network authorization in order to prevent them from seeing applications, DNS numbers, IP addresses and other sensitive network elements. This approach mitigates the most common network-based attacks, including distributed denial of service (DDoS) attacks, server scanning, SQL injection, cross-site scripting and more.

The SDP approach has been formalized as a specification published by the Cloud Security Alliance (CSA). It has recently been popularized by companies such as Google, with their BeyondCorp initiative, as well as several other enterprises active in CSA working groups. Gartner analysts say it is rapidly becoming an important element of security for today's open, multitenant cloud architectures.

"Organizations continue to struggle to properly segment and provide adequate access control over their sensitive networks, hosts and applications within their environments beyond the perimeter firewall or segmentation performed at network boundaries," Gartner noted in its Predicts 2016: Security Solutions report. "Through the end of 2017, at least 10 percent of enterprise organizations … will leverage software-defined perimeter technology to isolate sensitive environments."

> **"The primary objective of the SDP is to make the application infrastructure effectively invisible or 'black' by eliminating DNS information or IP addresses."**

Restricting Access

Traditional security measures have focused on creating a defensive barrier between the network and the open Internet. The problem is that the continued decentralization of the network through cloud and mobile technologies has created too many gaps to plug.

Time-honored defenses such as firewalls and intrusion prevention systems are not entirely effective in protecting cloud and critical web applications. In a June 2016 report, cloud security firm Netskope noted that the number of enterprises finding malware in their sanctioned cloud apps nearly tripled from 4.1 percent to 11.0 percent between the Q4 2015 and Q1 2016. The majority of malware detected involved JavaScript exploits and droppers, which are increasingly used to deliver ransomware.

In traditional security models, once someone is verified at the perimeter and allowed access to a network segment — whether legitimately or through a malicious attack — they gain the ability to see and potentially access everything within the network. However, an SDP creates a virtual "air-gapped" network in which unauthorized segments are simply not visible on the network at all. If they can't be seen, they can't be compromised.

This invisible infrastructure is created by strictly controlling network access not just with user authorization, but also with session-specific controls based on contextual variables. These variables can include the user's identity, the user's location, the time of day, the type of device being used, whether the device is running security software, and many more.

Aiding Compliance

SDP solutions go even further, providing additional security controls at the content level within a secured network segment. Even after a user is authenticated, classification and encryption tools ensure that only those with proper access can see and access sensitive data. Content-level controls can also dictate what actions a user can and cannot take with data — for example, whether data can be downloaded or attached to an email. Logging mechanisms allow tracking, alerting and analysis of any anomalies.

These functions also provide significant compliance capabilities. For instance, an SDP addresses Payment Card Industry Data Security Standards (PCI DSS) guidelines with network segmentation that isolates cardholder data from the rest of the network. It also supports current PCI DSS requirements for the use of multifactor authentication.

In addition to advanced protection and improved compliance, SDP solutions also bring new levels of simplicity and automation to the security infrastructure. By combining device authentication, identity-based access, fixed perimeter and dynamically provisioned connectivity controls, an SDP strengthens security while reducing management complexity.

The cloud computing facilitates simple, powerful and affordable solutions that resolve significant business challenges and deliver peace of mind. However, the open nature of the cloud also brings unique security risks. By blacking out sensitive network identifiers, the software-defined perimeter brings an old-fashioned sensibility to modern security requirements. Hackers can't attack what they can't find.

ShoreTel
Brilliantly simple™

Business VoIP with the industry's highest customer satisfaction & lowest TCO

You owe it to your company to check out ShoreTel.

Streamlining the work of IT staff and users alike, ShoreTel's unified communications phone system provides:

- **MANAGEMENT EASE** – It's plug-and-play, maintainable from anywhere on the network
- **UNPARALLELED USER EXPERIENCE** – call control like never before with full feature access, including IM, mobility, video, and collaboration tools
- **ABSOLUTE RELIABILITY** – 99.999% availability for 100% peace of mind with the best customizable business continuity strategy in the business
- **ROI** – Many customers say their ShoreTel system pays for itself within a year
- **THE SUPPORT YOU NEED** – Independent surveys, industry awards and carefully monitored feedback from customers confirm it

Contact Verteks to see how ShoreTel's unifed communications system will change how you view your business phone system.

VERTEKS
VOICE & DATA NETWORKS

1-877-VERTEKS | 352-401-0909 | www.verteks.com