January 2015

PROSYS

Tech Outlook

Samsung's 'business-rugged' Galaxy Tab Active stands up to harsh treatment.

Mobile technologies are driving profound changes in how organizations conduct business, interact with customers and streamline processes. As part of this progression, tablet computers are becoming increasingly valuable tools for business users. No longer merely personal productivity devices, tablets have evolved into powerful platforms for delivering a host of enterprise applications that support major business initiatives.

Market analysts with Frost & Sullivan report that nearly half of all enterprise organizations now issue corporate-owned tablets to their workforces. The firm predicts steady growth as organizations link tablets to enterprise communications, productivity and back-office applications.

However, there seems to be one nagging concern regarding tablets: are they tough enough?

Accidents Will Happen

While acknowledging increased confidence in tablets as a business tool, 53 percent of IT decision makers recently surveyed by Technology Business Research expressed apprehension about durability. A tablet that can't withstand the elements that mobile workers experience on a daily basis isn't worth the investment.

"You have to be prepared for the fact that tablets are probably going to take a real beating — whether they're being tossed into a car, splashed with

continued on page 2

TECH OUTLOOK

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

One Tough Tablet

continued from page 1

coffee, knocked off a desk or dropped on the floor," said Matt Merriman, VP of Professional Services, ProSys. "Most organizations don't want to risk becoming too dependent on any device with a potentially high failure rate.

"It's not just about the cost of the device, or the cost of repairs or replacement. There are just too many intangible costs — data loss, wasted time, lost sales, customer service impact and more."

Samsung is addressing these concerns with the introduction of the Galaxy Tab Active, a "business-rugged" tablet with improved durability features geared specifically for business users. With its protective cover, it can withstand drops from 4 feet. It has an IP67 certification, which means it is dust and water resistant. In fact, Samsung claims the Active can survive being submerged in over 3 feet of water for up to 30 minutes — without the need for any special port covers.

User Insight

Samsung engaged in a series of advisory group workshops with Fortune 500 companies in order to learn what business leaders wanted from a mobile device. Companies spanning 12 different industries were represented, including retail, logistics and transportation businesses. Samsung combined the results from the workshops with its own market insight for the creation of the Galaxy Tab Active.

"This device represents Samsung's commitment to develop a customer-centric model that can be used for vertical integration across all key industries," said Tod Pike, senior vice president at Samsung's Enterprise Business Division. "Samsung continues to develop new products with feedback from professionals to change the way people think about technology for business."

Professionals in field-service industries such as public utilities and telecommunications can depend upon the Active with its Ultra Power saving mode and a long-lasting battery to deliver up to 10 hours of continuous operation. Additionally, the detachable battery provides a quick and easy exchange for a fresh battery when necessary for uninterrupted working. A built-in pogo pin charging port allows quick and easy battery recharging without the need for a separate USB device.

Workers will be able to use the tablets even while wearing gloves or other hand protection through the inclusion of an integrated C-pen stylus, which can be used to "write" on the Active's screen.

The 3.1MP Auto Focus Camera can easily scan barcodes, and the Galaxy Tab Active's near field communications (NFC) technology saves time on communications and work process management. These essential features can greatly boost productivity, such as with transportation and logistics managers who can use the Active to seamlessly connect with a building's foreman on shipping and receiving.

Security and More

The Active includes Samsung Knox, a defense-grade mobile security solution. Knox is an Android-based platform that creates a virtual partition between personal data and company applications and data. Knox offers multi-layered protection from the device down to the kernel with two-factor biometric authentication for authorized device access.

The Active is powered by an Exynos processor, 1.5GB of RAM and 16GB of storage, which can be expanded via the microSD card slot. It comes with a three-year extended warranty covering damage caused by accidents. Also, the remote Smart Tutor Service gives users easy and quick tech support access anywhere, anytime.

The new tablets also feature enterprise-ready compatibility with Citrix and SAP certification for SAP Work Manager and SAP CRM Manager, with additional built-in application support and capabilities to come, according to Samsung.

"There's no doubt that tablets can help businesses of all types become more efficient, productive and effective," said Merriman. "The Galaxy Tab Active extends all those benefits to those who work outdoors or in harsh environments such as warehouses or manufacturing plants. It's built to take a beating."

The Galaxy Tab Active's long-lasting (8-10 hours) battery and an easily replaceable backup battery deliver uninterrupted working. That means this rugged device provides access to real-time information for workers on the move or on site all day long.

News Briefs

Security Pros Optimistic

Although 2014 stands as the worst year on record for data breaches, IT security professionals are surprisingly optimistic about their ability to prevent cyber threats going forward. Enterprise security staffers are so confident that 81 percent of those responding to a recent survey said they would "personally guarantee" that their company's customer data will be safe in 2015.

This result comes from a survey of 250 IT professionals from companies of 2,000 or more employees conducted by ThreatTrack Security.

Although 68 percent said their organization is more likely to be the target of a cyber-attack in 2015, 94 percent are optimistic that their organization's ability to prevent data breaches will improve — largely because they expect senior management to be more responsive to their security recommendations.

"What we found is that security professionals are supremely confident that their ability to defend against data breaches and advanced malware threats will improve in 2015," said Julian Waits, Sr., president and CEO of ThreatTrack Security. "That optimism seems rooted in their growing confidence in the leadership provided by their Chief Information Security Officer and the fact that they expect to invest in new cybersecurity solutions, including advanced threat detection technologies and threat intelligence services."

Respondents said the types of threats they most fear are advanced persistent threats (65 percent), targeted malware attacks (61 percent) and spear phishing attacks (42 percent). They fear mobile threats (22 percent) least.

Downtime, Data Loss Costs: $1.7 Trillion

Data loss and downtime cost enterprises $1.7 trillion in the past year, according to a new report from EMC. The firm surveyed 3,300 IT decision makers from 24 countries and found that while the overall number of data loss incidents has decreased, the volume of lost data has increased by 400 percent over the past two years.

Those surveyed said new technologies are creating challenges for which they are unprepared. Seventy-one percent said they are not fully confident in their ability to recover after a disruption.

Only 6 percent said they have a disaster recovery plan for incidents related to big data, hybrid cloud and mobile. More than half don't have a recovery plan for any of these emerging workloads, and 62 percent consider these environments difficult to protect.

Tech Outlook

Copyright © 2015 CMS Special Interest Publications. All rights reserved.

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.

Some parts of this publication may be reprinted or reproduced in nonprofit or internal-use publications with advance written permission. Tech Outlook is published monthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

ProSys locations

Atlanta, GA
(Headquarters)
Phone: 678-268-1300
Toll-Free: 888-337-2626
chash@prosysis.com

Atlanta, GA
(Integration Center)
Phone: 678-268-9000
Toll Free: 888-337-2626
twheless@prosysis.com

Austin, TX
Phone: 512-658-5847
Toll Free: 888-337-2626
jwestmoreland@prosysis.com

Birmingham/Montgomery, AL
Phone: 205-314-5746
Toll-Free: 800-863-9778
birminghamsales@prosysis.com

The Carolinas
Toll-Free: 888-337-2626
chash@prosysis.com

Knoxville, TN
Phone: 865-310-8843
Toll-Free: 800-863-9778
pmadden@prosysis.com

Lexington, KY
Phone: 859-887-1023
Toll-Free: 800-863-9778
dclemmons@prosysis.com

Louisville, KY
Phone: 502-719-2101
Toll-Free: 800-863-9778
dclemmons@prosysis.com

Miami, FL
Phone: 305-256-8382
Toll-Free: 800-891-8123
lspivack@prosysis.com

Mid-Atlantic
Phone: 800-634-2588 ext 2
midatlantic@prosysis.com

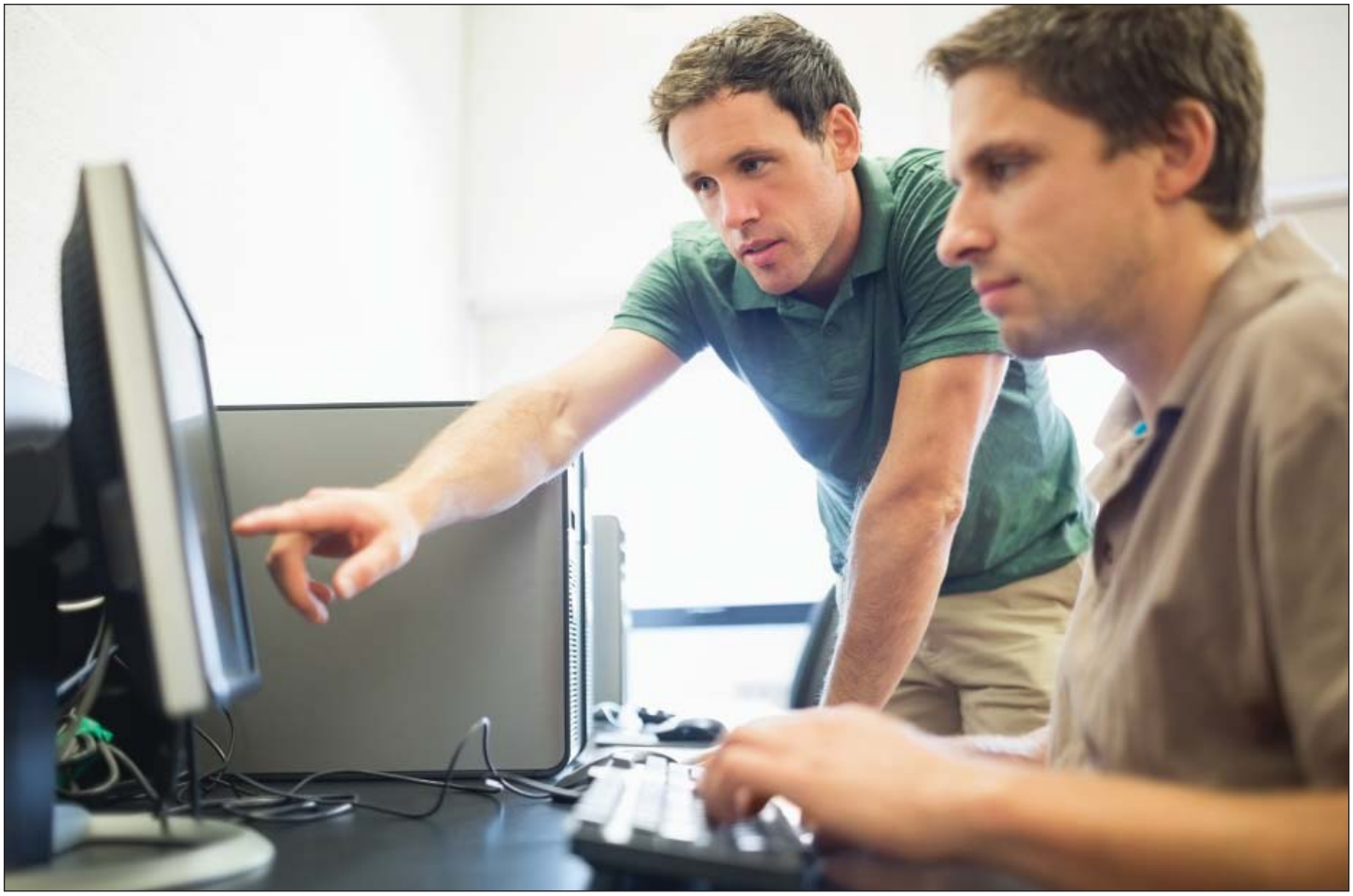
Nashville, TN
Phone: 615-301-5200
Toll-Free: 800-863-9778
dclemmons@prosysis.com

New England
Toll Free: 800-634-2588 ext 1
newengland@prosysis.com

New York/Metro
Toll Free: 800-634-2588 ext 3
nymetro@prosysis.com

Seattle
Phone: 425-939-0342
sballantyne@prosysis.com

Tampa, FL
Phone: 813-440-2410
800-891-8123
lspivack@prosysis.com



User-Driven Design

Microsoft is counting on unprecedented user collaboration to help deliver platform unification with upcoming Windows 10.

When Microsoft released Windows 8 in late 2012, it marked a radical departure from the company's operating system legacy, featuring a new interface designed for touchscreen, mouse, keyboard and pen input. It was Microsoft's response to the "post-PC era" — an OS that would unify desktops, laptops, tablets, smartphones and gaming consoles.

To date, however, neither businesses nor consumers have been overly enthusiastic. Windows 8 and version 8.1 combined currently have only about 12 percent of the OS market share, trailing Windows 7 (53 percent) and the out-of-support Windows XP (24 percent). Surveys show users have been confused over Windows 8's dual user interfaces, have trouble accessing installed applications and can't always figure out what apps they have open.

In an effort to address such user satisfaction issues, Microsoft changed its entire approach to the development of Windows 10, which is expected to launch in late summer 2015. The company's new "Windows Insider" program represents its largest-ever open, collaborative development effort, and it is designed specifically to produce a much more intuitive final product.

Program participants receive the technical preview of Windows 10 and a steady stream of revisions, and they will be able to give feedback throughout the development cycle. There are various ways for these "insiders" to engage in a two-way dialogue with Microsoft, including a Windows Feedback app for sharing suggestions and issues and a Windows Technical Preview Forum for interacting with Microsoft engineers and fellow Insiders.

Even the name of the product represents an important shift for Microsoft. Terry Myerson, executive vice president of the company's operating systems group, said they decided not to call this version Windows 9 because they consider it to be substantially more than an incremental product update.

Platform Unification

Windows 10 adapts to the devices customers are using — from Xbox to PCs and phones to tablets and tiny gadgets — and what they're doing with a consistent, familiar and compatible experience, enabling greater productivity. Windows 10 will run across the broadest range of devices ever, from the Internet of Things to enterprise data centers worldwide. Microsoft is also delivering a converged application platform for developers on all devices with a unified app store. Developers will be able to write an application once and deploy it easily across multiple device types, making discovery, purchase and updating easier than ever for customers.

Windows 10 builds nearly everything that businesses need right into the core of the product — including enterprise-grade security, identity and information protection features — in ways that can reduce complexities and provide better experiences than other solutions. One area of advancement is in the work Microsoft has done with user identities to improve resistance to breach, theft or phishing. Windows 10 will also help advance data loss prevention by using containers and data separation at the application and file level, enabling protection that follows the data as it goes from a tablet or PC to a USB drive, email or the cloud.

Management and deployment have been simplified to help lower costs, including in-place upgrades from Windows 7 or Windows 8 that are focused on making device wipe-and-reload scenarios obsolete. Businesses will also have the flexibility to choose how quickly they adopt the latest innovations and influence continued improvements. In addition, organizations will be able to customize an app store specific to their needs and environment. The intent is an app store that will allow for volume app licensing, flexible distribution, and the ability for organizations to reclaim or reuse licenses when necessary.

Early Reviews

The early technical preview of Windows 10 demonstrates new levels of flexibility, navigation and familiarity throughout the Windows experience. Features include:

Expanded Start menu. The familiar Start menu is back, providing quick one-click access to the functions and files that people use most, and it includes a new space to personalize with favorite apps, programs, people and web sites.

Apps that run in a window. Apps from the Windows Store now open in the same format that desktop programs do. They can be resized and moved around, and have title bars at the top allowing users to maximize, minimize and close with a click.

Snap enhancements. Working in multiple apps at once is easier and more intuitive with snap improvements. A new quadrant layout allows up to four apps to be snapped on the same screen. Windows will also show other apps and programs running for additional snapping, and it will even make smart suggestions on filling available screen space with other open apps.

New Task view button. The new Task view button on the task bar enables one view for all open apps and files, allowing for quick switching and one-touch access to any desktop created.

Multiple desktops. Instead of too many apps and files overlapping on a single desktop, it's easy to create and switch between distinct desktops for different purposes and projects — whether for work or personal use.

"Windows 10 represents the first step of a whole new generation of Windows, unlocking new experiences to give customers new ways to work, play and connect," said Myerson. "This will be our most comprehensive operating system and the best release Microsoft has ever done for our business customers, and we look forward to working together with our broader Windows community to bring Windows 10 to life in the months ahead."

Pirated XP Ripe for Botnets

Although Microsoft ended support for the XP operating system in April 2014, the decade-old OS still holds the No. 2 spot in the global desktop OS market. Industry watchers say many of those still using XP are running pirated copies from China.

It is estimated that millions of computers in China are running pirated copies known as "Ghost XP." This refers to copies of the OS made using the Norton Ghost backup utility. Because the ghost image includes all necessary drivers and software, it can be installed from disk in only about 15 minutes.

Experts say all those unsupported XP machines in China could pose a threat to the Internet in general if they become compromised by bot-herders, who could use the infected PCs to launch digital attacks. Recent events indicate that XP machines are a popular target for cybercriminals.

Researchers at the security firm Proofpoint recently reported gaining access to a server being used by a group of Russian-speaking hackers to control a botnet consisting of 500,000 hacked PCs — more than half of which were running XP. The Citadel botnet taken down by the FBI in 2013 was running primarily on machines using pirated versions of XP.

Protecting Cardholder Data

Version 3.0 of the PCI Data Security Standard aims to make payment card security an everyday business practice.

Target. Home Depot. Michaels. These are just three of the major retailers that fell victim to cyber crime in 2014, making it the Year of the Data Breach. Hundreds of millions of credit card numbers and other personal records were stolen from companies of all sizes during the year. According to Chester Wisniewski, senior security analyst at Sophos, as many as six in 10 American consumers have been affected.

Preventing 2015 from being a repeat (or worse) requires a new approach to credit card security. That's the aim of version 3.0 of the Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS), released by the PCI Security Standards Council in late 2013. The central message conveyed by the new standard is that payment security must be an everyday business process, a shared responsibility across the entire organization to protect cardholder data.

In many cases, organizations have been putting compliance on the back burner until it needs to be assessed and validated. According to a Tripwire survey, only 41 percent of retail establishments are taking steps to pinpoint security vulnerabilities.

Moving forward, the PCI Security Standards Council expects payment security to become a business-as-usual discipline. As part of this shift in approach, organizations will be required to self-validate their own processes, services and technology to identify and correct compliance issues.

The effective date of PCI 3.0 was January 1, 2014, but PCI 2.0 remained active through 2014 to allow organizations sufficient time to transition to the new standard. Most PCI 3.0 requirements go into effect January 1, 2015, although some of the new directives will remain "best practices" until July.

Ensuring Compliance

The PCI DSS, mandated by Visa, MasterCard and other card issuers, requires "all merchants with internal systems that store, process or transmit cardholder data" to comply with key data protection measures and submit to security audits. Under the rules, companies must protect cardholder transaction data through logical and physical access controls, activity monitoring and logging, encryption and regular network scans. Companies could face penalties of up to $500,000 for breaching customer credit card information.

Payment applications that are used to store, process and transmit cardholder data are governed by the PA-DSS standard, which is derived from the PCI DSS Requirements and Security Assessment Procedures. Use of a PA-DSS-compliant application by itself does not make an entity PCI DSS-compliant; that application must be implemented into a PCI DSS-compliant environment. However, payment applications should facilitate PCI DSS compliance.

PCI 3.0 represents a significant update of the standard. While version 2.0 contained only two different requirements compared to version 1.2.1, version 3.0 has 20 different requirements compared to version 2.0.

Most of the changes involve clarification of existing requirements as opposed to new ones, but PCI 3.0 also includes best practices for ensuring PCI-DSS compliance on a regular basis. These best practices include ongoing monitoring of security software and protocols to make sure they're operating

properly, and implementing processes to quickly detect and address security control failures.

An ongoing concern has been whether cardholder data is adequately segmented from other networks. In light of this, merchants must conduct penetration tests and vulnerability assessments according to an industry-accepted methodology to determine if a security breach is possible. Those organizations that don't have in-house personnel with the expertise to conduct such a test will need to hire a service provider who adheres to a formalized methodology that validates segmentation.

Maintaining Control

Merchants must maintain an inventory of system components that lists all hardware and software used in the cardholder data environment and describes what each piece of technology does and for what purpose. Organizations that have many locations and those that utilize virtualization may struggle to manage the inventory of these ever-changing system components.

Point-of-Sale (PoS) devices that capture cardholder data must be inventoried and periodically inspected to ensure they haven't been altered or replaced by different devices. Because card skimming is a prevalent problem, employees must be able to identify signs of tampering or suspicious behavior, which is likely to require additional security training for anyone who works at the point of sale. Physical access to PoS by employees must be controlled and authorized by the merchant, and if an employee leaves, access must be revoked immediately.

In addition to using unique authentication credentials for each customer environment, PCI 3.0 requires service providers to provide comprehensive written details of compliance-related services, roles and responsibilities. Documentation should clarify which PCI compliance requirements are the responsibility of the merchant and which are the responsibility of the vendor or service provider. Agreeing to the scope of each party's responsibilities in writing will add accountability and avoid confusion during compliance assessments.

Previously, anti-malware systems needed to work, remain current and produce report logs. Under PCI 3.0, merchants are required to "identify and evaluate evolving malware threats" and have a process in place that alerts the organization of new malware. The anti-malware system must also be configured to prevent users from disabling or altering the system without authorization from management.

No merchant wants to fall victim to cyber crime — in addition to financial costs, a data breach can irreparably damage a business' reputation. While PCI 3.0 won't prevent a data breach, organizations can reduce security risks by adhering to its requirements.

Samsung GALAXY Tab Active

BUILT FOR BUSINESS

Thrive in any business environment with a field-proven, work-ready tablet.

PROSYS

www.prosysis.com 888-337-2626

©2015 Samsung Telecommunications America. All rights reserved. SAM-05