Tech Outlook

April 2017

PROSYS
A PIVOT COMPANY

One for All

HP Elite x3 combines the best features of multiple mobile devices.

The continuing refinement of mobile computing has fundamentally changed the way people work. From notebook computers to tablets and smartphones, increasingly powerful devices have untethered workers from the desktop. Workers today spend more than a third of their time away from their desks, leveraging a diverse mix of devices and applications to collaborate with others and share information.

The average online adult in the U.S. has more than four connected devices, according to a 2016 Forrester Research report. It would not be uncommon for someone to start the day by checking email from a tablet, then updating a project proposal from a laptop, and finally using an app such as Slack or Microsoft Teams to collaborate with colleagues via a smartphone. It may sound like a fluid and effective work style, but it actually can be just the opposite.

"For all the productivity benefits these devices deliver, they also create substantial challenges," said Tommy Whatley, VP, Professional Services, ProSys. "From an IT standpoint, it is extremely difficult to coordinate and manage a collection of both company-owned and self-purchased devices that utilize different operating systems, applications and security measures. Users themselves also face the challenge of juggling multiple phone numbers, email addresses, passwords and collaboration tools."

Multiple Choice

HP is addressing those challenges with the HP Elite x3, a three-in-one device that combines PC power and productivity with premium smartphone capabilities in a sleek form factor that can also dock with large-format monitors and keyboards for a desktop-like

continued on page 2

TECH OUTLOOK

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

continued from page 1

experience. The Windows 10 Mobile operating system with the Continuum feature enables users to run key applications across these different experiences seamlessly.

By utilizing Continuum in Windows 10, the Elite x3 enables frictionless multiscreen transitions between a phone scenario and a desktop PC scenario. Users can dock the Elite x3 with its ecosystem of accessories while also retaining all the mobile functionality of a business-grade "phablet."

"What's really cool about Continuum is that when you've connected the Elite x3 to a desktop or a laptop to work in some productivity app, you can still use the phone features just as you normally would," said Whatley. "You don't have to disconnect to take a phone call. You can talk, text, tweet or whatever without interrupting what's playing on the big screen."

With this capability, users no longer need to worry about what device to use in what environment. The Elite x3 also utilizes biometrics to unlock the device — adding an extra layer of protection for enterprise customers.

Powered Up

The Elite x3 delivers this experience through the power of its Qualcomm Snapdragon 820 processor — a "System on a Chip (SoC)" semiconductor designed specifically to boost the capabilities of mobile devices. The Snapdragon central processing unit has four cores for extremely efficient multitasking. A graphics processing unit, a 4G LTE wireless modem, an image signal processor and other features allow the Snapdragon to support the device's global positioning system, camera, gesture recognition, video and more.

"The processor's powerful performance and low power consumption enable a PC-like experience, and HP has taken advantage of that power with an impressive array of accessories for the Elite x3," said Whatley. "The accessories really are key to moving beyond the sort of fragmented mobile environment we have now and towards a more integrated workflow transformation."

The HP Desk Dock and the optional Mobile Extender allow people to work with the device on their own terms, regardless of location. Users can also enjoy easier, faster charging with Qualcomm Quick Charge 3.0 technology.

The Desk Dock offers a full-featured desktop environment for the Elite x3. It includes a DisplayPort for external monitor support, two USB-A and one USB-C connections, and wired Ethernet connectivity. The Elite x3 docks in portrait mode at a comfortable viewing angle when sitting at a desk. The dock also supports the Elite x3 with and without a protective case.

The HP Mobile Extender creates a laptop-like configuration using a near-zero bezel 12.5-inch diagonal HD display. For additional security, no data is stored on the Mobile Extender. All apps, passwords and files are managed and stored from the Elite x3.

Support for Legacy Apps

The Elite x3 is not the first device to leverage the Windows Continuum technology to connect with large screens, mice and keyboards. However, those other devices have a significant limitation — they can only run Universal Windows Platform (UWP) applications. UWP is the application architecture Microsoft introduced in Windows 10 for the development of apps that can run on both Windows 10 and Windows 10 Mobile.

HP eliminates that limitation with the addition of its HP Workspace application in the Elite x3. HP Workspace is a virtualization service that allows users to remotely run legacy .NET and Win32 apps in addition to UWP apps. HP Workspace essentially creates a virtual PC, giving users access to an HP-curated catalog of x86 apps via a subscription service. Users benefit from quick access to their virtualized apps with full keyboard and mouse functionality not typically available from a mobile device when using the Desk Dock and Mobile Extender.

Today's workers rely upon multiple devices to get work done, but that workstyle has become difficult to support. IT departments are struggling to manage and secure company data on a growing range of devices, and employees are finding their productivity is hampered when they have files and data scattered across multiple applications and devices. With the Elite x3, HP is delivering the next generation of computing where smartphone mobility meets PC productivity on a single device.

News Briefs

IoT Vendors Urged to Improve Security

Manufacturers of Internet of Things (IoT) devices must employ "security by design" principles to reduce the growing cybersecurity risks created by the embedded connectivity of these devices, according to a new study from Juniper Research. The firm also calls on corporate-scale vendors such as Amazon, Google and Samsung to take the lead in galvanizing IoT vendors to apply security best practices.

The research firm estimates that the installed base of IoT devices will reach more than 15 billion units by 2021, an increase of 120 percent over 2016. Juniper cautioned that the vast scale of this connectivity will, unless action is taken, lead to an unmanageable cybersecurity risk created by botnets in excess of 1 million units.

A botnet comprising IoT devices was identified as the key factor in the 2016 distributed denial-of-service (DDoS) attack Domain Name System (DNS) provider Dyn. It was the largest such attack ever recorded.

"Attacks such as those on Dyn last October can be viewed as proofs of concept," noted Steffen Sorrell, author of the Juniper study. "In the medium term, botnets will be used far more creatively — not only to disrupt services but also to create a distraction enabling multipronged attacks aimed at data theft or physical asset disruption."

Juniper also predicts the cybersecurity industry will be forced to move beyond traditional signature-based detection methods in the near term, and will increasingly use machine learning to disruptively protect against DDoS and malicious network activity.

Hacker Takes Down 'Dark Web' Sites

A hacker claiming to be affiliated with the vigilante hacktivist organization Anonymous took down roughly 20 percent of the highly encrypted "Dark Web" in February by compromising the largest underground web hosting service, according to news reports.

The hacker, who contacted the online magazine Motherboard to claim responsibility for the operation, took down roughly 10,000 websites in a protest against child pornography. The hacker claimed to have harvested 80 gigabytes of files and databases from the hidden web-hosting service Freedom Hosting II — more than half of which was reportedly child porn.

The hacker told Motherboard he didn't originally intend to shut down the hosting service but became annoyed by the amount of child porn on the site — despite the service's claim that it has a "zero tolerance" for such materials.

"We are disappointed," the hacker wrote in a message left on Freedom Hosting II's site. "We are Anonymous. We do not forgive. We do not forget. You should have expected us."

Other materials reportedly exposed in the attack included numerous references to botnets — automated computer networks used to launch distributed denial of service (DDoS) attacks, spew out spam or steal data — along with email addresses, usernames and passwords from dark web sites.

Tech Outlook

Editorial Correspondence:
10221 E. 61st Street
Tulsa, OK 74133
Phone (800) 726-7667
Fax (918) 270-7134

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

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

Indianapolis, IN
Phone: 317-688-1283
Bill.sanders@prosysis.com

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

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

Mexico City
Phone: +52 (55) 3601 3755
info@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
info@prosysis.com

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

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

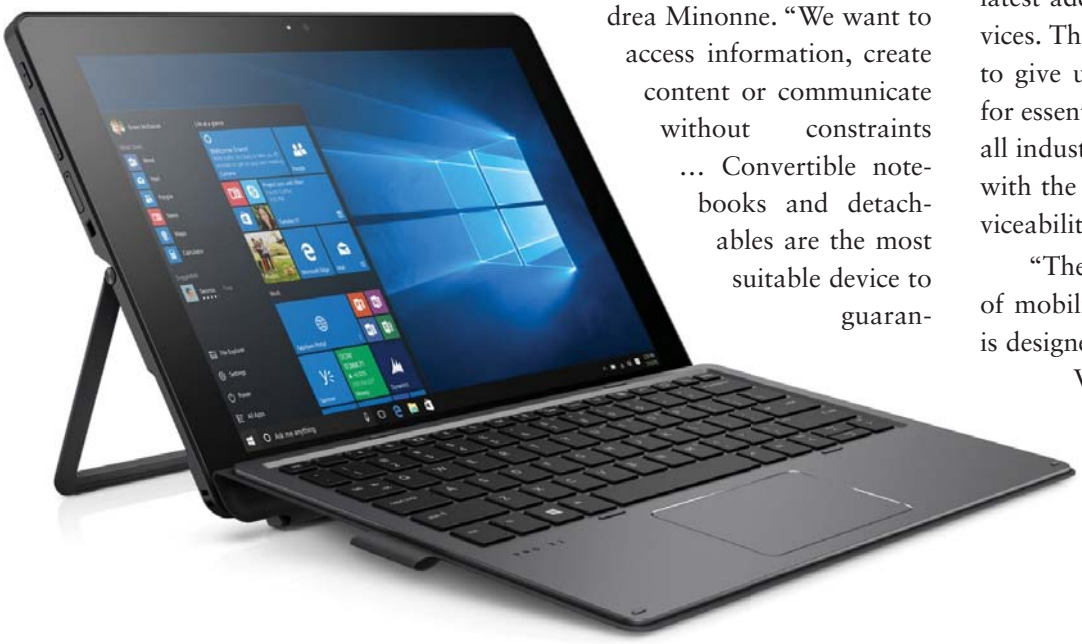
Tampa, FL
Phone: 813-440-2410
800-891-8123
lspivack@prosysis.com

Double Duty

HP's latest 2-in-1 device offers business-grade flexibility, durability and security.

After the initial popularity of tablet computers, business users are apparently finding the devices too one-dimensional for their needs. According to International Data Corp., the fourth quarter of 2016 marked the ninth consecutive quarter that tablet shipments have declined. However, 2-in-1 devices that share the characteristics of both tablets and laptops are gaining favor.

"Customers are looking for solutions that allow for flexibility," said IDC Research Analyst Andrea Minonne. "We want to access information, create content or communicate without constraints … Convertible notebooks and detachables are the most suitable device to guarantee functionality and mobility at the same time."



Convertibles are devices with keyboards that rotate, fold or slide behind the display, while detachables have removable keyboards. To date, these devices have generally been considered consumer-grade devices lacking the performance and durability required for serious business users.

Designed for Business

HP is changing that mindset with the latest addition to its line of x2 2-in-1 devices. The HP Pro x2 612 G2 is designed to give users the performance they need for essential workflow applications across all industries, delivering high productivity with the enterprise-class security and serviceability IT requires.

"The Pro x2 strikes the right balance of mobility and security in a device that is designed to last," said Tommy Whatley, VP, Professional Services, ProSys. "It's a versatile detachable device that features multiple modes ideal for power users — including presentation mode, inking mode for

taking notes, tablet mode for data collection, and notebook mode. It can be configured with a choice of the latest 7th Generation Intel Core processors, providing reliable performance to meet a variety of end-users' needs."

The design goals for the Pro x2 were focused on mobile productivity, with a fast-charging battery that offers up to 11 hours of battery life. The device's magnetically attached Collaboration Keyboard features dedicated keys to directly manage voice and video conference calls. For drawing and taking notes, the HP Active Wacom Pen with App Launch combined with the extended 165-degree kickstand make it easy to present and share. The Pro x2 includes a USB-C connection for quick charging and data transfers and USB-A for accessing traditional legacy peripherals.

Durability was another key consideration. The Pro x2 design underwent more than 120,000 hours of multitiered testing, passing the MIL-STD military-grade assessment standards for drops, humidity, temperature changes and functional shock. A ventless design keeps it operational in dusty environments. A ruggedized case is also an option for users in extreme work environments. It features a 360-degree rotating hand strap, shoulder strap, stylus holder and optional port plugs, and is compatible with the Pro x2 keyboard.

Focus on Security

IT requirements for security and full-lifecycle management were also key focus areas for the Pro x2. The device was built from the ground up for secure work environments and includes a built-in smart card reader, a removable SSD, and the HP Client Security Suite Gen3, along with fingerprint sensor and Near Field Communications options.

A number of accessories are designed to improve the device's functionality. The HP Elite USB-C Dock allows the Pro x2 and other x2 models to be linked with larger displays for a desktop experience. For mobile professionals who need access to additional peripheral ports while on the go, the HP USB-C Travel Hub delivers pass-through connectivity for displays. It also charges the device while it is being used. For retail environments, the HP Retail Case 12 combines with the Pro x2 to create a portable solution for store associates to sell and conduct mobile transactions on the sales floor.

"Organizations in all industries understand the value of a mobile workforce, and they are eager to empower employees with the tools that will let them effectively do businesses anytime, anywhere," said Whatley. "The Pro x2 is a significant step up from other 2-in-1 devices that have hit the market in the past few years. It has the processing power, battery life and durable design to handle the most important tasks a mobile worker is likely to face on a daily basis."

Beyond the Password

Enhanced biometrics solutions boost security through stronger authentication.

The password has been a linchpin of security for millennia, a common way to demand proof of identity in order to control access to an area. It may have been effective for medieval castle sentries, but the password has become notoriously inadequate for protecting modern IT environments.

Former Homeland Security chief Michael Chertoff says the password is "by far" the weakest link in IT security today, and the statistics back him up. Sixty-three percent of all confirmed data breaches involve weak, default or stolen passwords, according to Verizon's 2016 Data Breach Investigations Report. Many of the most high-profile data breaches in recent years have resulted from compromised passwords, including attacks on the Democratic National Committee, Yahoo and Sony Pictures.

What's worse, security experts believe these attacks will spawn an inevitable series of aftershock breaches in which passwords sold through "dark web" markets are used in new attacks — possibly several years after the original theft. Experian reports that credentials stolen in a 2014 Yahoo breach that exposed 500 million accounts were subsequently resold and used by other criminals to compromise accounts across a wide variety of services where consumers use the same username and password.

Unfortunately, there's no sign that understanding the danger changes user behavior. When it comes to passwords, convenience still trumps caution. For five years running, "123456" and "password" have ranked as the most commonly used passwords in an annual study by SplashData.

"Passwords are broken. They have become one of the weakest links in our security chain," said David Ferbrache, technical director at KPMG's cybersecurity practice. "People are being forced to adopt more and more convoluted passwords while simultaneously trying to avoid the temptation to reuse (them). It is high time we moved to a more sophisticated approach."

Getting Physical

With the shift to cloud and mobile technologies amplifying the nature of threats, the demand for strong authentication capabilities has never been higher. There is near-unanimous support in the security industry for increased use of multifactor authentication solutions that require a combination of two or more verification factors — something the user knows (a password or PIN code), something the user

has (a security token or mobile app) and something the user is (a biometric identifier).

Two-factor authentication, typically combining passwords with security tokens, have been required for years by financial institutions, government agencies, healthcare facilities and more. However, there is increasing support for systems that also require the third factor — biometrics.

Biometrics measure and analyze an individual's unique physical and behavioral characteristics and use this data to verify the user's identity. Physical biometric authentication can include everything from fingerprints and facial recognition to retina scanning and odor. Behavioral biometric authentication could involve voice recognition or the real-time monitoring of typing rhythm, device usage patterns, gait or gestures.

While most people associate biometrics with physical characteristics, behavioral biometric software has advanced dramatically in recent years. These tools can analyze how users pinch, zoom and swipe the screen on a mobile device, how they move a finger on a screen, how much of the tip of the finger is used, how hard they press, and how they hold the device. These behaviors are virtually impossible to replicate. When suspicious behavior is detected, a number of actions can be taken automatically. The user could be required to use another form of authentication, or an administrator could receive an alert that would necessitate a call to the user for verification.

Mainstream Applications

The rapid rise of smartphones and mobile applications have encouraged the development of more lightweight biometrics. Software developers can often add biometrics to their apps by including just a couple of lines of code. Leveraging the front-facing camera and microphone built into most handsets, applications can create voice and facial recognition capabilities even on older devices that don't offer built-in biometrics support.

MasterCard recently rolled out its "selfie pay" Identity Check solution, which uses facial biometrics for payment authentication. Using a mobile application, users simply show their face to their smartphone camera to confirm an online payment. To prevent hackers from using a static photo, the app requires users to blink. MasterCard also provides the option to choose fingerprinting for authentication.

Microsoft pushed biometrics further toward mainstream usage with the launch of Windows 10. A key feature of the operating system is Windows Hello, a biometric security platform that allows users to securely access Windows 10 devices without a password, using either facial recognition, iris scanning or fingerprints. Microsoft Edge, the new browser bundled in Windows 10, natively supports Hello and makes it possible to use biometric authentication to log into web sites. To date, there aren't many web sites that support biometric authentication, but Microsoft's strategy seems likely to encourage continued acceptance.

The need to improve authentication is driving biometrics into consumer, industrial and government systems at an increasing pace, according to the market research company Tractica. The firm forecasts that annual biometrics hardware and software revenue will grow from $2.4 billion in 2016 to $15.1 billion worldwide by 2025, representing a compound annual growth rate of 22.9 percent. During that 10-year period, Tractica anticipates that cumulative biometrics revenue will total $69.8 billion.

While passwords aren't going away any time soon, organizations need to take a hard look at their authentication tools and processes and move away from password-only data protection. With more than half of all data breaches linked to misused or stolen user credentials, it is clear that passwords no longer provide sufficient defense. Strong multifactor authentication systems that incorporate new biometric tools can significantly elevate the overall security posture and dramatically improve an organization's ability to protect its data, customers and reputation.

Keystroke Cops: Authenticating by Typing Style

In the early days of World War II, Army Signal Corps officers made a startling discovery about intercepted Nazi telegraph transmissions. Although they weren't able to understand the encrypted Morse Code messages, they were able to determine that the "dots" and "dashes" came in highly distinctive speeds and rhythms.

Using a methodology that came to be known as "The Fist of the Sender," the Allies were able to identify the unique typing style of individual enemy telegraph operators. Armed with that information, they were able to triangulate signals and trace the operators' movements across the continent — thus tracking the movement of their specific military units.

The same basic methodology — now generally referred to as "keystroke dynamics" — is now being used in biometric authentication solutions. The approach works with existing keyboards, using artificial intelligence to match two or more typing patterns consisting of "press" and "flight time" keyboard measurements.

The idea is that people type passwords so frequently it becomes an almost unconscious activity, much like a golf swing or a dance step. As a result, password typing has a nearly identical rhythm every time a person does it.

Global Industry Analysts projects the U.S. market for these solutions will reach nearly $800 billion by 2020, in part because they are easy to use and difficult to hack since typing patterns are virtually impossible to replicate.

The HP Elite x3 is the one device that's every device. It combines PC power and productivity, tablet portability, and smartphone connectivity in a sleek and secure device that can dock with your screens and keyboards when you need to work big. Crafted for business users, the HP Elite x3 is a robust device with powerful processing power and a long-life battery. Contact your ProSys representative to learn more.

PROSYS
A PIVOT COMPANY

www.prosysis.com 888-337-2626