Sigma**Uptime**

volume 16 number 5

EASY DOES IT

HP Elite x3 empowers the mobile workforce while improving device management and security.

Technology services to help you streamline operations, reduce costs and improve business processes.

Companies today must align IT strategy with their corporate objectives, strategy and business model. Pivot has created a portfolio of operating companies and partners with a focus on helping you enhance and extend the capabilities of your technology assets.

Pivot provides technology services ranging from initial needs assessment and design, through procurement and implementation, to on-going support. As an adjunct to your IT team, we provide the resources that allow your team to offload some of the day-to-day operational challenges and focus on innovations that will drive business value and competitive advantage.

Contact us to learn more.

PIVOT
TECHNOLOGY SERVICES

www.pivotts.com   888-895-0495

Contents

5

Sigma Uptime

Easy Does It

HP Elite x3 empowers the mobile workforce while boosting device management and security.

The so-called "digital transformation" is being driven by an increasingly mobile workforce using a growing array of devices to access data, services and applications from any location at any time. A September report from CCS Insight finds that U.S. employees now use, on average, about five separate devices in their efforts to maintain always-on connectivity and accessibility.

That workstyle has become difficult to support, however. Managing and securing the growing numbers of desktops, laptops, tablets, smartphones and smart watches with various operating systems from multiple vendors is a significant challenge. More than 60 percent of IT teams surveyed recently by research firm IDC say their resources are drained by device management.

Simplified management is one reason why many organizations have embraced a single-device mobility solution from HP and Microsoft. The HP Elite x3 is a three-in-one device that combines PC power and productivity with premium smartphone capabilities in a sleek form factor that also can dock with large-format monitors and keyboards for a desktop-like experience. The Windows 10

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

"New smartphones and mobile devices are being introduced into the work environment on an almost daily basis, and IT is tasked with making sure they are properly configured and compliant with the organization's technology and operational environment. It's becoming impossible to keep up," said Allan Doehler, Business Development Manager, Sigma. "By standardizing across all form factors with a single operating system and familiar Microsoft desktop applications, the Elite x3 relieves a lot of the device management burden."

Keeping it Simple

Many organizations have attempted to support multiple operating systems through the use of mobile device management (MDM) solutions. These typically are bolt-on solutions that require users to install an MDM client, which means that compliance can be hit or miss. In contrast, Windows 10 Mobile uses an OS-native MDM framework to enroll and manage HP Elite x3 devices. No separate client app is required.

The HP Elite x3 also simplifies things for users. Working with phones, tablets, laptops and desktop devices isn't always a seamless experience. Users often find their productivity is hampered because they have files and data scattered across multiple applications and devices. They also must juggle multiple phone numbers, passwords and collaboration tools.

"With the Elite x3, employees can start a task on the go and finish at their desks by docking to a desktop or laptop, which allows them to work on a larger display," said Doehler. "They don't have to save, sync or restart anything. Plus, all files and apps are stored on the Elite x3 or in the cloud — not across multiple devices — so IT only has to manage one device"

The HP Desk Dock offers a full-featured desktop environment, with a display port for external monitor support, three USB connections and wired Ethernet connectivity. The HP Mobile Extender creates a laptop-like configuration using a near-zero-bezel 12.5-inch diagonal HD display. All phone features work normally when the device is in either desktop or laptop mode.

"There's no need to disconnect to take a phone call," said Doehler. "Users can talk, text, tweet or whatever without interrupting what's happening on the big screen."

The Elite x3 also allows users to work with a variety of legacy Microsoft .NET and Win32 applications through HP Workspace, a virtualization service that essentially creates a virtual PC. It gives users access to an HP-curated catalog of x86 apps via a subscription service. This allows quick access to virtualized apps not typically available on a mobile device.

Boosting Security

The Elite x3 also improves management with enhanced device security. These features are critical at a time when mobile devices are becoming the pathway of choice for criminals seeking to infiltrate corporate networks.

In a recent survey of 4,500 business users, Ovum found that 70 percent have no device management or security functionality of any kind on their devices. It's no surprise, then, that attackers are increasingly seeking — and finding — vulnerabilities in mobile devices that can expose both business and personal data to risk.

With its March 2017 Threat Intelligence Report, Nokia reports an all-time high in mobile device malware infections and a sharp increase in compromised smartphones. The report revealed a surge of nearly 400 percent in smartphone malware attacks in 2016. Smartphones were the most-targeted devices in the second half of the year, accounting for 85 percent of all mobile device infections.

In an April report mandated by Congress, "Study on Mobile Device Security," the Department of Homeland Security concluded that threats "exist across all elements of the mobile ecosystem" and require a security approach that differs substantially from the protections developed for desktop workstations.

"Mobile devices have always required special security considerations," said Doehler. "Smartphones and tablets are increasingly being used to access essential customer and financial information from ERP, CRM and other essential backend systems. That means proprietary customer information is residing on a bunch of different devices that may not even have basic security measures in place."

With the Elite x3, HP has implemented security measures to encompass both data at rest and in transit. It features both an iris scanner and a fingerprint scanner for biometric authentication using Windows Hello. It also comes with FIPS 140-2 cryptography, 256-bit full-disk encryption, TPM 2.0, protection against firmware rollbacks and more. For additional security, all apps, passwords and files are managed and stored on the Elite x3 or in secure cloud backup — not across multiple devices.

Windows 10 Mobile also delivers "dual persona" capabilities that keep personal and business information separate and contained to prevent data leakage. This embedded feature automatically encrypts data coming from business sources and can be configured to block, log or red-flag any suspicious attempts to copy, paste, open or save encrypted data.

"The Elite x3 is a big step forward for improved device management and security," said Doehler. "It allows mobile professionals to seamlessly work with the form factor of their choice, and it allows IT to easily handle configuration and compliance tasks. That adds up to a significant productivity boost throughout the organization."

The power of a PC in the palm of your hand

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 Sigma representative to learn more.

www.sigmasol.com | 888.895.0495

BUILT-IN SECURITY
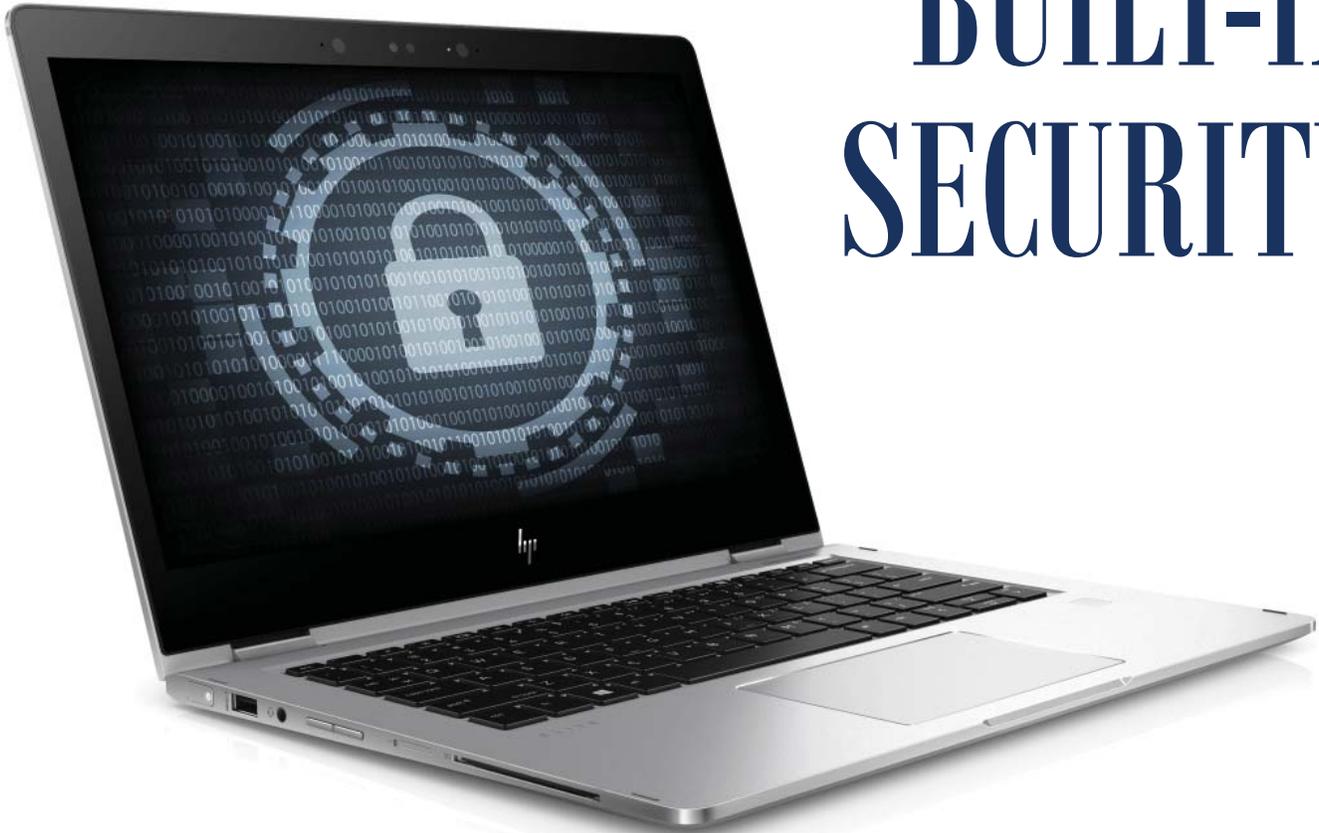
HP boosts laptop security by integrating numerous safeguards in EliteBook series.

The growing adoption of mobile computing has increased business flexibility and productivity, but mobile devices have also become attractive targets for a variety of risks such as mobile malware, noncompliant apps that leak data, Bluetooth attacks, operating system vulnerabilities and more.

Although there is increasing awareness of the need to secure mobile devices, recent surveys suggest U.S. users are overly focused on smartphone security. In fact, one survey finds that laptops may be far more valuable and vulnerable targets.

In its annual Data Breach Investigations Report, Verizon found a 132 percent increase in attacks targeting notebooks and desktops in 2016. This is particularly troubling in light of a new survey by cloud-based security firm AlertSec which finds that laptops generally contain far more sensitive material than phones and other mobile devices.

In the AlertSec survey of more than 800 U.S.-based consumers, users reported that their laptops contain sensitive work files, web browser histories, credit card and payment data, and tax information. Nearly half (46 percent) admitted they have exposed themselves to threats through behaviors such as leaving the

laptop unattended, leaving it in the car, declining security updates and attaching login information to the device.

Additionally, the survey found that most people don't know what sort of security software is installed on their laptops. More than half (55 percent) weren't even sure if they had antivirus protection.

Integrated Features

HP this year took steps to minimize risk and remove some of the security burden from users by adding built-in security features to its commercial laptops. Integrated security features in HP's EliteBook series are designed to protect not only the device, but also the user's identity and data.

HP's Sure Start Gen 3 is the world's only self-healing BIOS, automatically restoring the notebook's BIOS if it is attacked or corrupted. Runtime intrusion detection protects the critical and vulnerable BIOS firmware layer of the PC below the OS that advanced persistent cyberattacks target.

HP's new Client Security Suite combines hardened authentication such as fingerprints or PINs with soft factors such as passwords and facial recognition to boost end-user security. HP says these tools make it a million times more difficult to hack login passwords.

The HP Sure View privacy screen protects against "visual hacking," or unwanted shoulder surfing for those working in public places or open-concept offices. The world's only integrated privacy screen, HP Sure View reduces 95 percent of visibility when viewed at an angle.

Users who inadvertently leave an EliteBook up and running can lock it remotely with the HP WorkWise smartphone app, a first for enterprise PC management that protects PCs with Tamper Protection.

HP's new Sure Click technology provides hardware-enforced security for web browsers — preventing the spread of malware, ransomware and viruses. Each time a user visits a website, HP Sure Click creates a hardware-based isolated browsing session, which prevents a malicious site from infecting other tabs or the system itself.

"Mobile malware is growing in frequency and sophistication as cybercriminals look to capitalize on the mobile workforce," said Allan Doehler, Business Development Manager, Sigma. "HP understands that we can't depend entirely on end-users to implement device security. It's just too much to keep up with. HP is boosting security in the EliteBook line with built-in protections."

Security Checkup

HP provides the tools to help healthcare organizations protect sensitive data.

Given the wealth of sensitive, personal data they process and store, it's no surprise that healthcare organizations have become prime targets for cybercrime. In fact, healthcare has become the most-targeted industry in North America, accounting for more than a quarter of all publicly disclosed data breaches.

What's more, the consequences of these breaches are becoming more severe. According to the Brookings Institution, stolen patient medical records now cost organizations up to $363 per record — by far the highest among all industries.

As attacks get more sophisticated and the cost of a data breach continues to rise, security hardening across healthcare operations has become imperative. That means going beyond conventional perimeter defenses such as firewalls, access controls and intrusion detection systems. Because any smartphone, laptop or tablet is a potential entry point for attacks, endpoint security has become critical.

Printers and multifunction devices (MFDs) are often overlooked endpoints. In a recent study by Spiceworks, only 16 percent of organizations perceive these machines as being security risks, but even something as simple as an unclaimed print job can put sensitive patient data in the wrong hands.

"Like most technology in the workplace, printers and MFDs have evolved to include many new features, such as the ability to wirelessly communicate with computers and smartphones and to fax and email documents through network connections," said Allan Doehler, Business Development Manager, Sigma. "However, these features also create security vulnerabilities.

"These devices are connected to the network. If they become compromised, the entire network — and patient data connected to it — can be at risk."

Printers can become a point of entry to the organization, allowing unauthorized access to sensitive information. In addition, these devices often store data on a hard drive long after print jobs have been completed, creating another potential point for data leakage.

HP is addressing this issue with devices that offer built-in security features that help healthcare organizations reduce risk. With these features, HP builds layers of security into endpoint hardware in order to protect the device, identity, data and document.

Device Security

Like PCs, printers and MFDs all start up using Basic Input Output System (BIOS), a set of boot instructions used to load critical hardware components and initiate firmware. HP Sure Start technology works behind the scenes to validate the integrity of the BIOS when powering up. If a compromised version is discovered, the device restarts using a safe "golden copy" of its BIOS.

After a reboot occurs, HP JetAdvantage Security Manager automatically assesses and, if necessary, remediates device security settings to comply with pre-established company policies. Administrators can be notified of security events via Security Information and Event Management (SIEM) tools such as ArcSight, Splunk and SIEMonster.

Identity Security

Passwords have become the weakest link in IT security, with roughly two-thirds of all confirmed data breaches involving weak, default or stolen passwords, according to Verizon's 2016 Data Breach Investigations Report. HP is boosting security with multifactor authentication (MFA) built into its PCs.

MFA fortifies identity protection by using a combination of verification factors, such as 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 has been required in many industries for years, but there is growing support for systems requiring all three factors.

However, even devices with strong authentication systems can be vulnerable when left unattended after the user has signed in. HP's Work Wise is a smartphone app that provides protection through a cryptographically secure connection. The Work Wise app will automatically lock a PC or printer if it detects the user has moved away.

Data Security

Built-in authentication protects HP printers and MFDs from unauthorized access. HP also uses role-based access to limit the use of certain features to specific users. For example, HP Access Control allows IT to prevent users from using the email function of MFPs unless they are specifically authorized to do so.

Self-encrypting hard drives help protect data at rest, and HP also addresses data in transit with solutions such as HP Universal Print Driver, HP Access Control and HP JetAdvantage Connect. When used with Wi-Fi and network encryption protocols, these solutions protect data flowing to and from printers.

Healthcare organizations should make sure data on storage drives is made unreadable and unrecoverable before disposing of or repurposing hardware. HP Secure Erase meets various industry regulations to permanently erase data on PC and printer storage drives. HP also offers onsite data destruction and offsite recycling to erase sensitive information and help keep organizations in compliance.

Document Security

Unclaimed print jobs are one of the simplest and most common ways sensitive patient data can be exposed. Patient charts, critical lab results, treatment plans, discharge papers, and other important documents easily can be stolen when left unclaimed.

HP Access Control Secure Pull Print is a server-based software solution that can be set to require all users to authenticate at the device before the document is printed. HP JetAdvantage Secure Print provides an option for print jobs to be sent to and stored in a secure cloud queue until the user authenticates and prints the job. HP Universal Print Driver is a free print driver solution that includes a secure encrypted printing feature for sensitive documents. It allows users to send a print job to be held until they release the job via a PIN at the device.

"Hospitals, clinics and physicians' offices must build and maintain technology infrastructures that will allow them to acquire, store and analyze growing amounts of data about patient health," said Doehler. "They also are responsible for maintaining the privacy of that data. HP is providing tools to help healthcare organizations reduce risk and improve privacy."
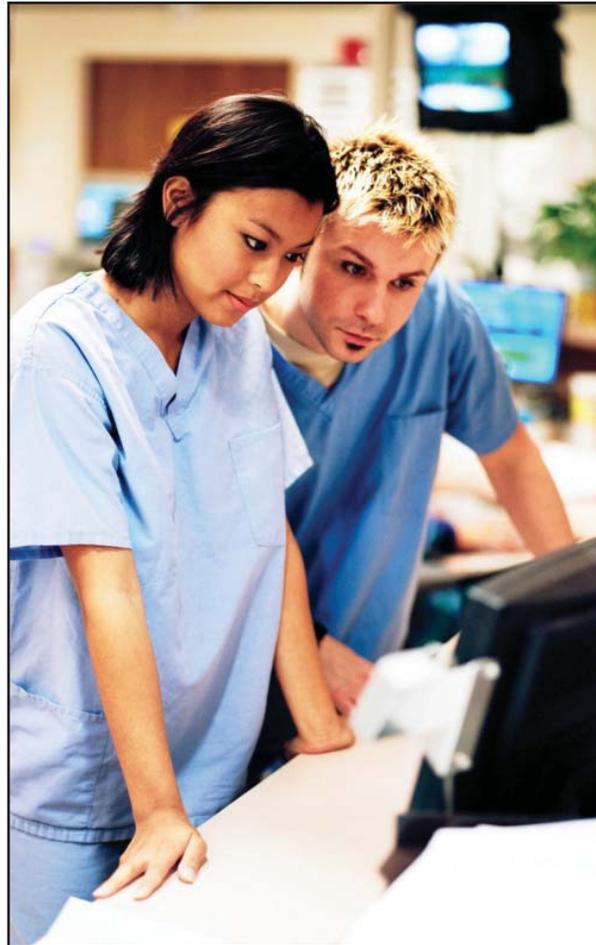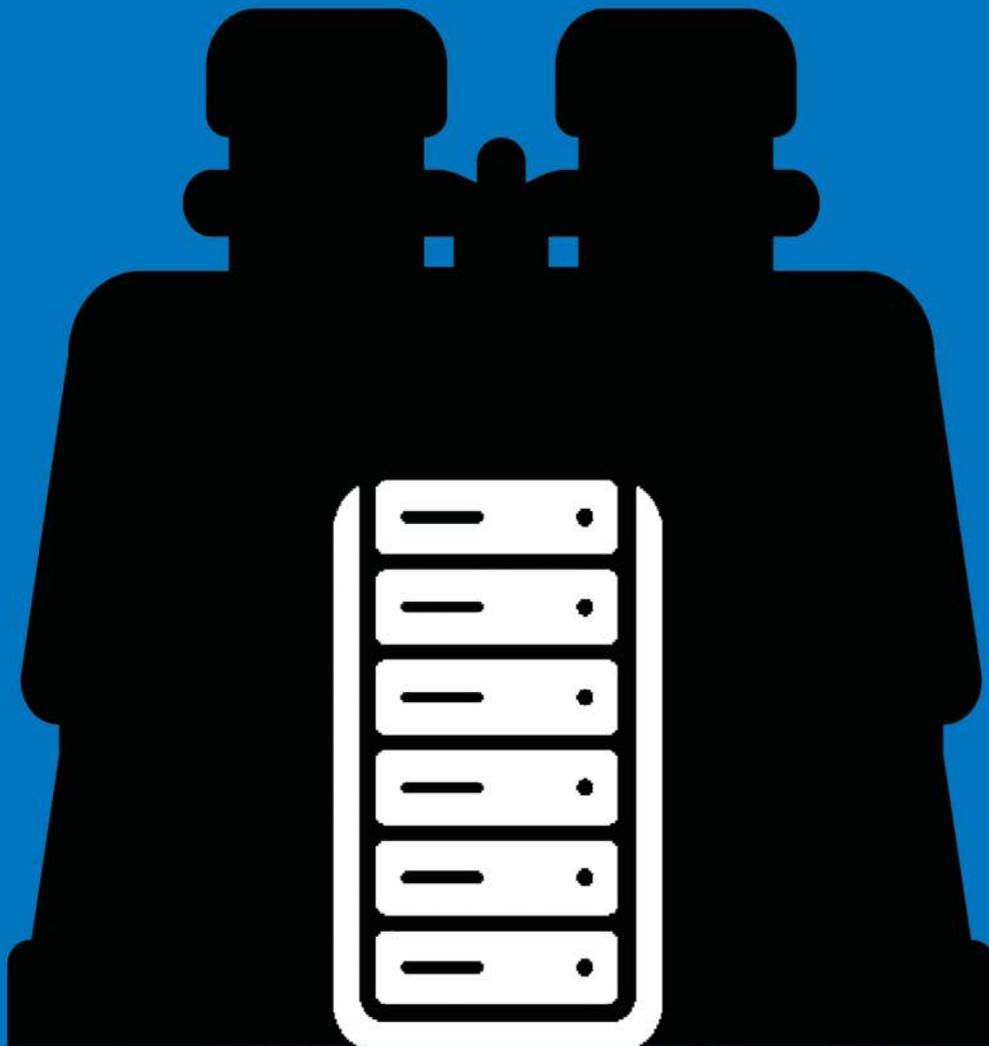
Small Wonder

New HP mini desktop computer
delivers both style and substance.

For years, tech industry analysts have heralded the imminent arrival of the "post-PC era" in which personal computers would give way to mobile devices such as smartphones, tablets and wearable devices that offered extreme portability and wireless connectivity. Although the term was coined by MIT scientist David D. Clark in 1999, it entered the popular lexicon years later when Steve Jobs began touting Apple's first iPhone and iPad devices.

Years of declining sales seemed to validate that viewpoint. Through 2016, competition from tablets and smartphones as well as lengthening lifecycles pushed PC shipments down roughly 30 percent from a peak in 2011.

However, the PC may be ready for a comeback. According to IDC analysts, the PC market saw its first quarterly sales boost in five years with 0.6 percent growth during the first quarter of 2017. Although the increase was arguably flat, it was a marked improvement over analyst expectations of a 1.8 percent decline.

Room to Grow

Because organizations have generally delayed PC replacements, IDC expects an impending replacement cycle will spark continued growth. By some accounts, more than 100 million commercial desktops still in use are greater than four years old, leaving businesses vulnerable to a range of cyberattacks targeting endpoint devices. These older machines also lack the performance and energy savings of today's devices.

Still, HP is betting that today's workforce is looking for something other than yesterday's oversized PC boxes that consume lots of valuable desk space. That's why the company recently introduced a small, sleek general-purpose machine as part of its 2017 lineup of commercial desktops and all-in-one (AiO) machines. Roughly the size of a standard cable modem or home network switch, the HP EliteDesk 800 G3 Desktop Mini nonetheless is a powerful, business-class computer.

The 800 G3 is powered by the 7th Generation Intel Core i5 processor in either 35W or 65W versions. The quad-core processor has 8MB of cache and 3.8GHz speed — sufficient processor power for multitasking with most business apps. The Mini G3 comes with 8GB of DDR4 memory installed, but can upgrade to 32GB. Optane, Intel's new class of hyper-fast memory modules, is an optional upgrade. The Windows 10 Pro 64-bit Edition operating system is standard.

Big Features

Security technologies included with the machines include HP's Sure Start Gen3 BIOS monitoring tool and Client Security Suite Gen 3 for hardware multifactor authentication. Managing the Elite line is made easier with HP's Manageability Integration Kit, which helps IT administrators more easily create recovery images and monitor security.

Alex Cho, VP and general manager of HP's commercial PC division, says the Mini G3 fits with the company's vision of providing desktop computing that offers both style and substance.

"The millennial workforce is clamoring for stylish devices that inspire creativity and an open exchange of ideas, and employers are demanding technology that looks beautiful in their open floor plans yet are powerful and secure with no barriers to their employees' productivity," said Cho. "The newest lineup of Elite desktops and AiOs reflects the vision of a business while reflecting the desires of employees, pairing beautiful designs with exciting features and performance that meet and exceed security requirements critical to all business environments."