HP FEDERAL

The importance of endpoint security by design

Delivering highly secure endpoints hinges on innovation and a holistic approach to supply chain decisions

Matt Barry
HP Federal

Endpoints can be vectors for bad actors to insert themselves into a company's network, which means endpoint security is a critical component of efforts to protect government and contractor systems. And it has long been a particular focus of HP's product development.

We think deeply about security by design right from the outset and take an integrated approach to how we source components and create products. When we design more secure solutions upfront, that security carries through the entire life cycle.

Furthermore, endpoints are intelligent devices. They have IP addresses, so as soon as they are powered up, they become part of a potential attack surface. To address such risks, HP has innovated for years at distinct levels — below the operating system, in the operating system and above the operating system.

> "Endpoints are intelligent devices. They have IP addresses, so as soon as they are powered up, they become part of a potential attack surface."

Enhancing resilience and minimizing downtime

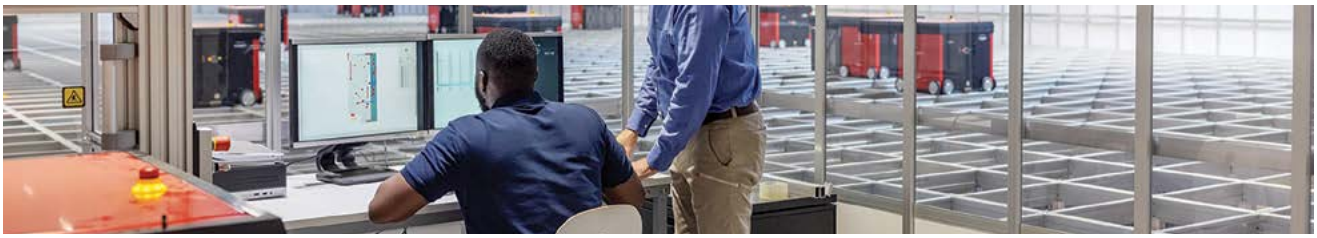
So much of our innovation in cyber-physical security revolves around managing risks in endpoints with confidence. We help our customers minimize their attack surface and strengthen their overall security posture. For example, each time a user powers up his or her device, HP Wolf Security compares the device's firmware to a copy on an embedded security controller chip. If malware changes the firmware, the security tool will recognize it and revert to the gold-standard version.

HP Sure Admin provides modern security for PC firmware configuration management by enabling remote administrators to securely manage BIOS settings. It also enables field support personnel to obtain secure in-person access to BIOS setup. Use of digital certificates and public-key cryptography eliminates the risks associated with legacy password-based approaches by using QR codes that return a one-time password when scanned by the Sure Admin phone app.

These tools ensure that our customers' resilience is significantly enhanced and downtime is minimized in the event of an attack.

Partnering with the government to advance cybersecurity

HP has acquired companies over the years to provide our customers with holistic solutions and integrations to enhance the end-user and IT experience. One of my personal favorites is our acquisition of a company called Bromium. We've fully integrated and further developed the solution and call it Sure



iStock

Click Enterprise. We use it every single day at HP. If I come across something malicious when I open an attachment or visit a website, it would ordinarily infect my device. But with Sure Click Enterprise, my activities run in a micro virtual machine so that my device still operates cleanly after I exit the session. That technology has prevented billions of attack vectors from infecting machines in our environment and our customers' environments. And this software works in any Windows 10/11 environment, not just on HP hardware.

HP helps companies strengthen their risk and compliance programs by taking a zero trust approach to developing our hardware and by aligning with the Cybersecurity and Infrastructure Security Agency's and the National Institute of Standards and Technology's (NIST) guidelines. We also partner with the government to advance its cybersecurity programs and certifications. HP has been an industry editor with NIST on a number of special publications focused on cybersecurity. Firmware resilience is one example. The Cybersecurity Maturity Model Certification (CMMC) program is an important development in safeguarding the defense industrial base and, by extension, our nation's cybersecurity, and HP has been a strong advocate of the program from the early days.

CMMC has gone through multiple iterations over the years, and I am confident that when the formal rule is fully deployed, defense contractors will step up to the challenge of protecting their networks from attackers. With the provisional CMMC rule published in late December, the time to act is now. ■

Matt Barry is chief operating officer at HP Federal.