Without modern protections, every device is an open door inviting a security breach. But there’s a way to turn these potential vulnerabilities into a protective barrier.

The first step is to upgrade your operating system. Many enterprises are already doing this. Security is certainly one of the reasons that corporate migration to Windows® 10 will be the fastest adoption of Windows in Microsoft’s history, according to Gartner. As Windows evolves as a service model, new hardware becomes even more important for keeping pace with the frequency of new features and critical updates to the operating system.

Software alone only provides one-dimensional protection when facing modern security threats. To tackle cybersecurity proactively, new hardware is essential to strengthening software.

“Hackers are phishing and hunting for zero-day exploits, so businesses better invest in new hardware that helps ensure security from the core to the application layer,” said Sumera Baker, a security consultant and the author of a recent white paper on the role of software and hardware in defending against modern cyberthreats. “Security can’t just be in applications, security tools, and perimeter firewalls; it has to be embedded in the hardware too.”

This level of security is what you find when new security features in Windows 10 are paired with hardware-based enhancements in new 7th Gen Intel® Core™ vPro™ processor-based devices.

Consider this. Verizon’s® 2017 Data Breaches Investigations Report found that 80 percent of hacking-related security breaches used stolen or guessed passwords. New 7th Gen Intel® Core™ vPro™ processor-based devices offer superior identity protection to strengthen Windows 10. Windows Credential Guard uses Intel® Virtualization Technology to sequester credential keys in containers, far from the eyes of hackers. When a device is first turned on, Intel® BIOS Guard and Intel® Boot Guard help the Unified Extensible Firmware Interface for Secure Boot make sure there are no threats present before the operating system launches.

Hackers are relentless. They go after easy targets and in most cases that means credentials. Modern biometric-supported devices can add a strong layer of protection. But you need the latest hardware to benefit from the full potential of technologies like high-fidelity fingerprint reading and infrared webcams, which make facial recognition more precise by blocking background lighting.
There's an additional benefit to biometric factors replacing passwords: IT tickets for password resets drop, saving IT an average cost of $70 per ticket, according to one study from 2014\(^4\).

The combined strength of Microsoft software and Intel-based hardware lets employees enjoy all the productivity benefits of Windows 10 along with security from new 7th Gen Intel® Core™ vPro™ processor-based devices.

Rather than see endpoint security as a porous border, IT specialists can turn devices into a barrier against today's threats. The key is having modern software with up-to-date, security-enhanced hardware.