Microsoft Surface

Safer together: How Surface can help keep your organization safe from cyberthreats

In 2019, Capital One bank reported a massive data breach of 106 million credit card applications from its customers. The victims' personal information, such as names, addresses, phone numbers, and dates of birth, were all compromised, along with 140,000 Social Security numbers and 80,000 bank account numbers. It was one of the biggest breaches of a major financial institution in history. The crime was allegedly carried out by a single hacker.

It's not just banks that are susceptible. In 2014, a hacktivist carried out a massive distributed denial-of-service (DDoS) attack on Boston Children's Hospital and a local nonprofit. Both systems were brought to a standstill for more than a week and cost the healthcare facilities hundreds of thousands of dollars. The event drove the point home that no organization is safe, regardless of its altruism or service to society.

In today's digitally driven world, data breaches, hacktivism, and cyberthreats are commonplace. Microsoft Surface has studied the particular needs of government organizations when it comes to security and compliance. Surface now offers features that make it easy for government organizations to adhere to the highest security standards and be in compliance at all times.

Fighting fire with firewalls

The right technology can help keep your organization safe. Windows 10 is well known to be a highly secure operating system, and Office 365 applications allow government workers to share documents and data more securely. But should your security considerations extend beyond firewalls and security applications to the hardware itself? The answer is yes. Even if just one chip in a device is compromised, it could undermine the rest of the security measures in place.

Surface devices can be managed and updated at the Unified Extensible Firmware Interface (UEFI) level, allowing organizations to efficiently mitigate endpoint vulnerabilities. Surface devices were designed from chip to cloud to work with Windows 10 security measures, and they feature device encryption to further secure data.

> **“We’re proud that Surface incorporates technology and features to make the devices safer for federal organizations. This is especially important in today’s environment, where working remotely is the norm.”**
>
> Dylan Evers, Microsoft Surface Team Lead, US Federal at Microsoft

Surface devices feature five elements that help ensure outstanding security:

Highly secure hardware. Surface security features include an antimalware solution, so your organization will have access to the newest Microsoft Teams and Office 365 security features on their Surface devices as soon as they are rolled out.

Encrypted software. When employees use Teams or Office 365 on their Surface devices, they experience end-to-end encryption. This means that even if hackers are able to steal transmitted data, they won’t be able to read it immediately. As a result, attackers become frustrated and therefore more likely to move on to another user with a less secure device. All Surface devices feature a Trusted Platform Module (TPM) that makes it fast and easy to encrypt your disk.

Automatic software updates. Surface comes with Office 365 software, which continually updates firmware, providing improvements in security, stability, and performance. This helps ensure that you always have the latest security patch for the software.

“Alternatively, agencies can use Windows Hello for Business to provide another layer of security to user names and passwords,” said Charlie Bolen, Surface Customer Success Manager & Architect, US Federal at Microsoft.

Remote device management. The Surface Enterprise Management Mode tool (SEMM) allows you to remotely secure and manage firmware settings within your organization. IT professionals can remotely control firmware elements, such as microphones, speakers, LTE, cameras, Wi-Fi, and Bluetooth. Remote device management can be applied to preventative action, such as turning off webcams within secure facilities. With SEMM, you don’t have to manually manipulate cameras and audio devices; instead, you can use the tool to create the desired outcome. Device Firmware Configuration Interface (DFCI) also enables IT managers to manage Unified Extensible Firmware Interface (UEFI) via Endpoint Manager for streamlined remote management.

LTE network capabilities. When employees work outside the office, there is concern that they will connect to public, unsecured Wi-Fi networks at different locations. Most Surface devices allow remote workers to connect to an LTE network tower—and enjoy highly secure access to the internet.

A highly secure solution is a complete solution

With Surface, you can ensure that you’re doing everything in your power to better protect your agency from the ever-changing threat of hacktivism, cyberthreats, and data breaches. Using a Surface device helps ensure you’re getting great performance from the security measures of Microsoft 365 and Windows 10.

“We are all in this together,” Bolen said. “Working closely with the right technological tools can make all the difference in helping keep your data and systems safe from compromise.”

To learn more, please reach out to your Microsoft Certified Partner.