CYBERSECURITY IN THE HYBRID WORKSPACE

As state and local governments incorporate remote and hybrid work scenarios into their permanent plans for the workforce, they are taking a fresh look at cybersecurity. This includes the prevalence of malware and other attacks that target end users' computing devices. To protect intellectual property, operational continuity and personally identifiable information (PII), and prevent downtime created by network intrusions, organizations should incorporate the following tactics into their device procurement strategies.

Choose endpoint devices with built-in protection.

Systems designed with security functions as the primary design criteria make security more seamless for users and less complex to maintain. For example, modern enterprise printers can automatically detect and self-heal from malware without interrupting printing operations. Laptops and workstations can automatically isolate and contain emails, websites or files from untrusted sources using micro-virtualization or segmentation techniques. When a user clicks on an untrusted browser link, the content is brought up in multiple virtual machines. When the user closes the link, the virtual machine disappears along with any malware. The entire process happens behind the scenes without impacting performance or the user experience. The real advantage is that no matter how much an enterprise trains its employees, someone will still click a harmful link. This design mitigates any negative effects from doing so.

Incorporate Zero Trust mechanisms at the hardware level.

Despite strong network defenses, bad actors can still infiltrate the network via software vulnerabilities, stolen passwords, malicious insiders and other threat vectors. A Zero Trust Architecture helps prevent malware infections and other attacks by limiting what a user can do once they have accessed a device. Zero Trust tactics at the hardware level include analyzing user behavior and context for indications of abuse, using cryptographic functions to detect and prevent tampering with the device's core processes, and implementing isolation and containment. Isolation can be used not only to keep malware out but also to protect high-value applications in a secure virtual container that can't be touched by any other process on the computer. Zero Trust is as much a design philosophy as an Identity Management scheme.

Work with a proven vendor.

Every procurement decision is a security decision. Industry-leading vendors have the expertise and resources to thoroughly vet the origin and integrity of device components; hire the best talent; and conduct the research, innovation and testing required to produce the most secure, highest-quality products.

To learn more about strengthening your security posture in remote and hybrid work environments, visit https://www.hp.com/us-en/solutions/government-it-solutions.html

HP creates new possibilities for technology to have a meaningful impact on people, businesses, governments and society. With the broadest technology portfolio spanning printing, personal systems, software, services and IT infrastructure, HP delivers solutions for customers' most complex challenges in every region of the world. More information about HP (NYSE: HPQ) is available at **www.hp.com**