Why is endpoint security so complicated?

- Expanding list of devices connecting to the network
- Increase in BYOD programs, desk sharing and mobile/remote workforces
- Employee non-compliance with data protection policies
- 52% of organizations report budget constraints as the biggest challenge related to implementing and deploying a physical device security policy for portable devices
- By the end of the year, 90% of businesses will utilize some form of 2-factor authentication (2FA) that includes biometrics
- Less than 3% of employees use privacy screens while on the road or out of the office and only 9% of organizations require full compliance with company security policies

What are the best practices?

- Deploy Physical Device Security for ALL Portable Devices
- Utilize Simple Solutions for End-Users
- Implement 2nd-Factor or Multi-Factor Authentication
- Train, Track, Certify and Enforce Compliance
- Seek Additional Cost-Effective Ways to Protect Data (like shredders!)

What are these security gaps costing us?

- Non-compliance with GDPR, CCPA, HIPAA, PCI-DSS and other regulations have cost companies more than $1.45 billion over the last eight years

How did we get here?

- Roughly 200 billion connected devices, yet nearly 15% of organizations do not use any form of endpoint security

Download Kensington's White Paper for More Details: Identifying the Gaps in Your Data Protection Plan