The New Frontier: Mobile Anti-Malware Protection

Viruses and malware
= Ubiquitous threat

- → Viruses & malware spread effectively because they are ubiquitous to computing

- → Malware relies on users taking few, if any, actions, and even those few actions are part of normal computer usage

Anti-virus and anti-malware
= Ubiquitous solution

- → Anti-virus software mitigates virus spread because it is ubiquitous

- → AV typically fails when it requires user action—e.g., renewing, installing or updating the software

- → Only ubiquitous solutions work

Everything old is new again—viruses ride the next generation of removable storage

- 1st decade of viruses spread by people exchanging games and pirated software via floppy disks
- Viruses did not spread quickly, but spread globally
- Mechanism was relatively simple
- Payloads were highly malicious
- Today, conventional USB flash drives = malware vector of choice
  - nearly 1 in 10 malware programs use AutoRun

Perceiving the real **malware threat**

21%

YES

disable endpoint security software up from 17% in 2007

–Ponemon Institute 2009

→ Viruses perceived as fast-spreading programs

- travel via e-mail or malicious compromised websites

→ Worms perceived to spread over Internet in hours

→ Users perceive unknown flash drives as safe

USB flash drives now ubiquitous
= New malware threat vector

Conventional USB devices bypass malware prevention, resulting in:

- → Significant incidents already
- → Drives pre-infected or infected with Internet updates
- → Spread automatically via AutoRun
- → Steal sensitive data and identities
- → Compromise networks

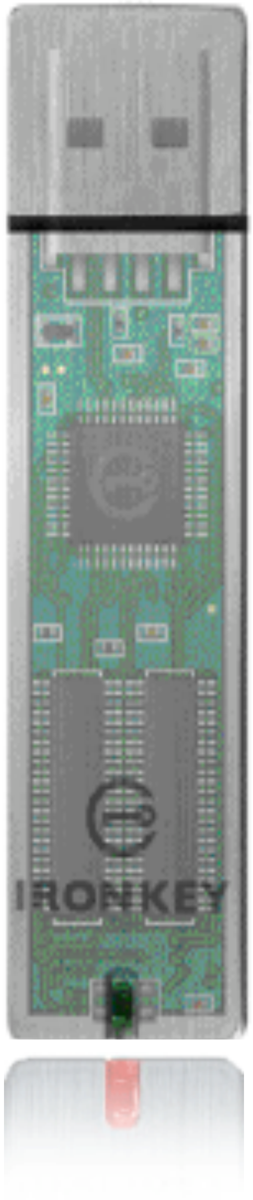
Ubiquitous protection to thwart a ubiquitous threat

→ Proactive defenses constantly protect IronKey devices from attack

→ Ubiquitous protection—no user action is required

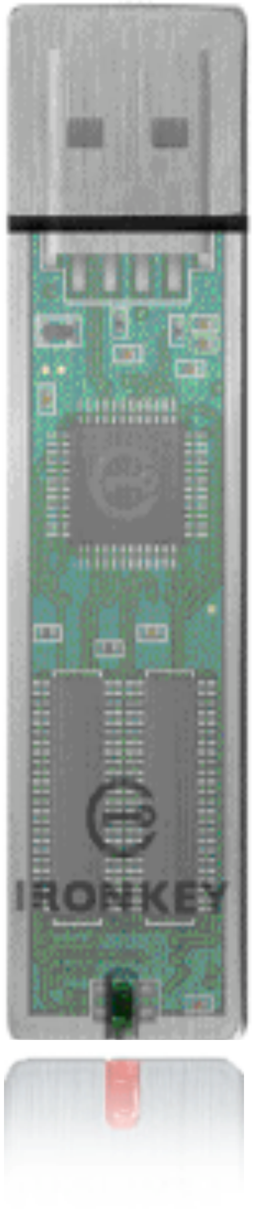
→ Transparent protection

- users neither impacted nor aware of protection



Trusting your hardware— **start** from a **secure** baseline:

- → Secure manufacturing processes
- → Trusted supply chain
- → Malware-protected software and digitally signed firmware updates
- → Secure provisioning and quality assurance processes
- → Always-on hardware encryption



Trusting your hardware—
stay secure with:

- → Keylogger prevention
- → AutoRun protection
- → Read-Only mode
- → Anti-virus scanning
- → Remote management & security updates
- → Policies that can restrict usage to trusted networks

Self-defending hardware

- → Self-defending devices return ubiquitous security (and control) to organizations—with ubiquitous protection
  - ✓ no user action is required

- → Users are neither impacted nor aware of protection
- → Allows users to enjoy the convenience—and organizations to enjoy the productivity benefits—of USB drives while minimizing malware risk

The New Frontier:
Mobile Anti-Malware Protection

For more information

John Jefferies
VP Marketing
mailto:JJ@ironkey.com

→ Office: 650.210.2255

IRONKEY™