Print security services —comparing HP and Xerox

Service Level
Managing Print Security across all levels

HP	Xerox
Print Security Advisory Services: • Certified consultants learn customer's current security policies and procedures • Security Workshops to educate on threats • HPSM demo • Risk Assessment • Risk Report and gather feedback • Retainer Service provides follow-up and continued guidance • Strategy Focus vs. Implementation Focus	**Print Security Auditing Service:** • Certified Consultants work with customers to define baseline policy which is pushed using Device Manager implementation • Ongoing reporting on non-compliant devices • No workshops/or follow-up • No Risk Assessment beyond Device Manager Reports • No Auto Remediation available through solutions • Implementation Focus vs. Strategy Focus

Network Integration Level
Protection for devices at the network level, identification of devices on the network

HP	Xerox
• Lacking Cisco integration* • IPSec • 802.1x • Network port management • IP/MAC access lists • Connection Inspector—Network Behavior Anomaly Detection	• Cisco TrustSec* – identifies devices on the network leveraging certificates • IPSec • 802.1x • Network port management • IP / MAC access lists • Lacks capabilities of Network Behavior Anomaly Detection

Fleet Level
Protection for multiple devices

HP	Xerox
• HP JetAdvantage Security Manager • Security Policy Creation • Instant On • Auto Remediation • Certificate Management • HP JetAdvantage WebJet Admin • Fleet Management Too—can push out device settings	• ePO integration—minimal insight into device security, no policies, auto remediation, or certificate management • Device Manager—MPS only fleet management tool. Can push out settings and provide reporting on compliance, no auto remediation or certificate management

Device Level
Protection of individual devices

HP	Xerox
Big 3: • Sure Start BIOS Protection & Self Healing • Whitelisting (Firmware/Solutions validation) • Run-Time Memory Inspection (Intrusion Detection and Self Healing) • Trusted Platform Module (TPM)	**McAfee integration:** • No BIOS Protection • Whitelisting (Firmware/Solutions validation) • Integrity Control (System file protection and monitoring) • No Run-Time Memory Inspection • No Self-Healing • No TPM

* Dependent on Customer leveraging Cisco TrustSec technology. HP has not seen enough customer demand to broadly adopt this approach.

4AA7-1353ENUS, Rev. 2, February 2018