Protect your printer.
Protect your business.

Comparing Kyocera and HP

Kyocera's website[1] (https://www.kyoceradocumentsolutions.com/security), under the header "Approach to security for MFP's and printers" describes their current offer as "Kyocera continues to enhance information security to protect our customers' information assets."

Positioning their business: "Kyocera's first priority is to securely protect the customer's information assets. We are taking necessary actions on numerous security measures to protect the customer's information assets against threats that are increasingly sophisticated and diverse. While constantly working to enhance the usability of the Kyocera MFPs and printers, Kyocera is simultaneously striving to maintain and improve the high levels of security on the Kyocera MFPs and printers, corresponding to each customer's working environment."

Kyocera security claims

According to the Kyocera website[1], "Kyocera is putting a strong and focused effort into developing security functions that will provide more security when using Kyocera MFPs and printers. We are also developing MFPs that comply with the Common Criteria international security standard (ISO/IEC 15408) so that customers will be able to use our products with ease. Kyocera products will be certified under IEEE 2600.1, which is an international security standard for hard copy devices enacted in 2009. In addition, the Federal Information Processing Standard, FIPS 140-2 certified hard drive is available for some Kyocera device models for sensitive data protection. Kyocera will continuously drive further improvements in security enhancement as standards develop or new technologies evolve to protect the Kyocera devices."

"Information Security protects printed documents, address books, and the like, against information leaks, data alteration, denial of service attacks, and other such threats while maintaining the three security attributes:

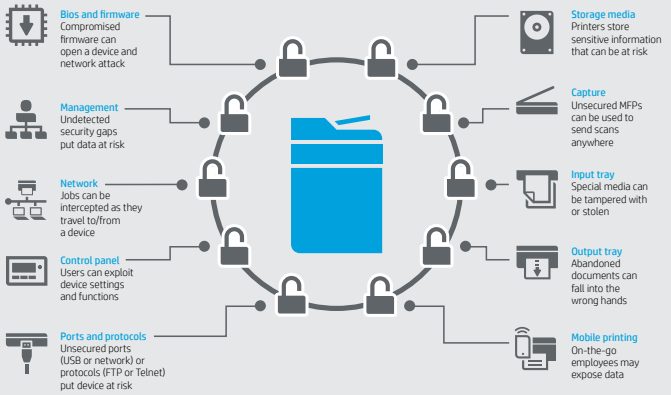
1. Confidentiality = access
2. Integrity = accurate
3. Availability = accessible

Kyocera develops MFPs and printers while having awareness of the three security attributes (CIA) in order for customers to securely use the Kyocera products."

HP Security Ecosystem

HP security:
Although many IT departments rigorously apply security measures to individual computers and the business network, printing, and imaging devices are often overlooked and left exposed. HP has taken the lead in print security by being the first and only company to deliver devices featuring "self-healing" and "real-time memory scanning and intrusion detection."

Device security is the true differentiator when contrasting HP and Kyocera MFPs and printers. HP devices are able to protect all the way down to the BIOS and firmware from attack and malware while keeping the device operational.



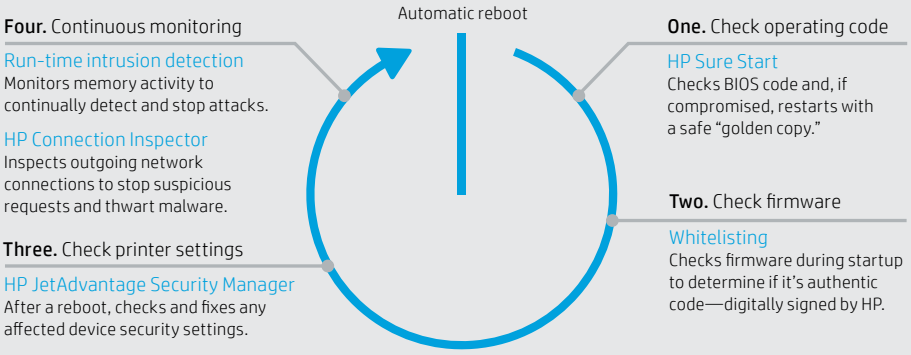
Self-healing HP Print Security—HP vs. Kyocera

Finding the HP advantages when comparing Kyocera against the four primary steps embedded in the HP MFP operating cycle.

How does it work?
The embedded security features address four primary steps in the cycle of an HP device.

If attacked, only HP Enterprise devices can reboot and self-heal.

HP JetAdvantage Security Manager completes the check cycle.



Kyocera device detection—features and claims vs. HP

Kyocera at the device
According to Kyocera's documentation, Kyocera relies purely on industry standards like code signing, hard drive encryption, closing of ports, and authentication for its security and device protection.

HP analysis
This is NOT new technology. Kyocera lacks the advanced security features that HP offers with HP SureStart, Whitelisting, Run-Time Memory Intrusion Detection, or TPM technology.

HP Secure Boot Process
The following items are aspects of a Secure Boot Process that should be included in leading security capabilities:

- At startup, the device must validate the integrity of the BIOS.
- The HP device will "self-heal" an infected BIOS by replacing it with a hardware protected "golden copy" of the BIOS.
- The HP device notifies the administrator via standard event mechanisms, including SIEM systems, of any issues.
- The HP device recovers to a known good state after detecting an infected BIOS and replacing it with the "golden copy".

HP response and benefits
Being able to detect and stop threats is key in printer security—and so is the ability for printers to automatically repair themselves from attack—in order to maximize uptime while minimizing IT interventions.

With HP's SureStart, the BIOS code integrity is validated. If the BIOS is compromised, the HP MFP reboots the device and loads a safe "golden copy" that is digitally signed by HP.

HP supports on-device Intrusion Detection which continuously monitors memory for malicious malware. Kyrocera makes no claim to memory scanning for injection attacks. Kyrocera can only detect the load of malicious firmware (aka whitelisting).

In addition, HP Connection Inspector works to stop malware from "calling home" to malicious servers, stealing data, and compromising your network. HP Connection Inspector evaluates outgoing network connections to determine what's normal, stop suspicious requests, and automatically trigger a self-healing reboot.

Kyocera document and data protection claims

Document protection
Kyocera relies primarily on 3rd-party partnerships to provide Print Management and Pull Print solutions.

Kyocera provides embedded and on-premise server data Loss Prevention solutions to better control and track print/copy/scan and fax workflows.

Data protection
Industry standards like:

- HDD Encryption—optional
- Closing of physical and network ports
- Device Certificates/SSL/TLS

New embedded security: HP Connection Inspector

The latest HP security differentiator stops malware from calling home.

- Monitors outbound network connections (packets)
- Learns what's normal, then inspects and stops suspicious packets
- Triggers a reboot to initiate self-healing procedures without IT intervention
- Creates security events that can be integrated with a SIEM tool like Splunk
- No competitor offers these features

HP analysis
HP provides a much more robust solutions offering with HP Access Control (HPAC), HP Capture and Route (HPCR) along with cloud based offerings like HP JetAdvantage Secure Print and HP JetAdvantage Private Print.

HP also partners with 3rd-party providers like SafeCom and PaperCut to broaden our Print Management offering.

In 2017, HP added Data Loss Prevention capabilities to HPAC and HPCR to extend security to the physical document.

HP response

Document protection:
- HP Access Control Secure Pull Printing
- HP JetAdvantage Secure Print
- HP JetAdvantage Private Print
- Locking input trays
- Counterfeit deterrent solutions
- Anti-fraud features

Data protection:
- Utilize 802.1x or IPsec
- HP AES256 encryption
- FIPS 140
- Protocol over TLS (IPPS)
- HP Trusted Platform Module (TPM)
- Certificates
- HP JetAdvantage Security Manager
- Native authentication (PIN, LDAP, or Kerberos)
- Active Directory
- Proximity cards
- HP Access Control Secure Authentication
- HP Access Control Rights Management
- HP Access Control Job Accounting

HP pull printing solutions help organizations meet confidential printing needs and reduce print costs. Each business is unique—and some are subject to regulatory or privacy requirements that mandate where a print job is held. That's why HP offers several pull printing solutions: cloud-based, on premise, and hybrid.

Protect sensitive documents from packet sniffing, with end-to-end encryption that safeguards your company's most valuable information—in transit and at rest. Notable to the industry is that HP provides additional protection with comprehensive security on the device from startup to shutdown with self-healing to minimize business disruption backed by solid enterprise solutions.

Kyocera explains their security approach through a product development lifecycle

Kyocera implements appropriate security countermeasures with respect to the different phases in the product development lifecycle of planning, development, evaluation, production, and sales.

Planning phase:
We continuously check for the newest security trends and vulnerability information. We extract and analyze security requirements based on customer's security requests so that we will be able to incorporate them in our new models and solve any issues in an early stage.

Development phase:
We develop security functions for customers to use Kyocera products in a more secure way. We strictly check potential vulnerabilities to ensure we do not embed these known items.

Evaluation phase:
Our products are not only passed through internal evaluation, but also through objective security evaluations by 3rd-party laboratories.

Production phase:
We establish a secure environment and ensure secure production by strictly following an operation process manual that enables us to perform precise operations.

HP analysis

Upon reviewing Kyocera's security approach, the impression is that they are customizing much of their solution implementation on available products as well as those in future production cycles.

Furthermore, Kyocera has pointed out their methodology for development of security functions as being proactive in nature.

Even after sales, we strive to respond promptly to any security concerns from the market (Figure 2)

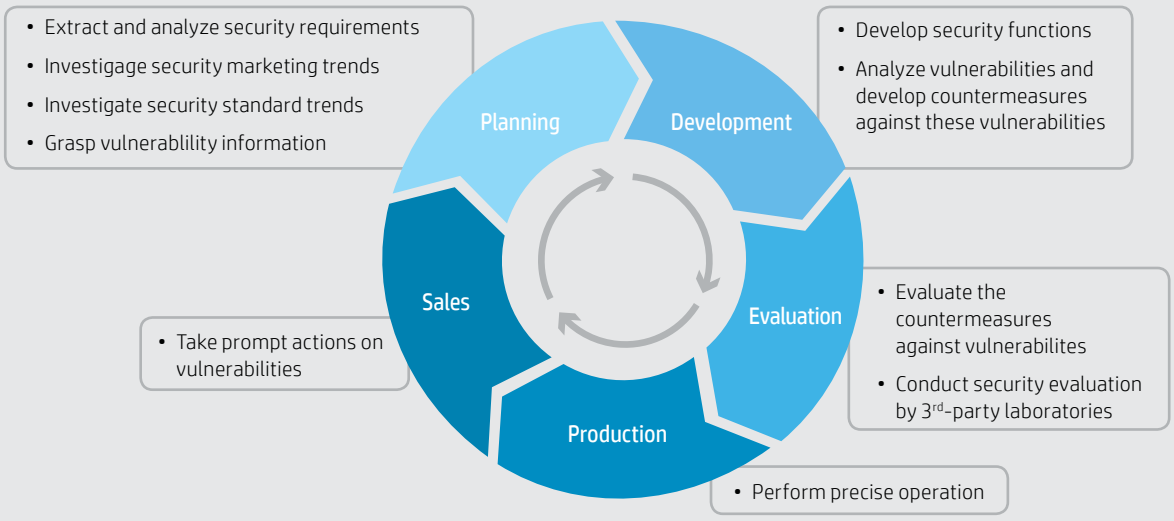


Figure 2: Product development lifecycle security

However, Kyocera does not say they are leading in the market with any security features.

After analyzing the Kyocera security documentation, there are clear differentiators in HP's offering compared to Kyocera.

HP response

HP provides the same level of security review and evaluation to our product development lifecycle.

Though Kyocera claims a proactive stance to security development, they have not made major advancements to their device security offering in quite some time. Likewise, while Kyocera has explained how they may be developing future security features, this process may not yield any market-leading security functions and features.

Assessment tools

How secure are your printers? Assess the security of your print environment with these helpful HP online tools:

- **HP Secure Print Analysis survey**—online self-assessment to determine if you are following best practices in print security: hp.com/go/SPA
- **HP Quick Assess**—free technical evaluation of top 13 settings on up to 20 HP printers (phone consultation available in U.S.): hp.com/go/quickassess
- **Learn more** about HP's embedded security features by watching the Printer Security Features video.

1 As noted by Kyocera, October 2017: https://www.kyoceradocumentsolutions.com/security

4AA7-2060ENA, Rev. 1, January 2018