Print Guardian

Print security with teeth.

Make Print Guardian your print estate's watchdog, catching threats, detecting intruders and securing the weakest link in your cyber defence.

Stop leaving the gates open.

+ Printers and MFPs aren't just office equipment, they're unmanaged PCs with operating systems, inside the fence.
+ They often run outdated firmware and open ports and communicate freely across networks. Yet they're often treated like office décor rather than network endpoints.

That's where we come in.

+ A fully managed printer security platform deployed within your network.
+ Risk findings, alerts, and enriched telemetry are securely forwarded into established SIEM, SOC, and SOAR environments for centralised response.
+ 24/7 monitoring and support delivered from our UK-based SOC in Reading. We utilise AI hyper-automation managed by our on-site security experts.

KYOCERA

Your print estate is your vulnerability*

68% of organisations have experienced data losses due to unsecure printing practices.

62% of IT decision makers acknowledge their print infrastructure is vulnerable to cyber attacks.

30% have suffered data breaches due to insecure print devices in the past year.

PrintGuardian leaves nothing in between.

Source: Northants Chamber

How it works...

1. Deploy
PrintGuardian is packaged as a VM or black-box appliance within your network.

2. Collect
PrintGuardian collects logs from Kyocera printers and MFPs across the organisation and pushes the data into our managed SOC.

3. Monitor
PrintGuardian continuously scans the device for known software vulnerabilities, identifies anomalies, and detects suspicious activity.

4. Report & Integrate
Risk findings, alerts, and enriched telemetry are securely forwarded into Kyocera's AI hyper-automated SOC for a centralised response.

PrintGuardian.com

Why it matters?

Hackers look for gaps. PrintGuardian closes them.

In 2023, attackers actively exploited critical vulnerabilities in print management servers used by enterprises, healthcare providers, schools, and government organisations worldwide. The flaw allowed remote code execution without authentication and was linked to ransomware activity.

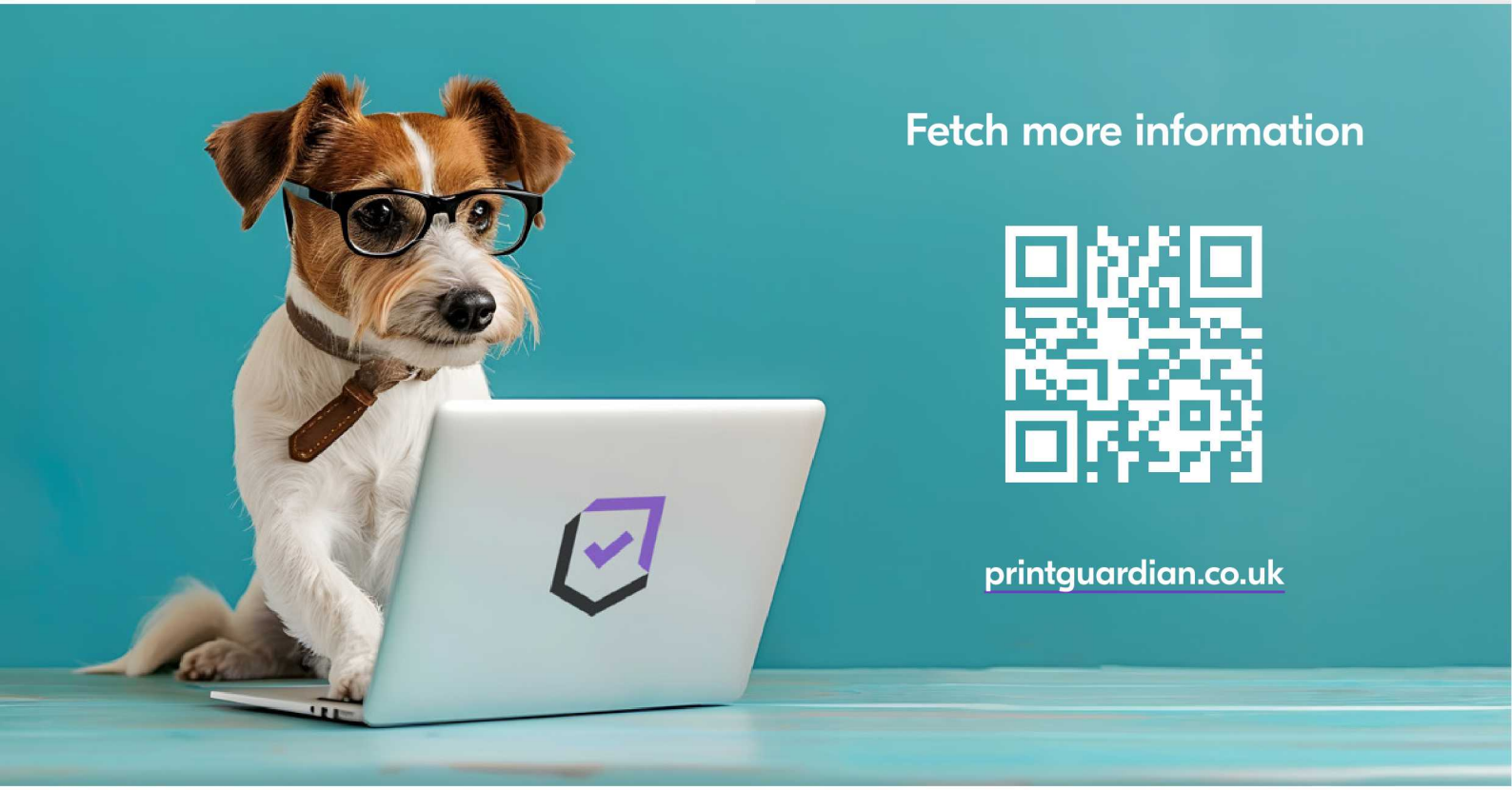
Source: TechCrunch - Vulnerability Report

How Attackers Exploit.

+ Intercept sensitive print jobs containing financial records, contracts, HR files, or customer data.
+ Capture stored credentials used for scan-to-email or directory integrations.
+ Move laterally across the network to access additional systems and servers.
+ Install persistent malware or backdoors that remain undetected for long periods.
+ Use the printer as a trusted internal device to bypass traditional endpoint controls.

What you gain

- UK based cyber expertise
- Reduced attack surface
- Centralised print visibility
- Faster incident response
- Continuous monitoring
- Compliance-ready reporting



Fetch more information

printguardian.co.uk

Get in touch:

printguardian.co.uk
kyoceracyber.com

KYOCERA