VASION

The hidden vulnerability: Why print security can't be ignored

Agencies can address an often overlooked vulnerability by strengthening the security of print servers

Justin Scott
Vasion

"PRINTERS AND PRINT SERVERS ARE ATTRACTIVE TARGETS FOR HACKERS BECAUSE THEY HAVE A PRIVILEGED NETWORK POSITION AND OFFER ACCESS TO MULTIPLE NETWORK SEGMENTS AND STORED CREDENTIALS."

Government agencies face unprecedented challenges protecting data as workforces shift to digital operations. Digital documents face global security threats, unlike physical files secured in filing cabinets.

A single breach could compromise millions of documents in seconds. The 2015 Office of Personnel Management hack[1] exposed over 21 million government employees' personal information. In addition, one person with legitimate access could download a vast amount of classified material and reveal it publicly, as Edward Snowden did.

Digital systems demand appropriate security measures and intricate permissions and structures that manage which people and devices have access to documents. Adding to the complexity is the need for agencies to coordinate their efforts across departments, classifications and government entities.

Printers are not 'set and forget' devices

Printing can often be overlooked as the source of major network vulnerabilities. Printers and print servers are attractive targets for hackers because they have a privileged network position and offer access to multiple network segments and stored credentials. Hackers who access a government CTO's printer can intercept all documents sent to that device.

The PrintNightmare vulnerability, which was discovered in Windows Print Spooler in 2021, opened a way for hackers to obtain system privileges and install malicious programs through remote code execution. Unfortunately, many organizations treat printers and print servers as set-and-forget devices. Administrators don't change the default credentials and run unpatched, out-of-date software and firmware, making those devices vulnerable to compromise. Furthermore, print traffic is often unencrypted and can be directly accessible from the internet.

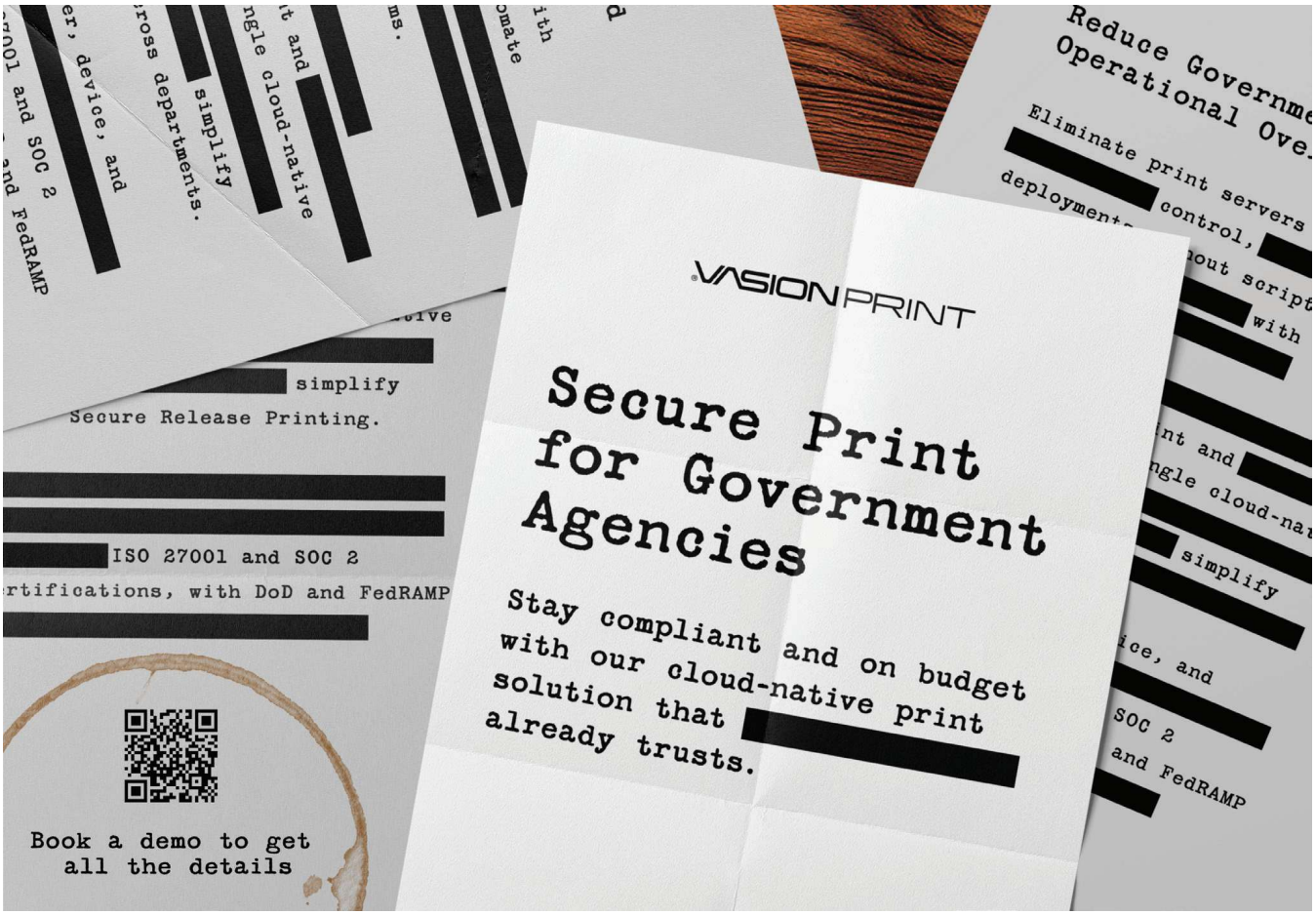
Agencies can reduce risks by patching print servers, changing default passwords, segmenting printing infrastructure on isolated networks and controlling printer access.

Removing single points of failure

Vasion Print (formerly PrinterLogic) eliminates print servers while strengthening security. Agencies can move the activities associated with print server security into Vasion's secure cloud. Our solution removes key vulnerabilities and single points of failure because it eliminates the need for traditional print servers while allowing agencies to maintain control over their printers.

Vasion's core solution is SOC 2 Type 2 compliant and ISO 27001:2022 certified. We adhere to the rigorous

[1] https://tinyurl.com/OPMbreach

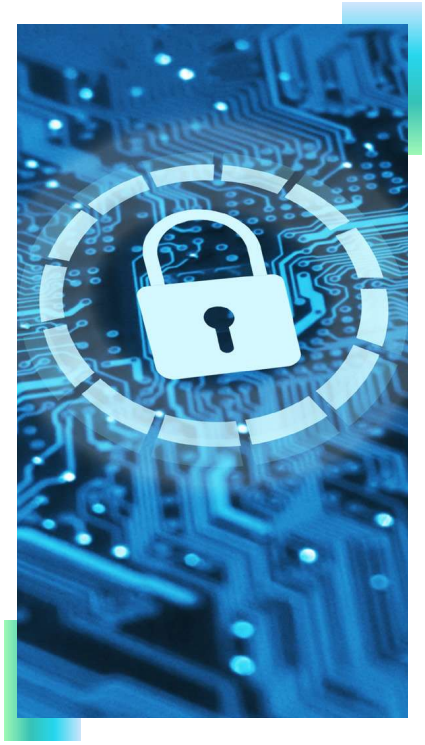


security requirements of the National Institute of Standards and Technology's Special Publication 800-53. We're simultaneously pursuing FedRAMP High and Defense Department Impact Level 4 authorizations with the Defense Information Systems Agency as our sponsor for the DOD certification. We are now actively listed on the FedRAMP Marketplace as "In Process," validating that our platform is actively seeking federal cloud security standards. We've completed the auditing and red-teaming activities, and once we receive FedRAMP authorization, our cloud service will be available in AWS GovCloud for federal agencies to use.

We use a Zero Trust approach to security, so data remains encrypted at all times. Although print jobs stay on the agency's network, administrators have the option of instituting Secure Release Printing, which requires users to present a personal identity verification card, Common Access Card, PIN or password to release print jobs. We also offer secure Off-Network Printing, a mobile app and QR-based touchless printing.

As the government's hybrid workforce rapidly expands, Vasion empowers IT administrators to deliver secure, seamless print services anywhere—whether users are inside the network, outside the network or off the network entirely. ■

Justin Scott *is senior director of DevOps and Security at Vasion.*



ADOBE STOCK // MICHAEL TRAITOV