FROM DEVICE TO DATA:

Creating an Efficient Workflow with Security in Mind in Higher Education

Colleges and universities store massive amounts of sensitive data — including research studies, student health records, and other personally identifiable information (PII). Due to this, they are a prime target for cyber attacks. Higher education institutions must also comply with various state and federal regulations to protect student privacy, which can further complicate the data protection environment.

IN 2016, THE EDUCATION SECTOR MOVED FROM

THIRD TO SECOND

FOR THE HIGHEST NUMBER OF BREACHES BY INDUSTRY.[1]

THERE WERE

562 REPORTED DATA BREACHES

AT 324 HIGHER EDUCATION INSTITUTIONS BETWEEN 2005 AND 2014, WHICH REPRESENT ABOUT 15.5 MILLION RECORDS.[2]

This infographic highlights some common areas of potential vulnerabilities in a typical higher education digital workflow. It also shows the access controls and security features that can be layered on to help enhance document protection, increase efficiencies, and support compliance obligations — allowing colleges and universities to focus on their core mission of improving student outcomes.

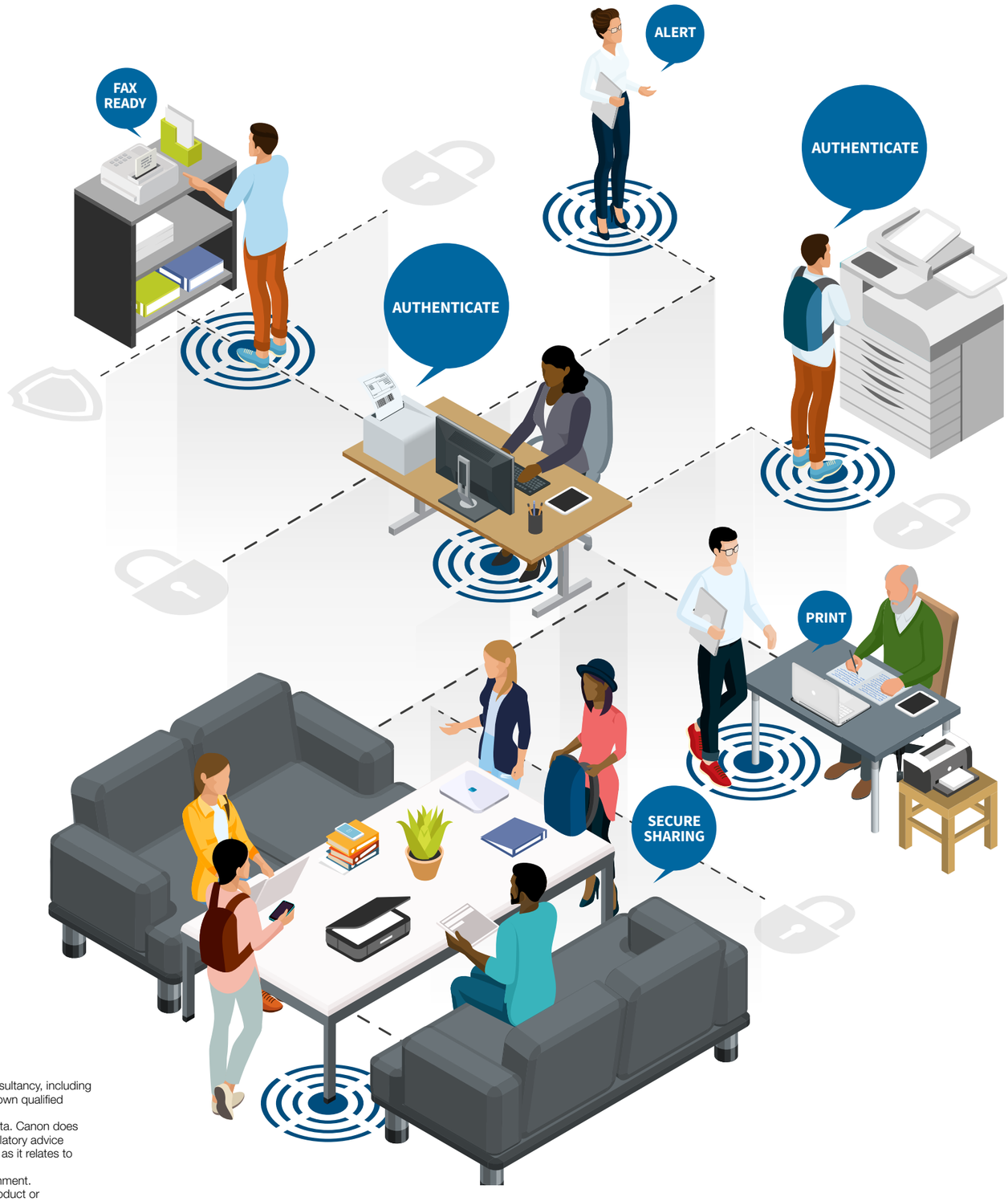
PRODUCED BY

CENTER FOR DIGITAL EDUCATION

SPONSORED BY

Canon

CANON SOLUTIONS AMERICA



Layered Security

Layered security comprises device security, print security, information security, and cybersecurity, resulting in a comprehensive approach to protecting student information.

Automatic Alerts

An administrator can be alerted should someone attempt to print, scan, or copy sensitive documents that contain keywords (confidential, faculty only, etc.).

Defense at Device

Before accessing a device to print, scan, or copy, an instructor can use a school-issued ID card to help gain the appropriate level of access.

PII Protection

An administrator can print student information from a mobile device, which is then held on a server with security features until he or she enters a password at a printer to retrieve it.

Compliance

A layered approach to protecting your organization can establish an effective security posture and thus facilitate compliance with regulatory guidelines.

Collaboration without Borders

When collaborating with staff and other departments, enterprise digital rights management (EDRM) tools enable administrators to control file level access to help ensure that information is not compromised.

1. Symantec's 2016 Internet Security Threat Report, https://www.symantec.com/security-center/threat-report 2.Just in Time Research: Data Breaches in Higher Education, https://www.educause.edu/ir/library/pdf/ecp1402.pdf