Datasheet

Print Security Advisory Services

Print Services

Service benefits

- Threat awareness
- Robust risk analysis
- Print security strategy recommendations

Feature highlights

- Onsite print security education and risk assessment
- Detailed risk report
- Security policy guidance
- Solution recommendations

Service overview

Data centres and corporate networks devote more and more resources to security, but many strategies fail to address printing and imaging vulnerabilities—even though the potential costs of a security breach are just as high. Lost or compromised confidential data, client records, or proprietary information can easily cost companies millions of dollars and create lasting damage to reputations. Securing environments adequately can be a real challenge: It often competes with other priorities—cost, ease of use, and more. And it's not uncommon for there to be a lack of knowledgeable, in-house printing and imaging security experts available. The many dangers that threaten hardware devices, important data, and printed documents demand a strong defence.

Features and specifications

Print Security Advisory Services will conduct a comprehensive site evaluation and security workshop. After these, our security advisors will help you develop a cohesive printing security strategy, and recommend solutions to help you achieve your security objectives.

- Current threat landscape review: Our print security experts will educate you on the current threat environment around imaging and printing devices and the probable threats confronting your organisation. We will also educate you about regulations specific to your geographic location and industry to help achieve and maintain compliance.
- Customer environment assessment: We conduct a thorough review of your printer fleet, looking for outdated software, improper configurations, and other lapses in print security that could expose your business to unnecessary risk.
    - Device: The physical device is the foundation of printing. If the device is not up to date with fixes, proper configuration, or security technology, then it is vulnerable.
    - Data: Data in transit and data at rest both need to be considered when evaluating security to protect from loss and prove integrity.

  - Document: If not proactively secured, documents can be at risk of theft and tampering, leading to data breaches or forgery.
  - Manage and monitor: All of the security efforts you put in place need to be monitored and maintained over time, without placing an additional burden on your IT staff.

- Security strategy recommendation: Print security advisors identify risks, estimate their potential impact, and present recommendations to help secure the printing environment.

At the end of this engagement, you will have the information you need to achieve the level of security that today's regulatory requirements demand—either on your own or with the help of a trusted HP partner.

Delivery specifications

Site evaluation and workshop

1. A print security advisor will address key stakeholders, educate them on threats, and help them reach consensus on the goals of a new printing security strategy—one that strikes the right balance between security, cost, and ease of use.
2. The advisor will assess vulnerabilities, gather information on the current print and security environment, and recommend updates to your security policy.
3. The advisor will conduct an exploratory workshop to identify business needs and associated security postures.
4. The advisor will educate your IT and security personnel and other stakeholders about industry-related risks, hosting information sessions on some or all of the following topics: logical access, asset management, patching and AV, business continuity, personal security, governance, security configuration, log management and security incident, network security, access control, physical security, data security, build and release, information security, system acquisition, and system development.

Security strategy recommendation

1. The advisor may recommend updates to your print security practices, including:
   a. Process recommendations to eliminate gaps in security coverage
   b. Hardware solutions to protect sensitive data stored on printers and MFPs
   c. Software solutions to protect data in transit through the office network or the cloud
   d. Services and solutions to monitor the printing environment
2. At the conclusion of the engagement, HP will deliver:
   a. An executive PowerPoint presentation summarizing relevant business needs and vulnerabilities, if any.
   b. A detailed security analysis report (PDF) that lists immediate and eventual needs relating to image and print security, along with a recommended security policy.

Customer responsibilities

- Personnel: Arrange for appropriate personnel to participate as needed.
- Workspace: Provide adequate workspace for use by HP personnel, including necessary access to building facilities, computer room facilities, systems, passwords, etc.
- Escorts: Assign project representatives to accompany HP personnel while they are on-site.
- Communication: Establish clear lines of communication for rapid resolution of critical problems.
- Safety: Inform HP personnel of any potential health or safety hazards.

Service limitations

This service is advisory in nature and does not include the sale, installation, or maintenance of any part of a recommended solution, unless explicitly stated. Additional services are available to assist the customer with their security journey. Services are not available on HP holidays.

Terms and conditions

See complete Care Pack terms and conditions.

For more information

Contact your local HP sales representative or channel partner for details or visit hp.com/go/printsecurity

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA7-1268EEW, October 2017