KEYPOINT INTELLIGENCE

Inaugural Event!

Custom Testing

BUYERS LAB VERIFIED SECURE TESTING PROGRAM

Introduction

According to a recent security survey from Keypoint Intelligence, on average less than 30% of organizations in the healthcare, financial services and government arenas—which are typically the most security-conscious organizations—take extra steps to secure their MFP devices. And among those that do not secure these devices, almost one-third still believe it is not necessary to support securing MFPs compared to other devices on the network. This study illustrates that, while security remains to be a #1 priority for IT, there is still quite a bit of mystery and confusion surrounding printer and MFP security in the marketplace.

Keypoint Intelligence-Buyers Lab, the industry's leading authority in hardcopy device testing and research, is looking to change this by creating, for the first time, an industry-standard security testing benchmark that standardizes the requirements for output device security. We understand that most equipment makers do their own rigorous security testing on their devices. This Keypoint Intelligence program looks to complement that by providing independent verification of an OEM's claims (or confidential feedback to program participants when improvements are needed) based on standardized testing derived by industry security experts in partnership with the manufacturers. This will create a new touchstone for the industry and provide manufacturers the option to use the exclusive "Buyers Lab Verified Secure" seal on products that pass the verification test suite.

Overview

- Initial and ongoing *confidential* security verification testing
  - Buyer's Lab and its partner, a recognized security-assessment leader, will set the testing criteria with input from OEMs
  - This fee-based program is a complement to Buyers Labs' traditional free testing conducted for our public test reports
  - Manufacturers will submit products that they wish to be evaluated; once testing is complete, the OEM will be provided a detailed private report of the results
  - For devices that pass the verification criteria, OEMs will have the option to license the exclusive "Buyers Lab Verified Secure" seal for use on websites, marketing materials, point-of-sale displays, product packaging and so on
  - If licensed, the seal will valid for use on all models in a device series (for example, C3500 series including the C3530, C3550, C3570) as long as the non-tested devices employ the same engine, controller, operating system and embedded software architecture, and essentially the same firmware
- OEM engineers and developers can use the test results to improve their machines' security; devices that do not pass can be resubmitted for re-testing at a reduced fee

Project Objectives

- Establish a benchmark for the industry when it comes to MFP security for devices intended for general-business environments
- Assist vendors with product development and planning
- Verify claims by OEMS
  - Independent third-party validation with our partner
- Cut through the jargon:
  - Educate industry and buyers what the various features accomplish and their potential differences
- Promote and award "Exceptional Security Capabilities" and the reasons why

Benefits to Participants

Strategic Planning/Development

- Understand any weaknesses in current design (confidential)
- Garner actionable information from specific testing details

Marketing

- First MFP-specific security seal/validation
- Claims regarding device security validated by the industry's leading testing company for MFP/printer devices as a neutral third party

Participation/Methodology

- Buyers Lab and a leading security testing partner will run devices through a test script that mimics real-world threat s and probes the various potential security shortcomings of networked/Internet-connected output devices
- Buyers Lab will provide participating OEMs with the testing criteria after they sign on to the program but before device submission
- OEMs will be able to specify the desired security settings to be used during the test (within certain parameters)

  - Major functionality of the device required for typical business use and remote dealer access should not be compromised by over-aggressive configuration of the security settings

- The device family models, security settings and firmware versions must be reported to Buyer's Lab at the time of submission
  - Firmware versions must be publically available for download; no custom firmware developed for the one device submitted will be accepted

- Keypoint Intelligence will provide the test results in a detailed report for vendor review. Test results will not be made public by Keypoint Intelligence (Buyers Lab / InfoTrends) unless mutually agreed upon between the two parties

Project Deliverables

- Test results report
  - Additional white paper/video on a contract basis

- Optional license: "Buyers Lab Verified Secure" Seal (if device passes testing)
  - Can purchase distribution rights if devices passesOutstanding Achievement Security Awards

- Outstanding Achievement awards for Security Methods & Services may be awarded to vendors that demonstrate unique, practical, business-functional, security solutions

Project Timeline

Scoping/TAC Meetings/Feedback	**July-August**
Sales Prospecting	**September-October**
Test development/Finalize Criteria	**October**
Testing Kick Off	**November**
Deliverables	**December (and ongoing)**

Frequently Asked Questions

What testing will be performed?

- To protect the intellectual property of Keypoint Intelligence and its security testing partner, the exact test methodology will be made available only to participating OEMs under contract for the program. In general terms, the testing steps will include:
  - Reconnaissance and Network Mapping
  - Automated Vulnerability Assessment
  - Manual Issue Verification and Exploitation (penetration testing)
  - Device-specific Attacks (based on vulnerabilities identified in previous steps)

Do I have to verify all our devices?

- No. The security-verification seals will be applicable for device series tested, not to a company's entire portfolio, so only device series that you wish to have tested (for your own internal knowledge or for the potential to use the seal publicly) need to be submitted.

- The test results will apply to all models in a series that are essentially the same as the particular model tested. This means the same engine, controller, operating system and embedded software architecture, and essentially the same firmware. As long as the series is still current, the seal will apply to new members of that series family. However, if (for example) the C3500 series is submitted for testing and 18 months later the OEM introduces the C3600 series, the seal earned for the C3500 family will *not* apply. A model from the C3600 series would need to be submitted for testing. In the case of mid-life model refreshes, significant firmware upgrades and/or changes need to be evaluated by Buyers Lab to understand differences between the new firmware and the as-tested firmware that may have impacted security capabilities before permission will be given to continue using the seal for that model

Will my vulnerabilities be exposed?

- NO. Only the contact assigned to the project will receive the test results

- If you attempt the certification for a device and it does not pass, that information will not be public

- We will not publicize who is and is not participating in the program

We already submit our machines for Common Criteria testing. How does your program differ?

- The Common Criteria (CC) for Information Technology Security Evaluation applies to IT products in general, and it does not directly provide a list of product security requirements or features for specific types of products. Instead, CC certification validates that claims about the security attributes of the evaluated product were independently verified against an agreed-upon set of standards.

- This Keypoint Intelligence program, by contrast, will be created specifically for connected MFP/printer devices, and the tests will simulate real-world threats posed to, and potential vulnerabilities of, todays sophisticated connected output devices.

About Us

Keypoint Intelligence

Keypoint Intelligence is built upon two brands: Buyers Lab and InfoTrends. Both brands have deep histories and strong presence in the document imaging industry, and will continue to be supported as product brands under the Keypoint Intelligence umbrella, which has been created to accentuate everything these respected properties have to offer.

Buyers Lab

For over 50 years, Buyers Lab has been the global document imaging industry's resource for unbiased and reliable information, test data, and competitive selling tools. What started out as a consumer-based publication about office equipment has become an all-encompassing industry resource. Buyers Lab evolves in tandem with the ever-changing landscape of document imaging solutions, constantly updating our methods, expanding our offerings, and tracking cutting-edge developments.

InfoTrends

InfoTrends has over 25 years of experience providing leading worldwide market research and strategic consulting for the digital imaging and document solutions industry. InfoTrends products include research, analysis, forecasts and advice to help clients understand market trends, identify opportunities and develop strategies to grow their businesses.

Terms and Conditions

Liability for Advice

Although reasonable efforts have been made by Keypoint Intelligence to ensure the completeness and accuracy of the information contained in written and oral reports in connection with the proposed study, no liability can be accepted by Keypoint Intelligence for the results of any actions taken by the client in connection with such information, opinions, or advice.

Copyrights

Confidentiality

Keypoint Intelligence will use its best efforts to ensure that any confidential information obtained about the client and its business during the course of the proposed study is not, unless agreed otherwise in advance, disclosed to any third party without the prior written permission of the client. Keypoint Intelligence retains the right to re-use any non-proprietary information as part of its ongoing analysis of the industry.

The Buyers Lab "Verified Secure" Seal

Introductory Pricing if Submitted by October 31, 2018	Pricing
Testing & Private Report Only	$15,000
Seal Purchase & Global Usage Rights (if seal is purchased more than 30 days after delivery of the final report)	$15,000
Testing, Report and Global Seal Rights package (if seal is purchased within 30 days of delivery of the final report)	$25,000
Re-test for devices that did not pass initial test phase	$10,000

Purchase order number: _____

Signature: _____

Name: _____

Title: _____

Company: _____

Address: _____

City, State, Zip Code: _____

Country: _____

Telephone: _____

E-mail: _____

Please E-mail completed form to sales@keypointintelligence.com