FORCEPOINT
POWERED BY Raytheon

Datasheet

Trusted Print Delivery™

PROVIDING SECURE PRINTING, ADDING POWER TO CLOUD SOLUTIONS AND ENABLING HARDWARE REDUCTION

FEATURES AND BENEFITS

- **Familiar** print submission and print attributes
- **Utilizes** proven, certified and accredited Trusted Gateway System guard technology
- **Reduces** the number of printers required to support multilevel print environments
- **Reduces** space, power, support and consumables
- **Increases** security through protocol and print file conversions
- **Improves** asset management and productivity
- **Extends** investment in cloud printing strategies

Printer consolidation not only saves hardware costs but also consumables and administration. Other benefits to printer consolidation include space savings, less networking, and improved asset management. Studies show that organizations can save up to 65% of their total printing costs through printer consolidation.[1] Apply that thinking to organizations with multiple sensitive networks that have, to this point, required numerous printers at each sensitivity level.

Including Trusted Print Delivery™ provides a secure means to consolidate printers (generally to the more sensitive network) and allows these organizations to eliminate hundreds to thousands of printers and meet cost saving mandates.

TRUSTED PRINT DELIVERY™

Trusted Print Delivery is a Commercial-Off-The-Shelf (COTS), highly secure solution that allows users to print from existing applications at different security or sensitivity levels to a single printer located on the more sensitive (high side) network. Reducing printer hardware at individual security levels reduces capital investment, printer inventory, hardware maintenance/ supplies, and administration. Trusted Print Delivery leverages the widely deployed, accredited, and United States Unified Cross Domain Services Management Office (UCDSMO) Baseline listed, Trusted Gateway System™ as the secure transfer guard component. Trusted Gateway System ensures that malicious data is not transferred from low to high networks and that sensitive data is not inadvertently or intentionally transferred from high to low. In addition to the Trusted Gateway System transfer guard, Trusted Print Delivery utilizes two Print Adapters, Ingress and Egress.

The Ingress Adapter accepts print jobs from users and submits them to the guard for review. Once approved, the inspected print job is transferred to the Egress Adapter, which sends the print job to the physical printer. Submission of print jobs appears standard to the end user.

Trusted Print Delivery converts all print jobs to Portable Document Format (PDF) for inspection. The guard performs

1 "Reduce Costs Through Printer Consolidation," Info-Tech Research Group

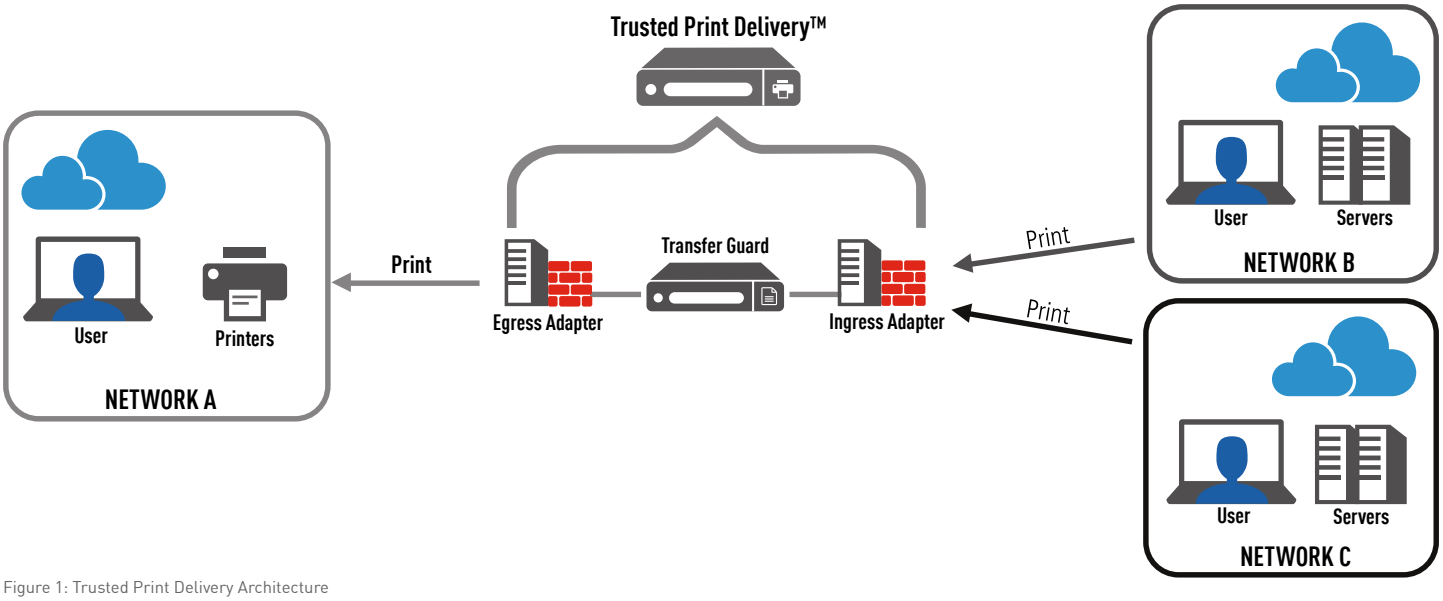

Figure 1: Trusted Print Delivery Architecture

built-in manual and automatic validations (such as virus scanning, dirty word search, and deep content inspection) and sanitizes the document as appropriate, enabling safe document printability between different sensitivity levels. The guard inspects all content associated with each print job such as user name and job control information. As an added security feature Trusted Print Delivery enforces pre-defined limits on the size of print jobs, number of simultaneous print jobs, and number of copies before the submission to the guard. This review ensures that an attempted denial-of-service (DoS) attack does not degrade legitimate use of Trusted Print Delivery. In addition, Trusted Print Delivery removes unrecognized or unsupported PCL commands present in the submitted Postscript file to eliminate potentially malicious printer commands (such as firmware updates).

Inspection and validation are transparent to the user as he or she prints from applications using familiar Windows® print options. Print jobs that fail any of the configured security validations are rejected and printing of that job is halted. Other print jobs continue to be processed unaffected by the halted print job. Trusted Print Delivery print jobs are secured throughout the print process and end-to-end auditing is recorded for administration and review. Robust auditing provides administrators with detailed logging and print delivery status for each print job. Print job status notifications (i.e., low toner cartridge, paper tray empty, service errors) are also presented to the user through the Windows tray application delivered with Trusted Print Delivery or through a web page.

EASE OF ADMINISTRATION

Trusted Print Delivery provides seamless interoperability with established print infrastructures. Minimal user desktop configuration is required and standard enterprise printers and drivers can be implemented. Banner and trailer pages are easily configurable to ensure that ownership and sensitivity levels are clearly identified (if required). Print status information is correlated across domains for a consolidated enterprise-wide view.

SECURITY

Communication between the Ingress Adapter and the guard is encrypted using Transport Layer Security (TLS) and authenticated using either username/password or certificates. The communication between the guard and the Egress Adapter is encrypted using Secure File Transfer Program (SFTP) with username/password authentication. Individual user access to the multilevel printers can be restricted using existing Microsoft® Active Directory permissions. In addition, the Ingress Adapter can restrict access by IP address/subnet through its Linux® kernel firewall.

CERTIFICATION AND ACCREDITATION (C&A)

Trusted Print Delivery utilizes the certified and accredited Trusted Gateway System as the transfer guard between Print Adapters to provide a secure multilevel boundary between different sensitivity levels. Trusted Gateway System is on the US UCDSMO Baseline list of approved cross domain

solutions and is widely deployed in operational systems around the world. Trusted Gateway System is engineered to satisfy cross domain security requirements for the Top Secret/SCI and Below Interoperability (TSABI) and Secret and Below Interoperability (SABI) certification and accreditation processes.

CONCLUSION

Trusted Print Delivery enables secure printing in environments where multilevel printing is a requirement. When extraneous printers at multiple sensitivity levels are eliminated, organizations recognize significant savings from reduced hardware, space, power, support and supplies. The robust security provided by the certified and accredited Trusted Gateway System transfer guard ensures that users can safely print to high side printers from multiple security levels without the risk of transferring malicious data or transferring sensitive data from high to low networks. Forcepoint™ secure information sharing solutions are designed to enable secure access and transfer of sensitive information for government, intelligence community, civilian, and corporate entities in the US and around the globe, including 5 Eyes nations and NATO. Forcepoint secure information sharing solutions continue to strike the right balance between information protection and information sharing—a vital component to enterprise security.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

INTERNAL REFERENCE #IIS2014-096 [DATASHEET_TRUSTED_PRINT_DELIVERY_EN] 100019FED.011416