Datasheet

Secure Sensitive & Mission Critical Data at the Endpoint

TRUSTED THIN CLIENT® AND IBM z SYSTEMS WORK TOGETHER FOR END-TO-END DATA SECURITY

One of the most important assets a corporation has is data – its own proprietary data, its customers' data, and its employees' data. The volume, tracking, and access control of sensitive data constitute some of the largest security challenges from the backend infrastructure to the ever-changing perimeter. The vast majority of security concerns today revolve around the "endpoint device." No matter how secure the infrastructure is, if the endpoint device is not secure, vulnerabilities exist.

Customers utilizing an IBM z Systems mainframe backend environment for a secure and resilient cloud-ready infrastructure with high-capacity processing capabilities understand the importance of their data and have taken steps to secure it in the datacenter. Now it is time to focus on securing sensitive and mission critical data at the endpoint – where it is most at risk.

With the inclusion of Forcepoint's Trusted Thin Client into this environment a stateless smart thin client replaces the PC, laptop or other device at the desktop.

PROTECTION AT THE ENDPOINT

Risk exposure is greatly reduced as no user data is stored on the client and there is no risk of downloading or executing malware. Due to the strict network and virtual desktop session separation, and the fact that Trusted Thin Client only provides a redisplay of data from the mainframe, no malicious code can move from one network to another greatly reducing the risk to the overall infrastructure.

Other similar solutions introduce additional risk because of the possibility that endpoints can access any data on multiple networks and those networks have access to anything on the host operating system.

Additionally, if a foreign or unapproved device is introduced to the client network, there is no mechanism for that device to retrieve a session from the Distribution Console. The system is completely controlled and isolated through the enforcement provided by the trusted operating systems on which the client and Distribution Console run and through the use of digital certificates.

Trusted Thin Client solves the difficult problem of satisfying security needs while enhancing user productivity. It provides users with secure simultaneous access to any number of sensitive networks through a single device, in support of an enterprise-ready trusted collaboration experience that brings people, data, security, policy, and governance into alignment.

SECURELY WORKING TOGETHER

The integrated solution of thin client and mainframe delivers an end-to-end independently evaluated solution that provides an environment that meets a Common Criteria Evaluation Assurance Level (EAL) of 4+ denoting high confidence that the solution's principal security features are reliably implemented.

Trusted Thin Client, has been accredited and evaluated and is in wide operational use throughout global intelligence and defense communities. It is designed and developed to meet or exceed the highest Protection Profiles and National Institute of Standards

& Technology (NIST) 800-53 requirements for securing the most sensitive information.

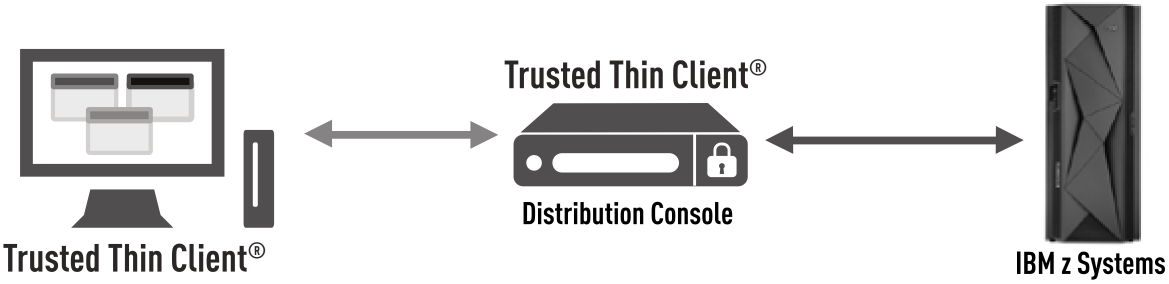
SECURE END-TO-END COMPUTING ENVIRONMENT IN PRACTICE

This solution is applicable to use cases where sensitive data needs to be isolated, yet accessible to authorized users, and protected from theft or leakage. It can also help organizations maintain the isolation of traffic between trusted Intranet and Internet networks.

The need for this type of endpoint security is seen in the financial sector. Most financial institutions have endpoints, typically personal computers, which operate on a non-secure operating system that is susceptible to malicious activity or accidental data loss. Many of these endpoints reside in open access spaces – such as a front office. These two conditions combine for a high-risk scenario where a malicious actor might gain access to a system to install malware or steal data.

By replacing these non-secure endpoints with Forcepoint Trusted Thin Client secure, read-only endpoints, should a malicious actor gain physical access to the device there is no resident data to compromise. If he or she attempted to insert a foreign device, such as another thin client, the security mechanisms built into the architecture would prevent device authentication.

A secure endpoint also protects against inadvertent or malicious data loss or leakage as the device itself prevents copying data to removable media such as a USB drive.



CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

Trusted Thin Client® is a registered trademark of Forcepoint, LLC.
Forcepoint™ Federal is a trademark of Forcepoint, LLC.
Raytheon is a registered trademark of Raytheon Company.
All other trademarks and registered trademarks are property of their respective owners.

INTERNAL REFERENCE #IIS2016-042 THIS DOCUMENT DOES NOT CONTAIN TECHNOLOGY OR TECHNICAL DATA CONTROLLED UNDER EITHER THE U.S. INTERNATIONAL TRAFFIC IN ARMS REGULATIONS OR THE U.S. EXPORT ADMINISTRATION REGULATIONS. [DATASHEET_SECURE_SENSITIVE_MISSION_CRITICAL_DATA_AT_ENDPOINT_IBM_EN] 100044FED.020516