FORCEPOINT
POWERED BY Raytheon

Case Study

Center for Army Analysis (CAA)

SECURE CROSS DOMAIN ACCESS AND TRANSFER ACCOMPLISHED WITH ONE WIRE TO THE DESK.

CUSTOMER
Center for Army Analysis

INDUSTRY
Combatant Commands

USER BASE
Authorized personnel are able to access mission-critical information for analysis of force structure, operational capabilities, resource analysis, readiness, sustainability, and logistical and personnel processes, all of which are critical in the agency's mission to help fight the Global War on Terror.

CUSTOMER

The Center for Army Analysis (CAA) located at Ft. Belvoir provides state-of-the-art analytical support to Headquarters, Department of the Army. As they conduct studies on important Army-related issues of strategic and operational concern for the Staff and major commands, the Department of Defense (DoD) and the Combatant Commands, CAA is totally dependent on information management systems to perform critical analytical functions.

CAA's mission is to conduct analyses of Army forces and systems in the context of joint and combined warfighting, which include theater-level investigation in the areas of force structure, operational capabilities, resource analysis, readiness, sustainability, and logistical and personnel processes.

CHALLENGE

CAA was working with an infrastructure in which access to all Command, Control, Communications, Computers and Information Management (C4I) networks required each user to have four separate workstations and a Black Box KVM switch at their workspace. This resulted in duplication of hardware and massive power consumption.

Another problem that CAA faced was a severe time degradation in moving classified information across multiple networks. This prevented the execution of critical Global War on Terror and warfighting analyses.

SOLUTION

CAA enlisted Forcepoint™ to implement the Trusted Thin Client® and Trusted Gateway System™ solutions to address their multilevel cross domain access and transfer needs.

Trusted Thin Client provides simultaneous secure access to Microsoft® Windows® applications running at different sensitivity levels – all from a single desktop. Trusted Thin Client is a controlled interface that provides access to four networks within the CAA Headquarters. Utilizing two IBM® System x® x86 servers for the back end Distribution Consoles and Hewlett-Packard® thin clients at the desktop, the system is configured to use Microsoft Terminal Services and Citrix® technology for remote connectivity to the high- and low-side network servers. Trusted Gateway System was implemented to provide a real-time data source for authorized CAA analysts. Users are able to access Trusted Gateway System from within their Trusted Thin Client environment

preventing the need for additional desktop hardware. Trusted Gateway System allows users to conduct multi-directional transfers of disparate data between their four networks in a timely manner, which provides users a secure way to share information. Trusted Gateway System also provides a strong barrier to prevent attacks (e.g., penetration attempts) from lower-level networks.

Multi-directional transfer of information includes sending sanitized information from a higher-level network to one at a lower-level, moving data from a lower-level to a higher-level, and moving files laterally across network boundaries. Trusted Gateway System can move one or more files from any level to any level, allowing many high or many low destinations, and it provides bulk one-way secure uploads while also supporting multi-directional transfer capabilities.

MISSION RESULTS

Simultaneous access to multiple security domains and the ability to utilize a multi-directional transfer solution through a single wire to the desktop is critical to the accomplishment of CAA's mission in support of the Global War on Terror. Through the Trusted Thin Client and Trusted Gateway System solutions, CAA analysts have the ability to conduct critical analyses utilizing all available information in the most efficient and secure manner possible. This solution substantially enhances user functionality and enforces a strong protection security policy to prevent cross domain contamination in a more stringent manner than the previous infrastructure.

By running cross domain software on the back end to enable domain separation, CAA not only decreased hardware, maintenance, and infrastructure costs but also improved information access and sharing capability while reducing power usage. The hardware requirements decreased from four desktop machines per user to one thin client device per user. It is anticipated that power usage will continue to significantly decrease and could reach an overall reduction approaching 75 percent.

SUMMARY

Modernization and accomplishment of "green" information technology initiatives

The implementation of Forcepoint solutions within CAA resulted in significant increases in the efficiency with which authorized personnel are able to access mission-critical information for analysis of force structure, operational capabilities, resource analysis, readiness, sustainability, and logistical and personnel processes, all of which are critical in the agency's mission to help fight the Global War on Terror.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

INTERNAL REFERENCE #2011-360 [CASESTUDY_CENTER_ARMY_ANALYSIS_EN] 300055FED.011416