



INDUSTRY PARTNER BRIEF: GOVERNMENT

FOUNDRY AND STILLSECURE

THE CHALLENGE



In securing networks and digital assets, government agencies face challenges beyond those encountered by the private sector. Government computer systems are attractive targets for hackers and terrorists. As public-sector IT professionals know, it is not a question of if you're getting attacked, it is a question of detecting when attacks have been launched, which attacks present legitimate threats, and how to avoid or mitigate damage.

THE FOUNDRY / STILLSECURE SOLUTION FOR GOVERNMENT

Together, Foundry Networks and StillSecure merge security with the government network infrastructure, embedding protection from a full range of network threats into the IT infrastructure and daily operations.

Government agencies have long looked to Foundry Networks solutions for performance, robustness, and innovation and support that exceeds competitive offerings. Whether it's a defense, intelligence, civilian, or a state or municipal agency, Foundry Networks supplies all the requisite connectivity and protection from the most remote edge device to the largest data center in a high performance computing environment. The Foundry government portfolio establishes new benchmarks in resilience, data protection, and network performance with a comprehensive suite of products and support services that help build a robust, scalable, and highly available network infrastructure for the expanding and evolving needs of mission-critical applications, IPv4 and IPv6 requirements, and data sensitive environments.

The integrated StillSecure[®] suite of network security solutions allows agencies to comply with applicable regulations, take preventative measures to eliminate network weaknesses, and protect critical systems from terrorists, hackers, and others with malicious intent.

The StillSecure and Foundry partnership for government agencies is based on deep integration of NAC at the hardware level, enabling the most secure method for enforcement, 802.1x based switch port based access control. Safe Access tests endpoint devices as they attempt to log onto the network and determines whether they should be permitted, denied, or quarantined based on their ability to comply with the organization's pre-assigned security policy. Once the device's health status is determined, the Foundry switch allows or denies access, enforcing the security policies.

ABOUT STILLSECURE

StillSecure[®] creates secure network infrastructures. By converging networking and security, StillSecure is the foundation for secure, intelligent, highly automated networks that are easy to manage and protect. By focusing on the convergence of networking and security, StillSecure provides the foundation for secure, intelligent, highly automated networks that are easy to manage and protect. StillSecure believes security is no longer an add-on—the network must have the inherent capability to protect itself. StillSecure customers range from midsize companies to the world's largest enterprises and agencies in government, financial services, healthcare, education, and technology.

CHALLENGES FOR GOVERNMENT AGENCIES:

- Achieving and demonstrating compliance with security regulations and policy initiatives
- Integrating networking and security for easy installation and management
- Dynamically managing network security across tightly defined organizational structures and in real time
- Delivering on the four vital areas of NAC: pre-connect testing, post-connect monitoring, identity-based management, and remediation.
- A high-availability architecture that ensures that the network continues to operate at peak performance

STILLSECURE

100 Superior Plaza Way
Suite 200 • Superior, CO 80027
Tel: 303.381.3800 • www.stillsecure.com

© 2007 StillSecure. StillSecure is a registered trademark. All other registered or unregistered trademarks are the sole property of their respective owners.

ABOUT FOUNDRY

Foundry Networks[®] Inc. is a leading provider of high-performance enterprise and service and backbone Ethernet switches, Web and content-aware application switches, network-wide security solutions, wireless LAN and access points, wide area access routers and internet provider edge and service provider core MPLS routers. Foundry's customers include the world's premier ISPs, Metro service providers, and enterprises including e-commerce sites, universities, entertainment, healthcare, government, financial, manufacturing companies, technology, and high-performance computing (HPC) sites.

4980 Great America Parkway • Santa Clara, CA 95054
Tel: 408.207.1700 • Fax: 408.207.1709 • www.foundrynet.com

© 2008 Foundry Networks. All rights reserved. Foundry and Foundry Networks are registered trademarks. All other trademarks are the property of their respective owners.

The foregoing may contain "forward-looking statements" which are based on management's current information and beliefs as well as on a number of assumptions concerning future events made by management. These forward-looking statements include, without limitation, statements by executives or spokespeople regarding Foundry's positioning and potential plans. The forward-looking statements are only predictions and are subject to a number of risks and uncertainties, which could cause actual results to differ materially. Foundry assumes no obligation to update the forward-looking statements contained in this document. Furthermore, no statements made by Foundry Networks, Inc. ("Foundry"), or information contained herein, may be deemed to constitute either an amendment of an existing agreement or an implied new commitment, promise or legal obligation by Foundry to develop or deliver any specific product, feature or functionality.