BROCADE

Network Security: Protecting Data in Flight

The right network data protection tools lower encryption costs and scale the network without adding complexity.

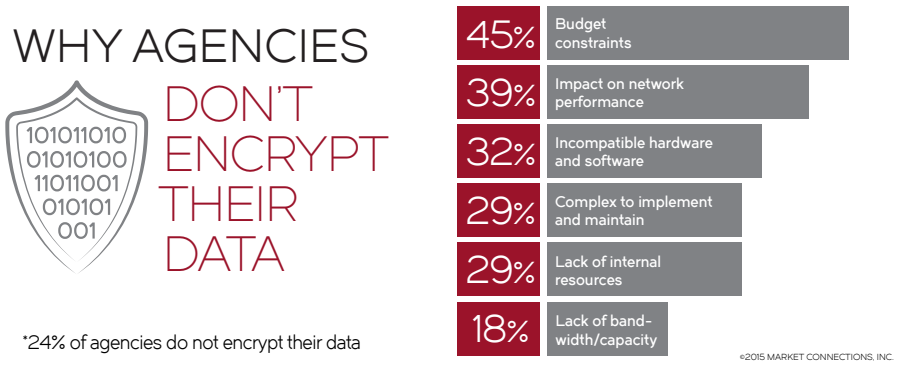
As networks become increasingly complex—and more data moves across the network—vulnerability to security breaches can increase. Despite the volume of unencrypted inter- and intra-agency data traversing most enterprises, many federal agencies are not implementing the right technology to protect the network because it is expensive and degrades performance. The right tools can help agencies overcome these network security obstacles, and provide end-to-end protection for data, within the data center and in transit.

Executive Summary

As agencies consolidate data centers and share resources, data is traveling farther away from the data center, while data rates on the network are increasing. At a time when the government is focused on preventing cyber breaches, finding ways to protect this data—both in the data center and while in transit—is a critical concern.

For years, agencies have used firewalls, encryption appliances, and embedded encryption service modules within routers to prevent breaches and protect data. And they leverage TLS/SSL extensively to secure Web applications. However in a study done by Market Connections, Inc., it was uncovered that these security measures do not address all "inflight" data transfers that exist. In addition, those tools can significantly impact performance and may not adapt well to today's complex networking environments.

More sensitive data transfers will require minimum encryption strengths of 128 bits for secret traffic and 256 bits for top secret traffic. In addition, networks are getting faster, and data-protection tools must scale as these data rates increase. Many antiquated encryption tools on the market cannot operate at 10 Gbps or higher, which is quickly becoming prevalent in federal IT infrastructure environments. Therefore, while agencies may have network data security measures in place, those measures may not address today's security needs.



Data Security Challenges and Priorities

Agencies understand the importance of encrypting data, but not all are doing so. Agencies are aware of the need to protect their data, and almost all respondents (96 percent) believe encrypting data on the network is important. However, one-quarter of agencies (24 percent) are not encrypting their data at all, though data encryption is a key measure in preventing threats.

IS DATA AS SAFE AS AGENCIES THINK IT IS?

Agencies have a false sense of security about the level of protection of their data.

96%
feel encrypting data on the network is important

76%
of agencies have encryption protocols in place, but ONLY 128 BIT AND 256 BIT ARE STRONG ENOUGH for the full range of network security needs

ENCRYPTION PROTOCOLS IN USE*

- SSL: 62%
- 256 bit: 32%
- 128 bit: 20%
- 64 bit: 9%
- Don't know: 9%

*128 and 256 bit encryption are required to protect Secret and Top Secret data on the network.

©2015 MARKET CONNECTIONS, INC.

Agencies are protecting data, but not at the level they need to. Almost three-quarters (72 percent) of agencies say prevention is the highest priority within their cybersecurity strategy, which makes sense as proactively preventing threats is preferable to reacting to a compromise in the environment. However, there is a disconnect between priorities and actions—of the agencies that encrypt their data, 62 percent are using SSL as their primary in-flight encryption mechanism and 9 percent are using encryption levels below 128 bits. These encryption methods are not strong enough to protect sensitive data traveling over federal networks.

Agencies believe Suite B is important. As agencies look at their network protection strategies, 87 percent believe it is important to leverage the Suite B algorithm—a set of cryptographic algorithms the National Security Agency, in conjunction with the National Institute of Standards and Technology (NIST), has specified as part of the Cryptographic Modernization Program. It serves as an interoperable cryptographic base for both unclassified information and most classified information.

The Suite B encryption algorithm supports the highest level of encryption strength—128 bits for secret traffic and 256 bits for top secret traffic. Yet, the majority of agencies are using SSL as their primary in-flight encryption mechanism, and they may not be taking steps to provide stronger encryption with Suite B.

How Secure Is Data on the Network?

Only one quarter (26 percent) of respondents believe they have full network-level security protection, and only 23 percent say their agency is fully cyber-secure.

Agencies need stronger encryption to protect all of their data. Of the 76 percent of agencies encrypting their data, only 20 percent are using 128-bit encrytion, and 32 percent are using 256-bit encryption. And, if only one quarter (25 percent) of respondents say their end points are fully encrypted, then the majority does not have a true end-to-end in-flight encryption solution in place. In addition, while almost half (49 percent) of respondents say their agency implements Access Control Lists (ACLs) to forward or block traffic based on rules, this does not address how the data is effectively secured in flight. This means that a majority of sensitive data is being transmitted un-encrypted within the enterprise—indicating that even for the agencies that believe they have full network-level security protection, most of their data is still unprotected.

Agencies need data protection tools that can scale. Another factor impacting data protection is the speed of the network. More than two-thirds (67 percent) of those surveyed have connection speeds over 10 Gbps. Many older data protection solutions on the market do not perform at rates over 10 Gbps, and those that do exist are costly and not able to scale effectively. Network speeds will continue to increase, and agencies need to find data protection solutions that scale up without adding complexity.

The farther data travels, the more at risk it is. Finally, the ability to protect data on the network diminishes the farther the data travels—a significant issue as agencies consolidate data centers. Only one third (33 percent) say their data protection implementations associated with agency-to-agency transit are excellent. However, given the issues around encryption strength and network speeds, this data may not be as secure as the agencies think.

Brocade Solutions

Brocade® data protection solutions eliminate the challenges the government faces, providing encryption at a lower cost, the ability to scale without adding complexity, or performance degradation,

and protection that adheres to Suite B specifications.

Scale With Increased Speed and Distance

As data travels faster, encryption throughput needs to scale beyond 10 Gbps to support much larger flows within the enterprise. Almost one third (31 percent) of agencies are at 10 Gbps and 36 percent of agencies are quickly migrating to 40 Gbps and 100 Gbps network interconnects. These network speeds are four to ten times the performance of most firewalls and encryption devices. If the encryption strength is at the SSL level, then the security measures in place for data in flight are inadequate. Most data security products cannot deliver IPsec and MACsec functionality at these speeds; those that can are costly, and in most cases, cannot scale without adding complexity to the network. Brocade provides data protection with IPsec and MACsec encryption without impacting the non-encrypted throughput values, and at a significantly lower cost than competitors.

Easy to Deploy and Manage

Brocade high-bandwith IPsec/MACsec solutions with the Brocade MLXe Router integrate smoothly into medium- to large-scale enterprise deployments, as well as support larger data transmissions within the data center. As data traverses the edges of the enterprise, agencies can use software encryption components to complement the physical encryption solutions. The Brocade Vyatta vRouter provides the ability to deploy encrypted IPsec VPN solutions at remote locations through software that is applied to any standard x86 platform. These software entities are easy to deploy and can be managed centrally. Given the flexibility of software, when the environment changes, agencies can adjust and move the software where needed. This approach will prove advantageous as tactical entities deploy and require reachback to a particular service within the network enterprise.

Using software-defined networking (SDN) to abstract IPsec and MACsec security services and centrally manage them provides a new paradigm for IT professionals. It enables them to provision new security models by dynamically leveraging both physical and virtual assets. This software abstraction allows them to adjust end-to-end security deployments based on a particular mission and adjust these security scenerios appropriately.

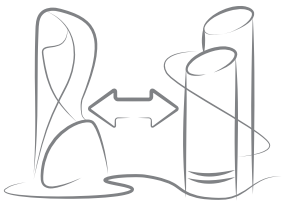
Flexibility to Scale as Needed

Budget challenges need not be a barrier to successful deployment of at-rest and in-flight security measures. The abililty to leverage software over existing computer hardware is one option to deploy compliant lower-cost solutions. In addition, the ability to invest in a single modular hardware solution that scales to support current and future in-flight encryption needs would provide a level of savings over time to prevent fork-lift upgrades. For example, the Brocade MLXe scales to 1 Tbps of encrypted throughput, which should support increasing data rate requirements over time. Leveraging software components alongside hardware components helps achieve the desired end-to-end security strategy that government organizations need.

Alternative Acquisition Strategies

To complement data protection solutions, IT professionals will need to look at new acquistion strategies to effectively modernize current security depolyments. Being able to modernize using operational dollars may be an advantageous proposition. Brocade Network Subscription lets customers invest in new security solutions with no upfront costs. Customers pay a monthly fee with OpEX dollars for the duration of the subscription service. Over time, the customer has the autonomy to scale the hardware and software associated with this offering

Network Speed



Networks are getting faster and data is traveling farther. Encryption tools need to be able to keep up and scale up.

67% OF AGENCIES
have network speeds 10Gbps or higher...

100Gbps	40Gbps	10Gbps
16%	20%	31%

...BUT MOST DATA PROTECTION TOOLS DEGRADE PERFORMANCE AT THESE FASTER NETWORK SPEEDS.

©2015 MARKET CONNECTIONS, INC.

based on their business requirements, as well as the ability to take advantage of new technologies with no penalties incurred.

Summary

Despite the priority that agencies place on security and prevention, the study results clearly show that most agency data is not fully protected, which increases the threat of cyber attacks. With the possible performance issues and increased network complexity and costs associated with most data security tools, it is no surprise that so much data is being left vulnerable. But as more and more sensitive data travels over government networks, encrypting data end-to-end is critical.

As agencies consider implementing stronger encryption methods, or developing a network cyber security plan, it is imperative to ensure the encryption products have the required strength to both secure data and meet current and future bandwidth needs. Brocade offers cost-effective Suite B-compliant solutions that protect sensitive data without degrading performance or adding complexity.

About the Study

Brocade commissioned Market Connections to learn to what extent agencies feel their data is protected and the challenges they face in addressing data protection proactively. The blind online survey of 200 IT decision makers included 76 percent from federal civilian agencies and 24 percent from defense and intelligence agencies. Respondents represent a variety of job roles, including CIO, network manager, data center manager/director and security administrator. Almost one third (32 percent) manage or implement network data protection solutions. Nearly half (46 percent) evaluate or recommend network data protection solutions, 45 percent are on a team that evaluates or recommends network data protection solutions, and 18 percent make the final decision regarding network data protection solutions.

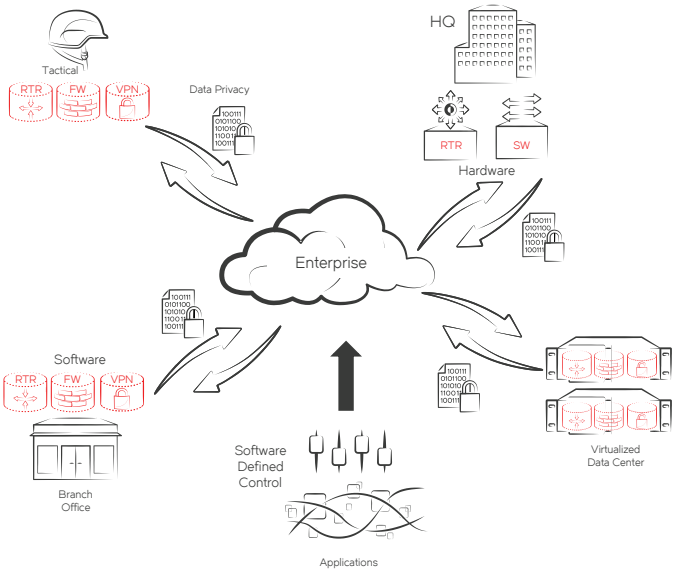


Figure 1: Centrally Managed and Controlled Data Protection Strategy across the Agency.

About Market Connections

Market Connections delivers actionable intelligence and insights that enable improved business performance and positioning for leading businesses, trade associations, and the public sector. The custom market research firm is a sought-after authority on preferences, perceptions, and trends among the public sector and the contractors who serve them, offering deep domain expertise in information technology and telecommunications, health care, and education. For more information, visit www.marketconnectionsinc.com.

For more information about Brocade Security Solutions, please go to http://www.brocade.com/solutions-technology/enterprise/network-security.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

© 2015 Brocade Communications Systems, Inc. All Rights Reserved. 06/15 GA-WP-1963-00

ADX, Brocade, Brocade Assurance, the B-wing symbol, DCX, Fabric OS, HyperEdge, ICX, MLX, MyBrocade, OpenScript, The Effortless Network, VCS, VDX, Vplane, and Vyatta are registered trademarks, and Fabric Vision and vADX are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of others.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment features, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This information document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

BROCADE