govCIO OUTLOOK

Top 10 Security Solution Providers 2016

From big data to mobile and social media, the 21st century has ushered a variety of innovative technologies that can help the government sector to better serve their constituents. However, unlike other businesses, organizations in the government sector face a more challenging reality while implementing today's "vast" infrastructures: a strong threat to data security.

This brings a number of important questions to the forefront—the issue of serving a population that is increasingly dependent on technology and leveraging the huge amount of data generated to better serve the public, while maintaining data security.

To address these issues, there are a number of security solution providers that draw upon large client base and best practices to help the government sector. These providers also assist government agencies keep pace with the rapid technology changes while helping them stay compliant and secure.

In this scenario, to help CIOs and CEOs find the right security solution provider, a distinguished panel comprising CEOs, CIOs, analysts and the Government CIO Outlook's editorial board has selected top players from over 300 solution and service providers.

In our selection, we looked at the vendor's capability to fulfill the burning need for cost-effective and flexible solutions that add value to the complex security landscape. We present to you Government CIO Outlook's "Top 10 Security Solution Providers 2016"

Company:
Accellion

Key Person:
Yorgen H. Edholm,
President & CEO

Description:
Accellion enables government agencies to securely access, create, edit and share information—wherever work takes them

Website:
accellion.com

Accellion

Kiteworks—Secure File Transfer Anywhere, Anytime

Yorgen H. Edholm

The holiday decorations were barely back in the attic when 2016 already saw its first high-profile cyber attack. Time Warner Cable recently reported that up to 320,000 customers had their email passwords stolen. The data breach is another wakeup call for government organizations, following attacks at the U.S. Office of Personnel Management and the IRS last year. "The sophistication of these attacks is increasing daily; hackers lie in wait and, once they emerge, you've got a fox in a hen house scenario," says Yorgen H. Edholm, President and CEO, Accellion. "Though firewalls can repel some of the attacks, they fail to protect against internal threats, whether it's an employee falling victim to a phishing attack, sending proprietary information to a competitor, or losing their cell phone." This is where Palo Alto based Accellion comes in. The secure file transfer and collaboration solutions company helps organizations prevent unauthorized access to sensitive data. "Our solution isolates and encrypts data, preventing unauthorized access—be it intentional or unintentional," adds Edholm. Accellion's secure content platform, kiteworks, offers a single pane of glass view to enterprise and cloud content stores like SharePoint, Documentum, Box, and Dropbox, and secures these files for sharing and collaborating between employees, partners and their multiple devices.

With the advent of cloud technology, businesses are migrating more of their data from traditional storage systems to the cloud. "To meet the security and compliance needs of enterprises and government agencies, these organizations require a solution that's flexible, scalable and secure," says Edholm. Accellion's secure content platform achieves these requirements with an industry first private cloud multi-tier architecture. Accellion continues to innovate, staying ahead of industry trends, customer needs, and stringent security and compliance requirements.

This is particularly critical when the unique needs of local, state and federal government agencies are considered. It may be a police department sending body armor video footage to a district attorney's office; a captain sending a battlefield map to a forward unit, or a doctor at a VA hospital accessing patient records stored in another facility. In such cases, the files are large, contain highly sensitive information, and would have drastic consequences if they were compromised.

It's because of these unique needs that the kiteworks platform can be fully customized. Enterprise-grade mobile SDKs and APIs enable rapid development of content-rich applications as well as integrate with and extend existing enterprise infrastructure to numerous devices. In addition to a development platform, private cloud multi-tier architecture and single pane of glass view into multiple content stores, kiteworks provides a number of key security features. These include: customer encryption key ownership, file tracking/reporting, fi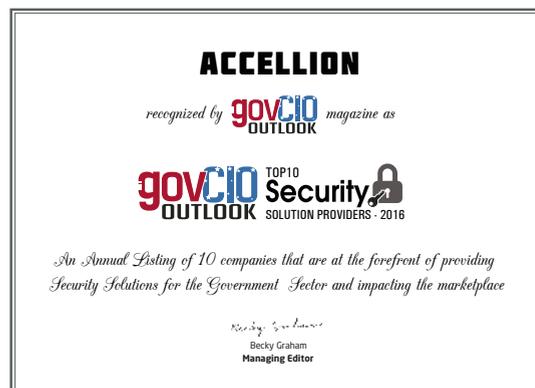le/folder expiration, two-factor authentication, remote wipe on mobile devices and desktop computers, offline PIN and app whitelisting.

> The sophistication of these attacks is increasing daily; hackers lie in wait and, once they emerge, you've got a fox in a hen house scenario

Compliance is another critical requirement for government agencies. Accellion's kiteworks has received FIPS 140-2 Level 1 validation and FedRAMP accreditation is currently in progress. NASA, the Securities and Exchange Commission, Texas State Juvenile Justice Department, City of Pleasanton and many other government agencies trust kiteworks for their secure file sharing and collaboration needs. Accellion's success serving government agencies has gained the confidence of other industries where security and compliance are paramount, including healthcare, legal, and financial services.

With mobile workflows on the rise and more sensitive data being transmitted across these devices, the stakes to preserve data authenticity are incredibly high. A data breach has become more damaging than a physical attack and Accellion finds itself on the front line helping companies preserve their most sensitive data.