TRUSTWAVE SECURITY SOLUTIONS

DATA SECURITY & COMPLIANCE MANAGEMENT SOLUTIONS FOR GOVERNMENT

Trustwave plays a critical role in the defense and safeguarding of the government cyber domain by securing all layers of networks and helping to ensure compliance with security regulations. With our comprehensive suite of data security and compliance management solutions, Trustwave secures the privacy and confidentiality of critical data for thousands of government employees and their constituents.

OVERVIEW

Trustwave enables our government customers to take a holistic approach to security risk management thanks to our long history of supporting the government. Since 1995, Trustwave has partnered with the federal government to help overcome the many challenges it has faced with implementing cybersecurity. Many initial Trustwave customers were government agencies. Trustwave learned firsthand about the changing expectations for securing information and supported early initiatives to use information security to verify and validate compliance with FISMA regulations.

Solutions for government to detect, respond to, and mitigate cyber incidents:

Security Information and Event Management (SIEM)
Our SIEM solutions collect, analyze and store logs from networks, hosts and critical applications. Trustwave SIEM solutions help government entities meet security standards and provide for a situational awareness capability for critical infrastructure. Trustwave SIEM has achieved Common Criteria validation with EAL 3+ level of certification.

Data Loss Prevention (DLP)
Trustwave Data Loss Prevention (DLP) is an inbound and outbound content control solution that enables government entities to gain complete visibility into all insider risk, whether inadvertent or malicious, and to control violations before they occur. With predefined compliance packages that specifically address government standards such as FISMA, NIST 800-53, DoD 8500.2 and the new Presidential Policy Directive 21 (PPD

21), Trustwave DLP avoids data loss that can lead to compliance violations and intellectual property loss, but can also provide the versatility to protect sensitive information.

Web Application Firewall
Trustwave's advanced, real-time Web application firewall provides defense against Web application threats, is an SC Magazine award winner and has achieved Common Criteria validation with EAL 2+ level of certification. With Trustwave's Web application firewall, government agencies can prevent their applications from being exploited by protecting against zero-day and targeted attacks, data loss, defacement and security information exposure. The solution also ensures Web applications operate as intended, are available when needed, are in compliance (e.g. PCI DSS, PII, HIPAA) and are always protected.

Network Access Control (NAC)
A network-agnostic solution, Trustwave Enterprise NAC requires no agent software and automatically performs risk assessments on all managed and unmanaged end points regardless of IP device type or operating system (OS). When an endpoint is determined to be out of policy with respect to network admissions policy, the Trustwave Enterprise NAC appliance virtually steps in to quarantine and isolate the endpoint from the network. Trustwave recently won the SC Magazine 2013 award for Best NAC (Network Access Control) product and has achieved Common Criteria validation with EAL 2+ level of certification.

Encryption
Coupled with our capabilities for discovery of sensitive and proprietary data, Trustwave FIPS 140-2 encryption provides comprehensive integrated protection of data-at-rest or in-motion. Offered as either a managed service or customer premise solution, Trustwave cutting-edge encryption travels with sensitive data wherever it traverses a government entities' network, whether through file transfer, e-mail communication or USB portable storage.

CYBER-BASED THREATS

The evolving array of cyber-based threats facing the nation poses danger to national security, commerce and intellectual property. Secured networks are essential to government in order to accomplish their missions from federal defense and civilian agencies to federal, state and local governments.

Secure Web Gateway

Trustwave Secure Web Gateway offers government agencies the most accurate protection from next generation threats and the most flexible deployment options in the industry, providing the same high level coverage to remote, mobile and on-premise users. It provides government agencies true, zero-day protection with the ability to instantly analyze the "intent" of the code and enables safe, productive access to Web 2.0 while ensuring compliance, minimizing data loss and eliminating malware risks. Centralized policy control and a single interface make the solution easy to manage—whether deployed as a traditional appliance, virtual appliance, hybrid cloud or any combination of the three.

Secure Email Gateway

Trustwave Secure Email Gateway filters all incoming and outgoing email at the perimeter and uses deep content inspection to scan all content—even within attachments. It provides total email content security through unified threat management, anti-spam, content security, policy enforcement and data loss prevention. It can be deployed as a standalone solution or as a distributed array designed to support large government networks. Trustwave Secure Email Gateway provides detailed reports that monitor usage data for security breaches and unproductive behavior.

PCI DSS Compliance Validation

For agencies that handle point-of-sale transactions, Trustwave helps government entities validate compliance with the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS is a multifaceted security standard that includes requirements for security management, policies that implement strong access control measures designed to protect cardholder data and personally identifiable information (PII). Trustwave has been selected by more enterprises for compliance—chosen more often than the next 10 service providers combined.

A TRUE PARTNER

Trustwave is a true partner to government solutions agencies in their efforts to achieve and maintain compliance with security regulations and standards which include:

• FISMA

• Continuous Monitoring

• NIST 800-53

• DOD 8500.2

• Situational Awareness

• HIPAA

• Protection of PII

• BYOD

• PCI DSS

• FIPS 140-2 Encryption

• Zero Day

• Presidential Policy Directive 21

• Executive Order—Improving Critical Infrastructure Cybersecurity

Trustwave®

Smart security on demand

For more information: https://www.trustwave.com.