SAFEND DPS FOR GOVERNMENT OFFICES

Whitepaper

safend

a SuperCom company

DO YOU KNOW WHO KNOWS WHAT YOU KNOW?

When others play at I Spy, your information doesn't need to be an easy target. Today's statistics show that government offices everywhere are potential candidates for more technologically-advanced threats on their data, its usage and security. Some more than others.

Bringing additional demands on government personnel and introduced to protect sensitive information, these threats have generated stringent internal regulations together with requirements to comply with major standards like GDPR EU.

Whether inter-office, country news or secreted to external parties, when considering data protection solutions a major need is to know exactly where data is most open to leakage.

Classified, secret, top secret, what are the main threats?

- Unauthorized access to protected and unprotected data
- Innocent provision of information related to lack of knowledge or negligence
- Extortion or forced handover of sensitive information
- Accidental or intended data leakage via endpoints: ports and USB storage devices, key loggers, BOYD and other external devices like CDs, DVDs and printers
- Introduction of viruses, Trojan horses or worms via endpoints like USBs or key loggers and the internet
- Trafficking and external use of stolen sensitive data
- City development, including planning permissions, tenders, future developments or legal actions
- Financial information related to employees, residents or municipal projects like payment methods or credit card numbers

What are the repercussions?

- Threat to the safety of a country and its civilians
- Malicious control of classified, secret and top secret government data networks
- Possession and use of civilian personal details and information
- Irreparable damage to a country's integrity and image
- Damage to ties with friendly countries
- Increased hostility with unfriendly countries
- Trafficking and reusing stolen/modified information
- Countless waste of time and money spent handling successful attacks

THEY WILL LOOK BUT THEY WON'T SEE CHALLENGES

Holding a country's past, present and future prized information, government databases are extremely interesting to hackers, organized groups and insiders looking for what they need. Often thriving in-tandem, data-theft technologies bring growing challenges to data-protection providers in their endeavour to remain that one step ahead. This includes complying to standards, controlling access to sensitive data files and folders, data encryption and how and where information is saved and downloaded to. Other integral requirements are use of external devices and remaining alert and in the loop by continual analysis of the solution's services.

Remaining updated with regulations and world compliancy standards

- Understanding and complying with internal government regulations
- Understanding and complying with local and international standards like GDPR EU
- Understanding and complying with standards in other friendly countries

A few facts and figures

- UK Ministry of Defense (MOD), 2016: Up to 831 members of Britain's defense community with high-level security clearances had their personally identifying information stolen when the Ministry of Defense's business networking organization was hacked
- Philippines Voter Registration System, 2016: believed to be one of the biggest data breach in Filipino government history personal information of 55 million Filipino voters was leaked and made available on the wehaveyourdata.com website
- US Office of Personnel Management (OPM), 2015: the largest government-targeted data breach ever, stealing an estimated 21.5 million people's personal information. This includes employees, former employees and people with background checks
- Bundestag (German Government) 2015: confirmed that hackers that attacked the Bundestag and accessed data from a targeted network

Where is sensitive data most open to threat?

- Endpoints on computers, laptops and mobile devices
- External media like USB storage sticks, hardware key loggers, CDs and DVDs
- During its transfer

Knowing where sensitive data is at all times

- Defining strong access permissions
- Preventing good people from doing bad things
- Preventing bad people from doing bad things

How to prevent stolen data from being used

- Defining which information can be uploaded to where
- Encrypting sensitive information
- Encrypting laptops and devices

HOW SAFEND DPS ANSWERS DATA PROTECTION DILEMMAS

Common Data Protection Dilemmas

- Finding a solution that works and that does not disrupt daily activities
- Finding a cost-effective and granular solution
- Understanding municipal privacy standards
- Understanding compliancy requirements like GDPR EU
- Overcoming integration pains
- Defining profiling, policies and exceptions

More facts and figures

- Vista Research: 70% of data leakage originates from within an enterprise
- Forrester: 52% of large North American enterprises lost confidential data through removable media like USB drives
- IDC: over 60% of confidential data resides on endpoints
- Ponemon Institute: over 16,000 laptops are lost each week by in-transit business men and women in USA, Europe and UAE

Silent operation without disrupting daily activities

The Safend DPS Data Protection for Municipalities solution is based on the Protector, Encryptor and Auditor modules which balance between productivity and performance without interfering with daily work activities.

When installing DPS onto a network, accurate analysis of data protection requirements are assessed. This enables building policies and their exceptions, profiling and adding user / machine permissions also regarding the use of USB storage drives and other external storage devices.

As a granular suite, monitoring and controlling the information flow on your municipal endpoints, DPS enforces these policies, permissions and exceptions as it protects, encrypts, audits and generates reports on use of ports and devices. For example, when uploading an Excel file to a CD - an external device - which is an exception to a policy blocking use of all external devices.

Cost-efficiency, leaving room for future growth

Integrating Safend DPS into your municipality's data network helps side-step costs associated with data leakage through unprotected endpoints. Safend DPS currently has the capacity to support over 250,000 endpoints via one environment.

Understanding compliancy requirements

Safend DPS already meets EU GDPR standards and as a customizable solution, can make necessary provisions should modifications be required. DPS also answers additional major compliance requirements like SOX, HIPAA, PCI, FISMA, BASEL II, UK Data Protection Act (DPA) and other stringent standards.

Overcoming integration pains

Safend DPS is designed for comprehensive installation and can be installed by both Safend certified experts or by your municipal systems administrator. Depending on the solution's requirements, the entire integration process should take a short time.

Safend DPS profiles, policies and exceptions

Prior to server installation, DPS can pinpoint the usage of USB, FireWire, PCMCIA, PCI, internal storage and WiFi connections at your municipality. Using this information provides administrators the knowledge they need to create enforced companywide preventative policies, permissions and exceptions.
This may include blocking all external devices and then assigning exceptions to different users / devices, or that specific information only can be uploaded to an external device.

Safend DPS offers the following options:

- Blocking / enabling data transfer
- Blocking data transfer and collecting information
- Blocking data transfer without collecting information
- Enabling data transfer and collecting information
- Enabling data transfer without collecting information

One Data Protection Suite, One Data Protection Agent

Built as a suite of data protection modules, DPS protects your information as it controls, encrypts, monitors and updates you about its whereabouts throughout its lifecycle.

Safend Data Protection Suite Modules

- Protector: controlled port and device endpoints and media encryption
- Encryptor: transparent encryption on laptops and PCs
- Auditor: immediate risk detection on WiFi ports / devices connected to endpoints

Protector, port and device endpoints control

A flexible and intuitive solution with strong rule-based file encryption capabilities, Protector averts inappropriate use of smartphones, digital cameras or memory sticks. Protector enables creation of highly granular and customizable security policies which automatically detect, permit and restrict files and selected devices according to levelled user permissions, type, model and serial number.

Encryptor, full data hard disk encryption

A full encryption solution for municipal information, Encryptor blocks inappropriate access or transfer of information. As it secures an organization's endpoints, Encryptor immediately alerts administration on all intentional / unintentional data leakage incidents.
Always one step ahead of existing and new data hacking technologies, Encryptor already protects data at rest and can cover 250,000 endpoints.

Auditor, pinpointing the real picture

Having the capacity to run on up to 60,000 computers, the clientless Auditor pinpoints usage of USB, FireWire, PCMCIA, PCI, internal storage and WiFi connections on your network. Auditor searches for information according to Microsoft Active Directory architecture, IP Range and Computer Name and is successfully integrated into the Protector.

SAFEND DPS, KEEPING YOUR COUNTRY'S DATA SECURELY SECRET

Understanding where the security challenges are and by introducing proven solutions, Safend DPS protects your government's endpoints as it monitors, encrypts and updates you on where your data is and who is using it.
Safend DPS is very stable and built comprehensively and once integrated into your network, runs automatically without interrupting daily activities.
Designed as a robust solution for port and device control with a strong anti-tampering mechanism, Safend DPS has built-in compliancy provisions, including for GDPR EU, PCI, HIPAA and SOX.
Safend is already used as a cost-effective data protection solution at major government facilities who have integrated it into their network to protect their sensitive information.