

Sensitive Data Requires Protection

With today's expanding mobile workforce, data security and data protection are top priorities for Chief Information Officers and IT management in both the public and private sectors. Additionally, significant returns-on-investment can be realized through data loss prevention, encryption and monitoring of data at rest (DAR) and data in motion (DIM). To reduce data leaks caused by negligence and theft, Intelligent Decisions (ID) has developed a seamless, integrated approach that supports the complexity of your organization's security needs while reducing vulnerabilities and IT costs.

ID's Solution

Intelligent Decisions has positioned itself like no other company in the IT security industry by offering comprehensive data protection solutions that include hardware, software and a full range of professional services for implementation and ongoing maintenance. Through partnerships with industry-leading security companies, our trained security professionals will work closely with you to assess, design, procure, implement and maintain your complete solution.

ID's Professional Consulting Services utilize proven best practices coupled with best-in-breed automated, security tools so you can be assured of maximum protection at competitive prices. Our end-to-end solutions-

- Accurately detect policy violations
- Qualify and quantify the risks associated with data loss and their impact on intellectual property and sensitive customer data
- Protect and secure both data at rest and data in motion
- Scour network communications for sensitive data

Data Protection Security Solutions from Intelligent Decisions address the following Federal initiatives:

- SP 800-53A
- HIPAA
- OMB M-06-16
- OMB M-06-19
- Federal Information Security Management Act Implementation Project (FISMA) Initiatives
- DOD's guidance on protecting Personally Identifiable Information (PII)

Data Security

Today, with more business conducted outside the office perimeter, there is an absence of physical security controls over data in motion (DIM). Existing intrusion detection, prevention and management solutions may provide adequate security behind your organization's firewall do little to reduce exposure and risks related to employees transporting information or accessing data remotely. Consequently, network boundary exposure becomes even more difficult to protect. ID's data protection solution minimizes risks and grants you piece of mind knowing that your data is being fully protected and secured from any access point.

ID's complete mobile security solution for DIMs :

LAPTOP

- Encrypts Communications
- Encrypts Files
- Encrypts Removable Media
- Secures Applications
- Maintains Machine Currency

NETWORK

- Views Policy Violations
- Scans Outbound Email Traffic
- Prevents Malicious Behavior
- Encrypts Communications

SERVER

- Secures Machines
- Checks for Vulnerable Information
- Enforces Secure Documents
- Maintains Machine Currency

MOBILE DEVICE

- Encrypts Communications
- Encrypts Files
- Encrypts Removable Media
- Secures Applications
- Maintains Machine Currency

Security Services Methodology

ID has created a comprehensive security services methodology to assist in achieving your security goals. The process begins with a data assessment to evaluate data leakage rates and vulnerabilities. Then ID creates an all-inclusive, comprehensive security plan for your review and approval. After approval, ID develops a procurement, implementation and management plan that has been tailored to meet your strategic security objectives. Also, ID provides operations and ongoing maintenance to ensure timely and efficient post-implementation success. Lastly, to complete the final stage of data security and protection, ID offers a full range of media destruction services that enables you to correctly dispose of sensitive media devices in compliance with federal and state regulations.

Data at Rest (DAR) & Data in Motion (DIM)

It is essential that all data within your organization be protected with sophisticated security tools and comprehensive policies thereby enabling you to meet all of your security requirements. IDSecurity provides protection of your data when it is in the confines of your organization or at rest on a mobile device. DAR is protected while sitting on laptops, desktops, shared file servers and web servers by our complete security architecture. The IDSecurity architecture-

- Searches network communications for sensitive DAR and protect it through authentication encryption
- Monitors all information stored on devices
- Protects data from rouge devices and data leakage through access control and user permissions
- Enforces ongoing compliance of security policies
- Reports and audits data vulnerabilities
- Monitors DIM (email, webmail, IM, file transfers, web postings and other sessions) for data leakage
- Recovers loss data

More business is being conducted outside of the office which leads to an absence of physical security controls over large amounts of data. Existing intrusion detection, prevention and management solutions may provide adequate security behind your organization's firewall, but do little to reduce exposure and risks related to employees transporting information or accessing data remotely. IDSecurity detects what information is considered sensitive and automatically encrypts it. So whether you are sending an email, file sharing, posting something on the web or IM'ing, IDSecurity minimizes risks and grants you piece of mind knowing that your data is being fully protected and secured from any access point.

These protective controls provided by ID will ensure that your data will be encrypted and secure while using various mobile devices:



What makes this solution so appealing is its simplicity. Employees can "point, click, and encrypt" files with an enforced password to ensure that sensitive information remains confidential when transferred to any mobile device. Also, Information Management teams can monitor successful and unsuccessful logins, times of updates, encryption start and end times and security policy enforcement.

SOLUTION HIGHLIGHTS

- Protects sensitive information and enforces employee privacy safeguards
- Discovers confidential data at rest and monitors confidential data in motion
- Detects breeches across all content groups
- Automates policy monitoring / enforcement, encryption visibility / control and response workflow
- Provides auditing and compliance reporting
- Reduces financial risks
- Ensures global scalability and supporting architecture
- Integrates with existing CCL
- Provides real-time and historic views of data access
- Eliminates unnecessary integration, administration and training