DataStealth

Security v Compliance

Datex

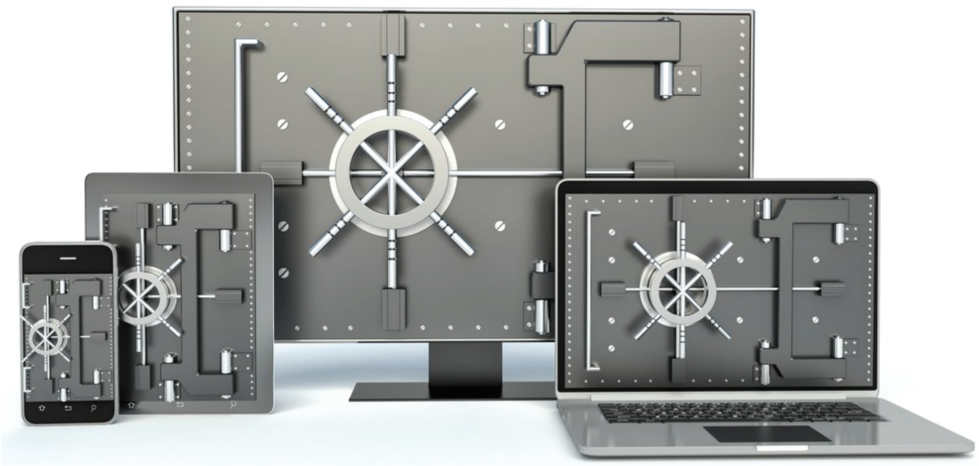
If you are only concerned with regulatory compliance for its own sake, and not for the sake of security and privacy, you are already in trouble.

Organizations around the world are being breached at a near constant, almost epidemic rate. It is becoming very clear that avoiding attack is shortsighted, because it is not a question of IF your network will be breached, but rather WHEN it will be breached. Public attitudes about data privacy are evolving rapidly as customers have started voting with their wallets, showing that tolerance is at an all-time-low. Organizations that are unable to provide a secure environment for sensitive, private or confidential data are being shunned as a provider of choice, while customer bases erode quickly.

To complicate matters, there is a plethora of different, often overlapping security standards and regulations to which an organization must adhere, some of which depend on the jurisdiction. It can be difficult and daunting to choose an appropriate strategy and starting point, let alone solve the problem with any confidence. While privacy and security were historically encouraged through policy and best practices, Forester has recently stated that half of all enterprises now view privacy and security as competitive differentiators.

Heidi Shey, a Forester analyst, stated that: “How you handle private and confidential data may spell the difference between consumer loyalty and business disaster”. More astute organizations are making efforts to earn customer trust by ensuring that data security and privacy are top priorities for their business, and that both are included in their agendas or mission statements. So how do you get your infrastructure secure? Meet DataStealth.

DataStealth is an inline security appliance that removes private and confidential information from data and documents, on the fly, in real-time. It requires no application development and no end user changes. Once it is deployed in your environment, all of your private and confidential information is removed at the point of ingress. When your network is breached, intruders will have nothing to steal. With DataStealth, intruders cannot steal what is not there.



PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

DataStealth is compliant with PCI-DSS 3.1 Service Provider Level 1, evidenced by our annual third party audit. This is the highest level of compliance available under the PCI DSS standard. DataStealth will uplift your entire downstream environment to a status of compliant. And to ensure you sustain your PCI compliance, DataStealth will remain in place, continually monitoring your streaming data and documents, automatically acting on any relevant information that is detected.

NIST

The National Institute of Standards and Technology is a non-regulatory government agency that develops technology, metrics, and standards to drive innovation and economic competitiveness at organizations in the technology industry. As part of this effort, NIST produces standards and guidelines to help organizations protect their information and information systems through cost-effective programs

NIST helps organizations meet the requirements of the Federal Information Security Management Act (FISMA) by helping to develop Federal Information Processing Standards (FIPS) in congruence with FISMA. NIST also provides guidance documents and recommendations through its Special Publications (SP) 800-series. NIST is a key resource for technological advancement and security at many of the country's most innovative organizations. As such, compliance with NIST standards and guidelines has become a top priority in many high tech industries today.

DataStealth was built on top of a 100% NIST compliant environment. As each iteration of DataStealth is released, we ensure that the NIST compliant status remains at 100%.

CIS

The Center for Internet Security (CIS) provides CIS Controls for effective cyber defense, a recommended set of actions that provide specific and actionable ways to stop today's most pervasive and dangerous cyber attacks. The CIS Controls are especially relevant because they are updated by cyber experts based on actual attack data pulled from a variety of public and private threat sources. CIS incorporates recommended changes from the cybersecurity community to reflect the latest technologies and threats including email and web browser protection, secure network engineering, and controlled use of administrative privileges.

We are a member of CIS and follow their guidelines and recommendations for secure configuration standards. We use various benchmarks and evaluation tools (i.e. CIS-CAT) that are applied and executed for all applicable components to ensure the effectiveness of internal security controls and processes.

Qualys

Qualys provides global visibility into IT systems, where they might be vulnerable to the latest Internet threats, and how to protect them. Qualys helps businesses simplify IT security operations, and compliance efforts, by delivering critical security intelligence on demand. Qualys automates the full spectrum of auditing, compliance and protection for perimeter systems, internal networks, and web applications.

DataStealth has deployed Qualys for continual and ongoing vulnerability management, solution monitoring, web application scanning, penetration testing, and other scans and services.

OWASP

The Open Web Application Security Project (OWASP) is an online community which creates articles, methodologies, documentation, tools, and technologies in the field of web application security. OWASP seeks to educate developers, designers, architects and business owners about the risks associated with the most common Web application security vulnerabilities. OWASP has become known as a forum in which information technology professionals build expertise. OWASP tools, document and code library projects are organized into three categories:

a) tools and documents for security-related design and implementation flaws,

b) tools and documents for guarding against security-related design and implementation flaws,

c) tools and documents that can be used to add security-related activities into application lifecycle management.

Datex Inc.

2333 North Sheridan Way

Suite 200

Mississauga ON L5K 1A7

www.datex.ca

+1 855.55.DATEX