SECLORE™

DATA SHEET

DIGITAL ASSET PROTECTION & CONTROL FOR THE SEMICONDUCTOR INDUSTRY

Seclore's data-centric protection platform provides persistent document and data protection that extends beyond boarders

Introduction

Globalization has had a profound impact on the semiconductor industry. In the 1980s, many companies began establishing factories in Southeast Asia and Eastern Europe to take advantage of low-cost labor and other benefits. This globalization of the industry has led to increased competition, as well as new opportunities for growth and innovation.

Today, the semiconductor industry is vital to leaders across sectors of the global economy. The chips produced by this industry are used in a wide range of products, from computers and cell phones to automobiles and medical devices. As such, the health of the semiconductor industry is crucial to the success of many businesses worldwide.

The semiconductor industry is one of the most highly regulated industries in the world. Companies operating in this space must comply with various domestic and international regulations. This can be challenging as the rules are constantly changing and evolving.

INDUSTRY USE CASES

Where Your Security is Failing

Collaboration requires exchanging confidential information outside your security infrastructure and corporate and national boundaries. It involves sending information such as technical specifications, design data, financial projections, and so on to external parties outside the organization that you cannot control, no matter how much you try.

Protecting Intellectual Property

Electronic component manufacturers work with a supply chain of vendors for procurement and contract manufacturing.

Different teams often share confidential material with external agents such as advertising agencies, graphic designers, vendors, and dealers. The organization also shares project bids containing the pricing structure and material costing with other stakeholders, both within and outside the organization. Negligent or malicious leakage of such Intellectual Property can seriously threaten the organization's margins and competitive edge.

Design Specifications

Companies manufacturing electronics for federal government agencies depend on semiconductor manufacturers to deliver new and improved components for their ongoing requirements.

They provide these manufacturers with their latest designs and specifications, which become a liability towards security and secrecy. Protecting this information before it is accessible to internal employees is key to covering the liability of sharing it within the company.

Protect your sensitive data from unauthorized access

$8.86M Annual cost of Insider threats for the manufacturing industry (USD)

209 Cyberatttacks suffered by the semiconductor industry, including privacy breaches

55% of integrated chip (IC) manufacturers have reported counterfeited versions of their products

83% of security professions believe that employees expose sensitive data in their organization

3.7 how often businesses suffer a disruption that lasts one month

Employee Data

Organizations outsource the employee background verification process to external agencies that share employees' confidential information. These records contain sensitive information such as Personally Identifiable Information (PII), Personal Health Information (PHI), and travel data. The employee travel information often resides within the internal portal. The HR department also shared the PII with the Finance department and the banks for employee salaries.

Financial Data

Corporations applying for large loans send their confidential data (financial information, business models, and revenue projections) to help the bank analyze credit risk. Credit analysts analyze the data and decide on an appropriate lending rate of interest and other loan conditions. Leakage of any of this sensitive information can land the organization in lawsuits and cause a loss of market reputation.

Operational Reports

Confidential Operational and MIS reports represent another significant security risk if they fall into the wrong hands. Operational reports may contain financial data, corporate statistics, sales information, and equipment utilization, which are highly sensitive. These documents are vital in planning business strategies and should be shared strictly on a need-to-know basis.

Mergers & Acquisitions

Semiconductor companies undertaking M&A activities need to be especially vigilant about data security. Semiconductor IP is among the most valuable and sensitive information and is likely to be leaked during an M&A transaction.

Organizations use Virtual Data Rooms (VDRs) to share data related to M&A activities. VDRs are cloud-based repositories offered by third-party vendors. Although considered a secure mechanism, the data remains outside the organization, not governed by the organization's governance policies.

Customer Stories

US-Based Largest Wireless Semiconductor Company Protects COVID-19 Case Logs to Achieve HIPAA Compliance

The COVID-19 case log files are created by the HR team and shared with particular groups for insurance or administration purposes. The employee's medical information is sensitive data with a high risk of getting compromised. The California Division of Occupational Safety and Health ("Division"), also knows as Cal/OSHA, issued guidance for employers in California to maintain and report COVID cases to Cal/OSHA. Seclore controls access to these records and prevents unauthorized medial data sharing insight and outside the organization.

Secure External Collaboration for a Leading Semiconductor Capital Equipment Manufacturer

Multiple teams would share data with third parties and customers using collaboration platforms like Box, OneDrive, and SharePoint on-premise. The company wanted a solution enabling their teams to share extensive data securely. They wanted to automate the workflows to secure documents and dynamically assign appropriate controls based on the sensitivity of the data. They also wanted the solution to be integration-ready with multiple collaboration platforms for easy data sharing. Seclore's data-centric security and seamless integration with existing solutions ensured frictionless workflows without compromising security.

Securing Your Information Inside and Outside the Perimeter

Your data is already at risk of exposure by the employees of the manufacturing organization. However, the risk increases dramatically when confidential information travels to third parties outside your security. The semiconductor industry needs a new approach to ensure holistic data protection and high usability.

To mitigate your information security risk, consider the following three tenets:

- Maintaining security and control of information wherever it travels – inside and outside the organization
- Preventing unauthorized users from accessing and misusing the information
- Maintaining complete visibility over all activities performed by all users – employees and third parties – on all sensitive information regardless of where it is stored.

The semiconductor manufacturer must extend its security and risk management infrastructure to its vendors, advisors, sub-contractors, and partners.

About Seclore

Protecting the world's sensitive data wherever it goes. Seclore protects and controls digital assets to help enterprises close their data security gap to prevent data theft and achieve compliance. Our data-centric approach to security ensures that only authorized individuals have access to sensitive digital assets, inside and outside of their organization. Enterprises can set automated policies and enable users to control and revoke who has access, what access they have, and for how long. Learn why leading enterprises like American Express and Applied Materials choose Seclore to protect and control their digital assets without sacrificing seamless collaboration and data sharing. Visit www.seclore.com for more information.

SECLORE™
info@seclore.com
www.seclore.com