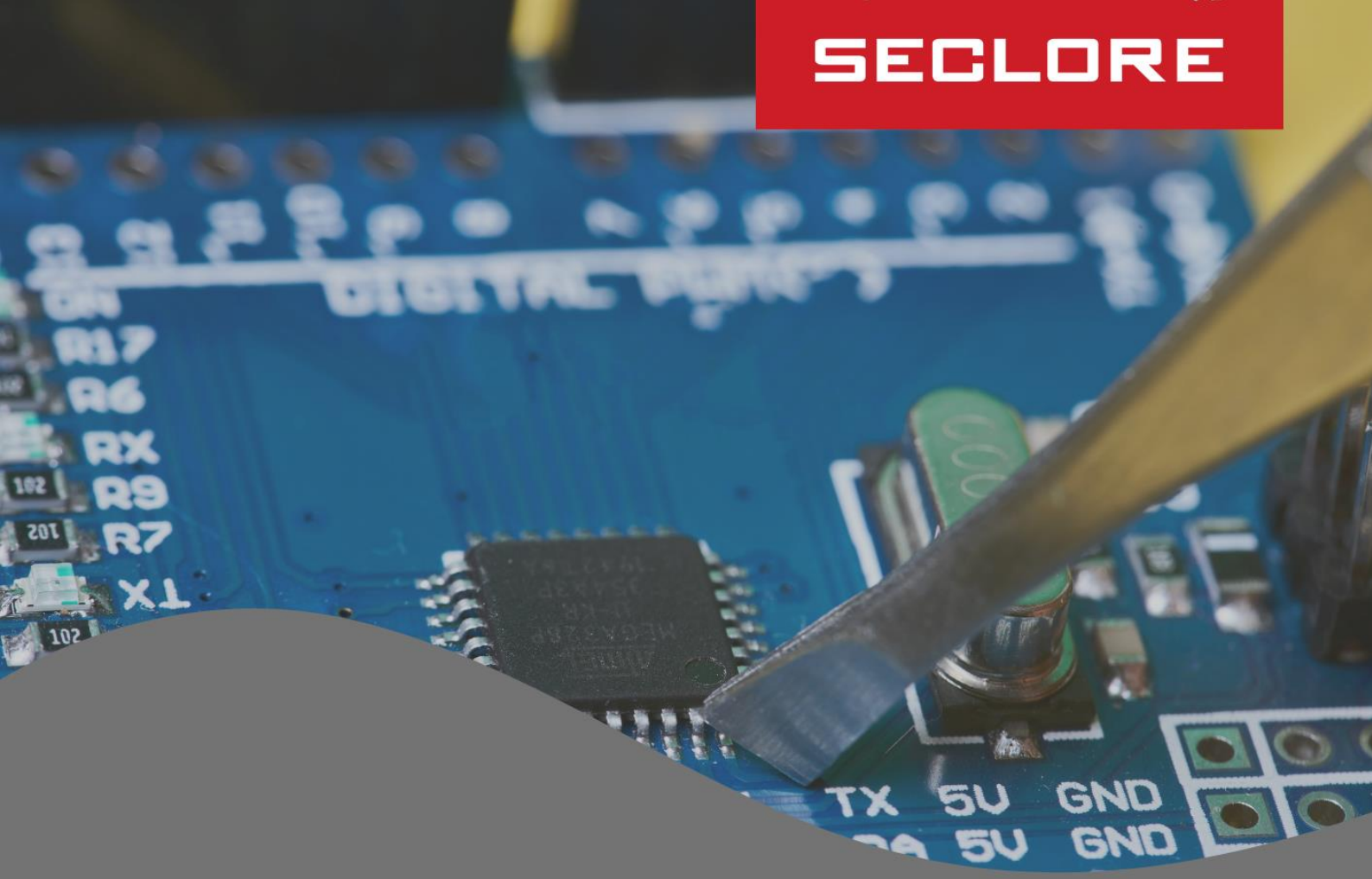
SECLORE



Digital Asset Protection & Control

for the Semiconductor Industry

Seclore's Data-Centric Protection Platform provides persistent document & data protection that extends beyond enterprise borders

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.

PROTECT YOUR SENSITIVE DATA FROM UNAUTHORIZED ACCESS

Manufacturing organizations pay **$8.86 million annually** as a result of **insider threats**

Semiconductor industry has suffered a **290 cyberattacks** including data privacy breaches

55% of Integrated Chip (IC) manufacturers have reported **counterfeited versions** of their products

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

Businesses suffer disruptions lasting one month every **3.7 years**

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.

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.

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.

The Problem with Traditional Perimeter-based Security Tools

A serious loophole in traditional "perimeter-centric" security measures is that they focus on everything except the actual information stored in documents. Firewalls secure networks, Virtual Private Networks (VPNs) secure the transmission channel, encryption tools encrypt the device or the folder – and so on. These traditional security systems certainly reduce risk – but only inside your enterprise. What is protecting the information in this entire stack without a dependency on the network, device, or platform?

Once your confidential files leave the perimeter to support external collaboration, they also leave the jurisdiction of your traditional security solutions. These files are free to move about without any protection or security. In addition, perimeter-based security is not information-centric: the information owner has no visibility over who is accessing the document and what the recipient is doing.

Today's information-sharing environment calls for a radical shift in mindset to cope with external collaboration and the ability to adopt new technologies. Traditional perimeter-based security measures –focusing only on securing the organizational perimeter– are not enough. Although necessary, these solutions only partially reduce the risk of data leakage. What is needed is an information-centric approach to security. A file can reside anywhere – on the cloud, on any device, with any team or organization – and will continue to be protected. We are talking about a

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 known 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 medical data sharing inside 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 unperturbed workflows without compromising security.

security mechanism that firewalls the file so that access to the information remains restricted and controlled regardless of transmission medium or storage mechanism.

Seclore's Data-Centric Protection

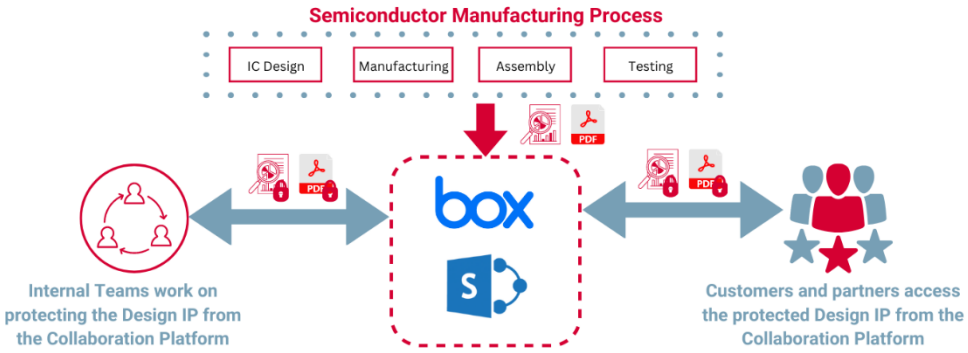
Many organizations are looking at how to build a Data-Centric Security infrastructure to efficiently eliminate security gaps, especially in light of new regulations. Regulations, such as ITAR/EAR, NIST, etc., require sensitive data to remain protected, whether the data is in your custody or an authorized third party's custody. Unfortunately, many current Data-Centric Security tools work in isolation (e.g., Data Loss Prevention, Rights Management, and Data Classification) and only partially meet these security regulations requirements.

A comprehensive Data-Centric Security strategy includes four essential components: Discover, Identify, Protect and Analyze. The tools to perform these functions include Data Loss Prevention (DLP), Data Classification, Rights Management (RM), and Security Information and Event Management (SIEM) systems.

Seclore's Data-centric protection consists of three aspects:

- **Authentication**: No unit of sensitive information is accessible without stringent user authentication.
- **Authorization**: Only the file owner decides who can access their information and who cannot. They can also first grant access and later revoke it if required.
- **Auditing**: The file owner can track their data's journey and get detailed audit logs to detect unauthorized access.

Seclore's Data-Centric Protection successfully mitigates security risks and allows you to collaborate with external parties, adopt innovative technologies, and achieve business objectives – without worrying about security.



About Seclore

Seclore is the data protection platform securing the enterprise's digital assets wherever they go. The platform allows organizations to use best-of-breed solutions to discover, classify, protect, and track enterprise data within and outside the organization’s boundaries. Over 2000 companies and government organizations in 29 countries use Seclore to achieve their data security, governance, and compliance objectives.

Learn how easy it is to keep your most sensitive data safe and compliant.

Contact us at: info@seclore.com or CALL 1-844-4-SECLORE.