CUSTOMER SUCCESS STORY

Multinational Semiconductor Company

MANUFACTURING

Industry
- Semiconductor design and manufacturing

Environment
- 12,000 workstations
- Linux
- Windows

Challenges
- Comply with ITAR regulations that prohibited foreign nationals accessing export-controlled designs
- Integration with multiple source code control, CAD and simulation applications
- Allow, but control, internet access for users
- Monitor activities of foreign nationals

Results
- Enterprise-wide discovery of export controlled information
- Over $4 million in annual savings from duplicate facility consolidation
- Improved productivity through enabling access to designs from any location
- Achieved virtual network segmentation and a more streamlined physical
- Infrastructure
- Identification, arrest, and prosecution of foreign national attempting to steal designs

DIGITALGUARDIAN™ by VERDASYS

Export Control Compliance, Improved Productivity and $4 Million Annual Cost Savings

A global leader in the design and manufacturing of semiconductors faced a difficult challenge. With facilities worldwide, it relied on the engineering expertise of employees in several countries. However, because of their advanced designs and potential uses, many individual components within their products fell under the requirements of the International Traffic of Arms Regulations (ITAR).

ITAR compliance meant that only US citizens could view the layout of these export-controlled components. This requirement forced segmentation of the company's workforce and reduced productivity. Designs from the overseas centers were shipped to a separate US facility, where US citizens could integrate the work into the chip design and build process.

> "Digital Guardian enabled our global users to be more productive and our operations to run more effectively while meeting ITAR compliance."
>
> **Director, Worldwide Security**

THE BUSINESS CHALLENGE

The semiconductor market is highly competitive, and rapid time-to-market is critical.

ITAR restrictions complicated the company's development process. The company's engineers accessed all chip designs through several different source code control, CAD, and design verification applications. The classification of data varied, often even within individual design documents. Some components were viewable by all users, while others were subject to ITAR restrictions. Simply classifying an entire design in a least-privilege manner would not work. The manufacturer needed a solution that could apply policies to the individual components within a design document.

To improve its competitiveness, the customer required secure collaboration between users at any of their locations, while protecting ITAR-regulated components from disclosure to foreign nationals.

CRITICAL SUCCESS FACTORS

- Any user, from any machine, must be able to access design data, while having the appropriate policy applied to the individual components within that document or file
- Greater visibility into all data movement and a forensic trail proving that no foreign national had access to export-controlled data

DIGITAL GUARDIAN FACTS

Customers
- Over 250 customers
- 130 of the Global 2000 and government agencies
- Used by 7 of the top 10 patent holders
- Over 2,100,000 endpoints protected
- Only solution to scale to 250,000 agents

Information Discovery and Classification
- Context-based data awareness
- Content inspection
- User classification
- All content is tagged with permissions
- Permissions persist through reuse, renaming
- Over 300 data types
- 90 languages

Response Options
- Monitor, log, report
- Prompt, justify, and report
- Block and report

Supported Platforms
- Desktop/Laptop
- Server
- Network
- Virtual
- Supports devices on network and off network

Supported OS
- Microsoft Windows®
- Linux
- Mac OS X®

Deployment Models
- On Premise
- Managed Security Program (MSP)
- Hybrid MSP

DIGITALGUARDIAN™ by VERDASYS

www.digitalguardian.com

- Enforcement of the controls on foreign nationals must not break the functionality of design software and simulation applications
- Allow internet access to the manufacturer's full resources within each facility, but strictly control their use

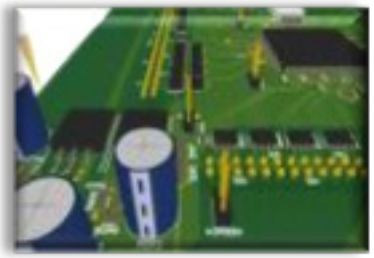
THE SOLUTION

The Digital Guardian services personnel reviewed the design applications, using Digital Guardian's contextual awareness classification and policy indentification to automatically classify, and report on the presence of ITAR-restricted components residing on servers, desktops, and laptops across the enterprise.

Foreign National View

Once data was classified properly, Digital Guardian's "masking" policy could obfuscate ITAR-regulated components from foreign nationals while allowing complete visibility of other fields and components. The masking policy also recognized users who were US citizens and allowed viewing of all components.

US Citizen View



Prior to deploying Digital Guardian, internet access was denied to employees working on sensitive designs due to security concerns, and cooperation between facilities suffered. Digital Guardian worked with the organization to create policies allowing controlled internet access through the company's virtual private network (VPN). Since Digital Guardian can distinguish a public from a private network, remote employees could still access the internet. Digital Guardian allowed users to reach a login page for a private network (such as a hotel's network), but then required the user to connect to the company's VPN to reach any other URL, while monitoring and logging all data activity.

THE RESULTS

Digital Guardian greatly improved productivity and competitiveness. Masking policies with user-level controls provided foreign nationals with the information they required to complete and test designs, without exposing ITAR-restricted components. This eliminated the need for physical segmentation of foreign nationals and US citizens, and duplicate infrastructures. The customer estimated that this benefit alone saved $4 million annually.

Digital Guardian's ability to allow controlled internet connections enabled the company to provide internet access to offshore workers, while forcing connections through the organization's VPN. This provided a valuable, yet safe communication link with workers in the US.

The productivity gains were quickly visible and popular with the company's employees. On a site visit, local employees thanked the manufacturer's CISO for implementing the Digital Guardian solution. Further proving its value, Digital Guardian provided alerts when a foreign national attempted to steal sensitive data on behalf of a competitor. The company successfully prevented the theft and prosecuted the individual thanks to Digital Guardian's evidentiary forensics.