CUSTOMER SUCCESS STORY

DIGITAL GUARDIAN®

Gaining IP Visibility and Control Without Impacting Endpoint Performance

About the Customer

This customer is one of the world's largest companies dedicated to industrial automation, producing hardware and software that helps their customers be more productive and efficient. The company spends more than $300 million on R&D each year that results in high-value IP that is their competitive differentiator.

The Business Challenge

Research and development is the lifeblood of the industrial automation market. Should a competitor gain access to the company's IP, their competitive advantages could be irreparably damaged. A hacker gaining access to the IP increases the chance of compromising the software, damaging their reputation and putting customer's assets and businesses at risk.

The company's Chief Information Security Officer, began looking for a solution to protect their critical IP after becoming increasingly concerned about industrial espionage from both domestic and foreign sources.

The first priority was to protect was the company's engineering resources; software source code, design documents, and trade secrets. But while protecting IP was critical, the solution needed to be non-invasive. Engineers designing and testing complex software cannot have their devices slowed down, nor can they interrupt normal workflows. Changes to workflows and additional approval processes would negatively affect employee productivity and adoption. In addition, the company needed a solution that integrated with their existing infrastructure and privilege management systems.

Critical Success Factors

- Provide complete visibility to the targeted IP at all times
- Integrate with existing internal environment and outsourced IT infrastructure
- Zero impact on endpoint performance
- Free up internal security resources
- Collaborative partner from pilot to full rollout

Industry

- Manufacturing, Technology

Environment

- 5,000 workstations
- Privileged users and software engineers
- ClearCase source code repository
- Splunk SIEM in the cloud

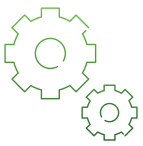
Challenge

- Threat from sophisticated adversaries
- Low impact on endpoints
- Integration with existing infrastructure
- Solution provided "as a service"
- Competing vendor claims required a trusted partner

Results

- Full visibility and control over critical IP
- Fully integrated with ClearCase and Splunk
- MSP solution rolled out to 5,000 endpoints
- A vendor-client partnership built on openness

Data Types We Protect



Advanced Engineering

- Source Code
- Designs
- R&D Data
- Supplier Contracts

Contract Manufacturers

- Customer IP
- Component List
- Business Processes
- Customer Contracts

Aerospace/Automotive

- Design Specifications
- CAD Drawings, Blueprints

The Solution

After an extensive selection process, the company determined that Digital Guardian provided the best mix of visibility to IP, control over information movement, and low impact on the endpoints and users. The Digital Guardian team worked side by side with the company's subject matter experts to develop policies and ensure that they had full buy-in to each step in the pilot.

Work started with the engineering teams that used IBM® Rational® ClearCase® to manage their software assets. Digital Guardian automatically classified all information stored in ClearCase®, avoiding the often tedious and error prone task of manually classifying IP. Integration with Active Directory® allowed Digital Guardian to understand and "inherit" the permissions of each user. This ensured that each engineer had unimpeded access to the files they required to do their jobs, while blocking access to IP for which they lacked permissions. Finally, integration with Splunk allowed the company's outsourced IT vendor to process Digital Guardian alerts using existing methods.

Initially, the company wanted visibility to the IP and an understanding of how users moved the information. Automatic classification along with Digital Guardian's endpoint Agents and reporting and analytics interface provided this immediately. The next step was to reinforce company policies through soft blocking; DG generated prompts to notify users taking unauthorized actions. Finally, full blocking that enforced appropriate use policies and alerts to actions that could put IP at risk provided the controls the company required.

The Results

Digital Guardian was deployed across 5,000 endpoints. The CISO gained the visibility into the risks to the company's IP and applied controls to policies that had previously been unenforceable. Digital Guardian's MSP provided the support the company desired without the overhead of additional IT staff.

> *"The pilot solution perfectly aligned with our requirements and clearly excelled through our formal selection process."*
>
> **- Senior Manager, Technical Security Strategy**

About Digital Guardian

Installed Based

- Over 700 customers from across the globe
- Industries served: Business services, education, energy, financial services, government, healthcare, manufacturing, retail, technology
- Used by 7 of the top 10 patent holders

Discovery and Classification

- Endpoint, network, cloud and local data storage
- Content, context, and user classification
- Fully automated to fully manual classification
- Over 300 data types, over 90 languages

Educate and Enforce

- Monitor log, prompt, justification request
- Auto-encrypt, quarantine, move, block

Actionable Analytics

- System, user, and data level event visibility
- Analytics that filter out the noise
- Drag and drop incident management
- Right click remediation in real time

Operation System Support

- Full visibility, analytics and controls across multiple operating systems
- Mac
- Windows
- Linux

Deployment

- Managed Security Program
- SaaS
- On-Premise

DIGITALGUARDIAN®