CUSTOMER SUCCESS STORY

ANDRITZ Gains 24x7 Data Security Expertise While Reducing Overhead

About the Customer

The ANDRITZ GROUP is a global leader in turnkey equipment across a broad cross section of industrial businesses including hydropower, paper, steel, and biofuel. With more than 25,000 employees spread across 40 countries, understanding where the company's intellectual property resides and protecting it from misuse without business impact is critical.

The Business Challenge

The ANDRITZ GROUP is a long-time Digital Guardian customer. They use Digital Guardian to track and control the use of their IP across more than 250 global offices. They recognized that competition from large multinational companies, including state-owned entities, made IP protection their top priority.

Like many organizations, ANDRITZ faced the growing complexity of its IT environment compounded by scarce security resources to staff it. The task of managing and monitoring multiple products stretched their internal resources and made it difficult to take advantage of the full benefits of their security stack. Security analysts were focused on making sure their tools were running, not on higher value security tasks.

Even with the proliferation of new, more complex threats, adding more personnel to manage additional security technologies was not a feasible option. ANDRITZ needed to improve their security profile in both data loss prevention and endpoint protection without putting additional pressure on their internal resources.

Critical Success Factors

- Protect sensitive information from outside attack, insider threats, and inadvertent disclosure
- Improve the company's security profile without adding to their infrastructure or overhead
- Respect the privacy rights of their employees and adherence to Works Council and GDPR requirements
- Relieve burden on internal IT resources to focus on more business-critical tasks

Industry

- Manufacturing

Environment

- 250+ locations in over 40 countries
- 25,000 workstations
- Small internal security team

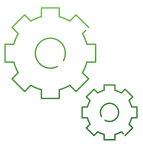
Challenge

- Underutilized solution due to scarce internal resources
- Significant and expanding volume of IP
- Works Council and GDPR regulations
- Geographically dispersed workforce
- Potential for nation-state threats

Results

- Protection from both internal and external threats
- Internal resources freed up for more critical tasks
- Quick time to value leveraging a managed solution
- Enhanced performance, including industry best practices

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

Moving from an on premises to a managed security solution was the right decision for ANDRITZ. They already understood the visibility to and granular control over their IP provided by Digital Guardian. Transferring the responsibility for running, maintaining, and optimizing their data protection was the logical next step. Digital Guardian's Managed Security Team allowed ANDRITZ to broaden the protections provided by Digital Guardian. Digital Guardian's efficiency and expertise provided constant "eyes on glass" for threat hunting and gave instant access to security experts. ANDRITZ could refocus internal resources on strategic tasks such as engaging with the business on secure expansion into new markets. The Digital Guardian team actively monitored their environment 24x7, providing alerts and escalating issues as required. ANDRITZ no longer had to worry about "off hours" scheduling and monitoring.

The transition to a fully managed solution was straightforward. A change in configuration, pointing the Digital Guardian agents to the Cloud-based servers instead of internal servers, began the migration. With Digital Guardian's team managing the environment, upgrading agents and policies was simplified. This saved ANDRITZ thousands of euros annually in services fees and allowed the company to expand their protection by adding Digital Guardian's Endpoint Detection and Response (EDR). Because EDR leverages the same agent as Digital Guardian's DLP, no additional steps were required.

The Results

Digital Guardian earned the position as a trusted advisor, which allowed ANDRITZ to move the monitoring and management of their data protection solutions to dedicated experts. This freed up internal resources without the need to deploy additional endpoint agents. In all, over 24,000 workstations and servers will be moved to the managed solution, maintaining employee privacy while improving the security of critical IP and supporting compliance efforts.

> *"With DG's MSP service, I can rest easy knowing that we have 24/7 protection and my team's resources are allocated effectively"*

- Scott Wiggins, CIO, ANDRITZ GROUP

ANDRITZ

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®