CUSTOMER SUCCESS STORY

A Fortune 200 Global Manufacturing Services Company

MANUFACTURING

Industry

- Manufacturing

Environment

- 90 plants in 23 countries with local IT
- Cloud-based IT environment since 2010
- 52,000 workstations

Challenges

- Data protection, while important, was in catchup mode
- Needed to identify and locate intellectual property, but IP "could be anything defined by the customer"
- At risk of financial penalties if customer NDAs were violated in a security incident
- Believed that security could be a competitive advantage, but didn't have headcount to accelerate security maturity

Results

- Managed service option sped implementation and time to value to less than four months
- Immediate visibility into data access and usage across business units
- Business unit leader adoption and collaboration resulted in dramatically more efficient data classification
- Data workflows defined with improved controls and data encryption enforced as required
- Developed the foundation for a mature security model as a competitive advantage

DIGITAL GUARDIAN®
Formerly VERDASYS

JABIL

Data Visibility, IP Protection and Business Unit Adoption in less than 120 Days

Jabil helps bring electronics products to the market faster and more cost effectively by providing complete electronics product supply chain management around the world. The company creates competitive advantage for their customers at every step in the value chain.

As the CISO, John Graham likes to say, "Jabil builds everything from toasters to drones." Built on a foundation of 180,000 empowered employees spread across 90 manufacturing plants in 23 countries, Jabil has quickly grown to be a Fortune 200 company. When Graham joined Jabil as CISO in 2013, he discovered that as a result of the company's fast growth, Jabil lacked some important processes and had no IT standardization. John believed that security could be a competitive advantage for Jabil. And with the goal of accelerating Jabil's security maturity in months instead of years, he knew he would need outside help. So he turned to Digital Guardian's Managed Security Program.

THE BUSINESS CHALLENGE

When Graham joined Jabil in 2013, a comprehensive security review revealed that Jabil had 52,000 workstations that were secured, but not at the levels the security team thought appropriate given the risks. Should a security breach leak a customer's intellectual property and violate NDAs, Jabil would risk significant financial penalties. Jabil also had valuable IP of their own, such as pricing deals from their suppliers, that they needed to protect.

CRITICAL SUCCESS FACTORS

- Build a program quickly by focusing on agility and collaboration for some quick wins
- Identify and locate critical IP as broadly defined by each business unit and its customers
- Increase visibility on data movement in the context of user, location and application
- Apply new protection controls across autonomous regional operations
- Implement a tiered control set where business units could choose from baseline security to higher, more restrictive levels
- Rely on a managed service provider to administer data protection, freeing the internal team to focus on data governance

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

DIGITAL GUARDIAN®
Formerly VERDASYS

www.digitalguardian.com

THE SOLUTION

CISO Graham had the vision to understand that data security could become a competitive advantage at Jabil.

The company's small but dedicated information security team needed to update its data protection processes and technology, but didn't have two years to devote to the effort. Graham knew they needed outside expertise to implement faster. A managed service would free internal operation personnel to focus on better data governance while leaving 24/7 global program administration to the experts. The company had prior success with cloud services and had already ramped managed services handling web proxy and single sign-on programs.

Jabil understood that its new data protection approach should pivot to focus on securing endpoints, not the perimeter. Digital Guardian was selected because its agent technology increases visibility on data movement with deep contextual awareness. Plus the managed service promised a very fast rollout of only three months – no other vendor gave quicker time to value.

Digital Guardian had to go beyond traditional data loss prevention. At Jabil, intellectual property is defined as anything that the individual customer wants protected: tooling sets, molds, component designs, CAD drawings or assembly plans. The security team gave each Jabil business unit the ability to classify IP by the way they worked with it, where was it stored, who had access to it, and what applications relied on it. A set of tiered controls define a baseline security level that meets corporate policies as well as higher, more restrictive levels for employees dealing with more sensitive data. Log data on violations is collected and filtered on metadata without inspecting content to protect employee privacy.

After a successful four-week test deployment of 3,000 agents in a closely-held development environment, Jabil deployed 49,000 agents to monitor machines worldwide – in less than 90 days from initial engagement with Digital Guardian. Any application conflicts that arose were resolved quickly using incident response procedures.

THE RESULTS

Within 30 days of full deployment, Jabil's security team gained visibility into all data access and usage across all 52,000 workstations. They immediately identified data being copied to USB drives more commonly than anyone expected. Digital Guardian's detailed egress reporting on the data leakage from USBs enabled Jabil's security team to have more collaborative conversations with the business unit (BU) leaders.

Instead of asking the BU leaders "what data do you think is sensitive" the Jabil security team went to them and said, "Did you know your people are copying data from these servers to USBs drives?" The BU leaders responded "this stuff (data) is important because it's on this server with sensitive information." With this approach Jabil was able to identify and classify their most sensitive data faster and dramatically more efficiently than the traditional approach.

External storage devices such as USB drives now have to be registered and sensitive files are encrypted as necessary. More secure employee workflows were defined that prompted users on risky behaviors. Jabil continues to improve its controls, classification and policy. Digital Guardian will be integrated with patch management, advanced threat detection, forensic analysis and connected to regional IT departments.