FORTRA™

5 Tips To Protect Manufacturing Trade Secrets

Lessons From A Fortune 100 CISO

Table of Contents

Foreword By A F100 CISO

According to the Manufacturing Institute, the shortage of skilled workers is cited as the single greatest impediment to a manufacturer's ability to expand operations, drive innovative new products and improve productivity[1]. However, as a manufacturer sources top engineering talent internationally and expands its global supply chain, it also broadens the footprint of its most sensitive and proprietary data.

One only has to look at the daily paper to see the evidence of state-sponsored espionage. Executives, security professionals, plant managers and research scientists in the manufacturing sector realize that a number of bad actors are trying to steal their intellectual property, or IP.

It's not just foreign governments like China—criminal organizations seek to steal and sell your IP as well as competitors conducting industrial espionage, hacktivist attacks and disgruntled parties. Even company insiders making honest mistakes—all threaten disclosure of your valuable trade secrets.

When I headed worldwide information security for DuPont, we learned some valuable lessons on how to mature a holistic IP protection program under executive sponsorship. In partnership with leading data protection solution providers, we learned how to safeguard our data assets without impeding product innovation and business growth. The result is these 5 Tips that will help you realize some quick wins in your own efforts.

Larry Brock, CISM
Principal, Brock Cyber Security Consulting LLC

About Larry Brock

- Currently consults to companies helping improve their IP protection capabilities
- Former Global Chief Information Security Officer at DuPont for 11 years
- Former CIO of DuPont's Nylon Flooring business unit
- Served as Information Security Officer within the U.S. Air Force
- Served at the National Security Agency (NSA) for 4 years, in reserves for 26 years
- BS and MS degrees in electrical engineering
- Certified Information Security Manager (CISM)

[1] All statistics: Manufacturing Institute

PART ONE

The Threats To Manufacturing Trade Secrets Are Real

Manufacturing At Risk

Your valuable intellectual property is already under attack. Manufacturers should assume both malicious insider and cyber-attacks are already occurring and take appropriate action. Do not underestimate the capability and persistence of your adversaries. They are smart, nimble and more financially motivated than ever. They won't stop until they reach their target—your sensitive data.

Trade secrets are the coin of the realm. As an industry, manufacturing pours billions into research and development to produce the IP that becomes new, marketable products. Overall sector investment in research and development drives economic growth around the world. Yet there remains a barrier to further market expansion—and it's a burden borne by information technology.

Offshoring has complicated the job of trade secret protection for IT security. Manufacturers continue to outsource skilled labor, research and qualified engineers where they are both abundant and affordable. In a world of distributed IP, procedures to both inventory and safeguard trade secrets have become exponentially more complex. Overseas suppliers and contractors require application access and information transfer across borders and geographies.

Here's betting your confidential IP is stored somewhere in the cloud right now, or sitting on laptops and mobile devices in foreign countries. Are you sure it's completely safe?

3.9% of manufacturing net sales reinvested in research innovation—the highest of any industry[3].

$300 BILLIONS Is the cost of IP theft to U.S. companies annually[4].

$8 TRILLION in lost R&D investment directly attributable to lack of skilled workers.

[3] Brookings Institute
[4] National Science Foundation

PART TWO

Calculating The True Cost of IP Theft

The True Cost Of IP Theft

The legal bar required to prove a theft of trade secrets is high. The Economic Espionage Act established that the victim must prove "reasonable protective measures (not all conceivable efforts) have been established to protect the information from both internal and external theft and misappropriation." This clause recommends that manufacturers implement technical safeguards "tailored to the day-to-day business of the particular enterprise, the confidential information sought to be protected, the community in which the company operates, and the established awareness of the individual participants to whom access to the information may be granted[5]."

One calculation of IP value used in legal cases alleging theft of trade secrets is net present value of future sales. The most alarming court judgments have set that value to ZERO if the manufacturer neglected to take proper action to safeguard its own secrets. This is also a common defense tactic by those charged with corporate espionage. Judges have ruled that, absent proper IP stewardship, the potential value of stolen trade secrets doesn't matter in the eyes of the law. There is no inherent right to damages from a competitor, foreign entity or anybody else. The company risks forfeiture of its trade secret title to any party exposed to the information absent adequate access and usage restrictions (e.g. administrative, technical, physical). Why should the courts protect information that the manufacturer itself has not adequately protected?

There's no better way to justify greater investment in IP protection.

IP Theft Can Lead To Material Damages, Including:

- ✓ Loss of product/market advantage
- ✓ Missed business opportunity
- ✓ Loss of reputation or brand loyalty
- ✓ Direct loss of revenue
- ✓ Direct loss of profitability
- ✓ Declines in stock price or valuation
- ✓ Lawsuits and fines

[5] Economic Espionage Act of 1996

PART THREE

The Scary Data

The Scary Data

92%
of incidents perpetrated by outsiders.

70%
of IP theft cases committed by internal people took place within 30 days of them announcing their resignation.

76%
of network intrusions exploited weak or stolen credentials.

50%
Over half of the insiders were former employees taking advantage of old accounts or back doors that weren't disabled.

Outsider Threats to Trade Secrets

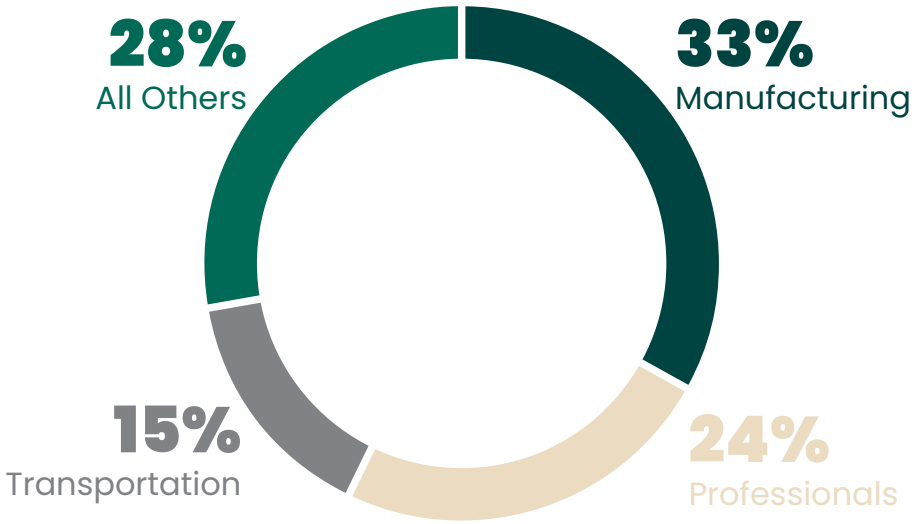
19%
of all attacks analyzed in this year's report were perpetrated by state-affiliated actors—in other words, a form of espionage.

15%
of incidents were perpetrated by insiders or business partners.

Insider Threats to Trade Secrets

The Scary Data

1/3 Of Espionage Attacks Are Targeted At The Manufacturing Industry



PART FOUR

5 IP Protection Tips

5 IP Protection Tips

There are no “silver bullets” for defending trade secrets, but based on the common experience of Fortra™’s Digital Guardian®’s customers— manufacturing executives in charge of information security—these five key recommendations will help you evaluate if your organization’s current IP defenses are sufficient.

1. Make the case for investiment in ongoing IP protection.
2. Establish a holistic IP protection program.
3. Protect your crown jewels from growing insider and cyber threats.
4. Discover the weaknesses in your security and how to address them.
5. Improve your ability to detect cyber-attacks.

TIP #1

Make The Case For Investment In Ongoing IP Protection

Obtaining adequate funding and resources for IT security initiatives is a process of executive education as much as advocacy. Many CIOs (typically the boss of IT security) simply aren't aware of the scale of the threats. Many think copying the precautions of their peers at other manufacturing companies is enough. Producing a well-thought out plan is required to convince them otherwise.

78% of intrusions rated as low difficulty[6].

66% of breaches took months—or years—to discover[6].

69% of incidents were discovered by external parties[6].

[6] All statistics: Verizon Data Breach Incident Report 2014

TIP #1 (CONT.)

Make The Case For Investment In Ongoing IP Protection

Your IP Protection Plan Should Explain:

- Why improved IP defense is essential to continue global expansion and profitable products
- How it will support key business initiatives
- How it will speed regulatory compliance efforts (e.g. ITAR, HIPAA, PCI, SOX, CFATS)
- Who will be responsible for managing the program
- How return on investment will be demonstrated

TIP #1 (CONT.)

Make The Case For Investment In Ongoing IP Protection

Do not request budget based on fear alone, or on vague industry statistics. Do not request security technology purchases without a solid business case. Make your chief executive not only aware of the threats, but troubled by them. To be viewed as a business partner by senior management, think in terms of “managed risk.”

Risk management forecasts and evaluates risks in order to avoid or minimize any potential negative impact. Use net present value of future sales to calculate the impact of any potential loss of valuable trade secrets and put your IP Protection Plan in stark business terms. Use actual examples of security incidents when your trade secrets were under direct threat; or public cases if unavailable. The CIO should believe that protecting IP is one of their key mandates or their own job is at risk.

Finally, you need advocates from other business functions on your side. Build support for the plan with R&D scientists, compliance auditors, business risk managers, corporate counsel and the heads of key business units. It takes an army to fight cyber criminals!

TIP #1 (CONT.)

Make The Case For Investment In Ongoing IP Protection

Investment Case Checklist

- ✓ Have an IP Protection Plan - Include everything needed to implement it
- ✓ Demonstrate how improved IP defense will help support key initiatives
- ✓ Demonstrate how improved IP defense will help support compliance
- ✓ Present specific actual incidents when your UP was under threat
- ✓ Use net present value of future sales to calculate impact of IP loss
- ✓ Assemble an army of advocates for the program from other departments

TIP #2

Establish A Holistic IP Protection Program

The best IP protection programs take a holistic approach, where senior leadership takes ownership but everyone in the organization and the extended enterprise has an equal stake in its success. Taking effective governance, risk and compliance programs as a model, your IP protection framework should have the following elements to organize and manage risks, objectives and reporting.

The governance structure of IP protection programs when done correctly is hierarchal as well as cross-functional. Here's how it works:

CEO

- Your company's chief executive retains ownership, remains routinely engaged, reviews the program periodically and helps drive a successful effort across the organization and beyond.

Company's Governance Team

- Governance teams typically include function leaders from IT, Risk & Audit, HR, Legal and key business units.
- Leverage this existing group to help support the program by asking them to influence their executive peers, eliminate barriers to success, recommend and approve data protection policy

IP Protection Program Leader

- This all-important role can be filled by an individual from corporate IT (e.g. CIO), information security (CISO) or corporate security (CSO).
- The program leader heads a collaborative cross-functional IP Risk Committee.

IP Risk Committee

- This committee includes executives like the CIO, CISO or CSO, the Compliance lead and duly appointed IP protection leaders from select functional areas such as R&D, Engineering or Operations.
- Every business line should appoint someone who's responsible for IP protection to smooth IP identification and classification, business process changes and user education initiatives.

TIP #2 (CONT.)

Establish A Holistic IP Protection Program

Written Policies & Procedures. It goes without saying that IP protection relies on unambiguous, clearly communicated policies and procedures. These define what is required of employees, outsourcers, suppliers, contractors, consultants, vendors and all other third parties when accessing, utilizing and properly handling the company's trade secrets. These rules need not be draconian, just reasonably capable of reducing the risk of mistake or misconduct. Compliance with these policies must be a condition of employment, contracting and procurement by the corporation.

Regular Risk Assessments. Audit, Monitor & Report. The next two elements of our framework, borrowed from compliance programs, focus on routine measurement and course correction. Are the recommended IP protection procedures being followed? Are our policies too confusing? Are corporate standards too strict or too loose? Once a year, risks to trade secrets should be reassessed and reprioritized. The IP Risk Committee can use metrics, audits and incident reports to make improvements to the program as necessary, over time.

TIP #2 (CONT.)

Establish A Holistic IP Protection Program

The IP Risk Committee...

- Identifies and assess threats, likelihood of harm and potential damage
- Writes IP confidentiality policies incorporating organizational principles & processes
- Implements safeguards to prevent unauthorized access, use or disclosure
- Manages response plans developed by committee member organizations
- Enforces policies with all parties, subject to security and confidentiality protocols
- Audits policy metrics to assess effectiveness
- Fixes deficiencies and adjusts to new threats

TIP #2 (CONT.)

Establish A Holistic IP Protection Program

Effective Education. The quickest route to success is to create an ownership culture where all are committed to safeguarding secrets. Anyone who handles sensitive or proprietary data in the course of their jobs should be trained on company standards, policies and procedures. Communication methods range from mandatory computer-based training to newsletters, bulletins to videos. Educate everyone on the realities of both outsider and insider threats, such as the disgruntled employee, careless contractor or honest mistakes by the local supplier. Users can be human detectors watching for phishing attacks and other IP loss red flags. A truly committed trainee goes beyond doing the minimum necessary to understand that their livelihood is at stake when trade secrets are lost.

Delegation of Authority, Consistent Enforcement & Response to Violations. The last three elements describe effective administration of a consistent IP protection program. Strict "need-to-know" guidelines should be implemented, granting IP access authority only to those who have earned that trust. Maintain multiple avenues for reporting potential breach incidents (e.g. a hotline and email). It's everyone's responsibility to be on the lookout for violations of data protection policy. Corrective actions should be taken swiftly and consistently at all levels (assuming the violator was previously trained, of course). Don't be shy about reporting these incidents across the company. This is not to instill paranoia but rather to teach by example. Recognize and reward those involved for their vigilance.

TIP #2 (CONT.)

Establish A Holistic IP Protection Program

IP Protection Checklist

- ✓ Establish clear policies and procedures
- ✓ Assign senior leadership with high level ownership of the program
- ✓ Create a culture where all are committed to IP protection
- ✓ Effectively educate everyone on both outsider and insider threats
- ✓ Monitor, enforce and report IP security violations
- ✓ Audit the program's effectiveness annually
- ✓ Improve the program over time as needed

TIP #3

Protect Your Crown Jewels From Growing Insider & Outsider Threats

What isn't known can't be protected. Every kingdom has its crown jewels, and every manufacturer should know where all of its most valuable (and potentially profitable) intellectual property resides. IP can be defined as any type of financial, business, scientific, technical, customer and engineering information which is deemed proprietary. Every manufacturer files patents to protect their inventions, industrial designs and plant processes—but trade secrets can also include plans, prototypes, procedures, in-process research, names, codes and lists. Any intangible information, even employee knowledge and ideas, is worthy of protection.

The process of identifying and classifying all of your enterprise IP is not an easy one. Many believe this is the job of IT, but there is a good reason why you've appointed IP protection leaders in each business and function. They know where their jewels are hidden, including cloud services which may or may not be authorized (e.g. Dropbox). They need to both lead this effort and assume accountability for the protection of their own crown jewels. IT security should not assume accountability, but instead help with tools, best practices and resources.

TIP #3 (CONT.)

Establish A Holistic IP Protection Program

Defining Intellectual Property

- Patents & trademarks
- Financial data
- Industrial designs
- Manufacturing processes
- Plans & prototypes
- Plant procedures
- R&D testing
- Customer information
- Names, code & lists

TIP #3 (CONT.)

Protect Your Crown Jewels From Growing Insider & Outsider Threats

Consider using an automated data protection platform like Digital Guardian to classify each asset based on distinct levels of sensitivity and then define specific rules for each level. Your crown jewels need to be protected throughout their IP life cycle: from lab idea to written procedure, plant process to shipping product. Control access using the principle of least privilege—granting people the lowest level of user rights necessary to do their jobs effectively.

Lock up your crown jewels in secure electronic "vaults" where strong multi-factor authentication and robust account management restrict access by user role. Investigate technologies such as digital rights management (DRM) and data loss prevention (DLP), which provide data encryption and export restriction capabilities. As content is removed from the vault, it is controlled and protected by the policies associated with how it was tagged during classification. Monitor and audit IP usage by partners and suppliers throughout your supply chain. Set up alerting whenever an established control such as user privileges or firewall configuration is changed. Secure endpoints such as PCs and mobile devices when off the network, where many data breaches originate. All these actions will make it very hard for attackers to gain privileged access to any of your crown jewels.

TIP #3 (CONT.)

Protect Your Crown Jewels From Growing Insider & Outsider Threats

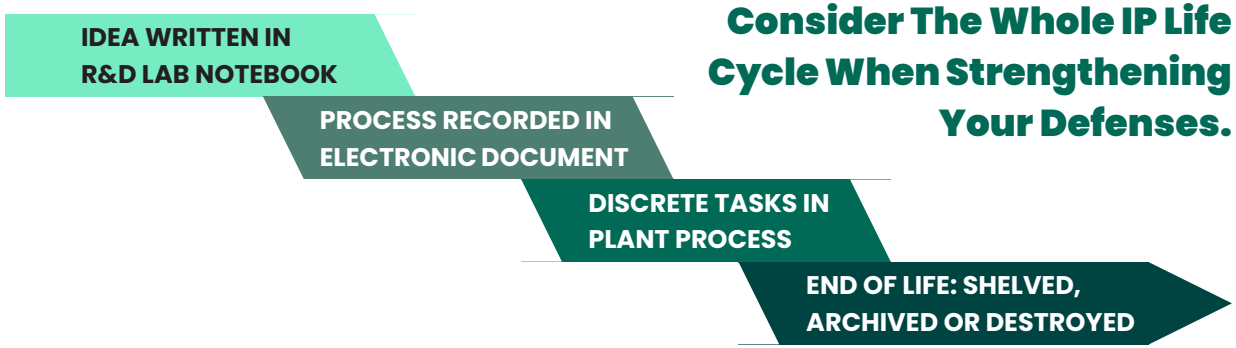
Data Protection Checklist

- ✓ Consider an automated tool to identify & classify your IP
- ✓ Create policy rules & privileges for each type of asset
- ✓ Establish very tight electronic access controls
- ✓ Tag & monitor IP throughout its lifecycle
- ✓ Investigate technologies such as DRM & DLP

TIP #4

Discover The Weaknesses In Your Security And How To Address Them

Become a student of information security. Even the most seasoned IT professional has more to learn, as the tools and techniques of cyber attackers are constantly evolving. Ongoing threat intelligence will help you understand the current indicators of compromise and stay a step ahead of the bad guys. Cyber risk information is readily and publicly available from organizations such as CERT, SANS and antivirus vendors. Many offer subscription-based threat and vulnerability feeds. Collaborate with government and public institutions such as the Department of Defense DSIE, DHS Information Sharing, ISACs Council and the FBI. Form a small information sharing group with other trusted manufacturers. Learn to benchmark your organization's approach against IP protection leaders with mature programs. Eventually, you may become a contributor of intelligence to aid the collective struggle!



Consider The Whole IP Life Cycle When Strengthening Your Defenses.

TIP #4 (CONT.)

Discover The Weaknesses In Your Security And How To Address Them

The main lesson to learn from your pursuit of IP protection is that the business of IP protection is never finished. Continue to improve your capabilities as your organization matures in its understanding of the threats faced. To get to the next level, relying on a little outside expertise is often a good thing. Skilled penetration testers are consultants that analyze your prevention, detection and response capabilities by mimicking the tactics of seasoned cyber attackers. These “white hat” hackers will target your system admins with benign phishing, drop “infected” USB drives and perform social engineering with key business users—among other ploys to gain privileged access. Sneaky.

To assess your program’s development, an overall security review by an unbiased third party should be considered. It will evaluate your security framework and architecture, outline major business risks and identify gaps in current controls, processes and resources. Once these weaknesses have been identified, review the results with senior management to gain approval and funding of an improvement project to close the gaps. Prioritize fixes based on level of risk and difficulty to execute. Then wait a while and review the program again.

TIP #4 (CONT.)

Discover The Weaknesses In Your Security And How To Address Them

Data Protection Optimization Checklist

- ✓ Pursue ongoing threat intelligence to stay ahead of attacks
- ✓ Collaborate with external groups to share information
- ✓ Benchmark your performance against IP protection leaders
- ✓ Consider a security review to identify protection gaps
- ✓ Hire skilled penetration testers who mimic cyber attackers

TIP #5

Improve Your Ability To Detect Cyber-Attacks

To match your improved knowledge and understanding, make your IT systems more intelligent as well. Security information and event management (SIEM) solutions provide real-time analysis of activity logs and high risk alerts generated on the network. Start by pointing these intelligent systems at your highest value assets or highly privileged users such as plant operations or R&D labs.

Data access and egress controls on your information flows can also benefit from greater intelligence. Evolve your organizational mentality from keeping the bad guys out to keeping the crown jewels from leaving. Your enterprise may want to control outbound Internet access to unsecured sites, restrict use of outbound protocols (e.g. FTP, SSH, Telnet), limit public sharing and email services for unencrypted data or provide virtual server access where data can't be downloaded. Intelligent monitoring of web and email content can flag and block prohibited activity before your IP is gone.

TIP #5 (CONT.)

Improve Your Ability To Detect Cyber-Attacks

Cyber Security Checklist

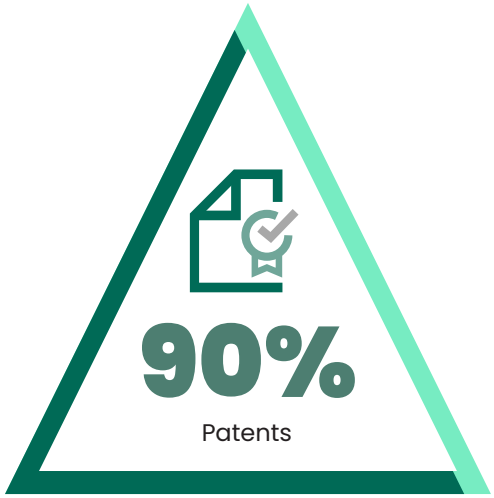
- ✓ Make your systems more intelligent to match threat intelligence
- ✓ Improve IP egress controls as your capabilities mature
- ✓ Constantly improve your IP protection based on what you learn
- ✓ No manufacturer is an island - collaborate with others oncommon goals

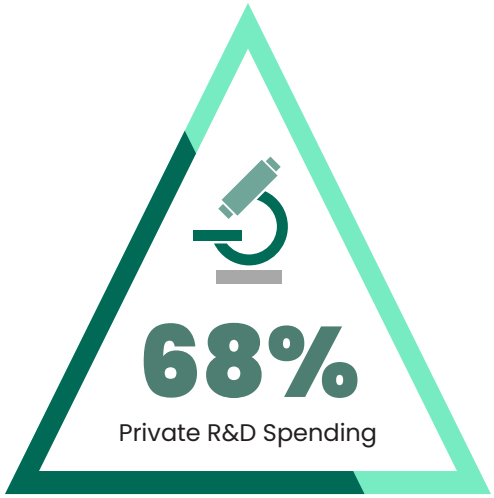
PART FIVE

Summary

Summary

Protecting your manufacturing trade secrets is a journey, not a destination. It requires a holistic approach beyond purely information technology controls, which are still necessary but insufficient without user education and awareness. The best programs have the active support and participation of senior leadership. They are based on solid governance, risk and compliance principles. Protecting your critical IP is an ongoing process of detection and response that's continuously measured and improved over time. As an industry, manufacturers must collaborate to protect our common interests against those who would do us harm.





90 percent of Patents, 68 percent of Private R&D Spensing, and 11 percent of U.S. GDP Attributed to the Manufacturing Sector overall[7].

[7] Brookings Institute

PART SIX

Digital Guardian: Next Generation Data Protection

Next Generation Data Protection

Data protection is at the core of our company mission. Our next generation data protection platform is purpose built to stop data theft. This platform is designed to:

- Discover and protect sensitive data throughout the data lifecycle and across the enterprise
- Protect sensitive data on the network at the endpoint, in storage and in the cloud
- Provide automated classification
- Provide integrated advanced protection to protect data from external threats
- Provide flexible deployment options including a managed security service manned by our peerless analyst team with deep, real-world expertise

Management Console

Data Discovery

Data Classification

Advanced Threat Protection

Endpoint Data Loss Prevention

Network Data Loss Prevention

Cloud Data Protection

Free Download

Digital Guardian Platform Technical Overview

Free Download

Digital Guardian Managed Security Program Technical Overview

Case Study

A Manufacturer's Quick Win

SITUATION: Jabil is a Fortune 100 contract manufacturer. The company was at risk of large financial penalties if customer NDAs were violated due to a security incident.

SOLUTION: Within 30 days of DLP deployment, Jabil's security team gained visibility into all data access and usage across 52,000 workstations. They immediately realized that users copying large data files to USB drives was far more common than anyone expected. Digital Guardian's detailed egress reporting on the data leakage from USBs enabled Jabil's security team to have more productive conversations with business unit leaders. These exchanges focused not on defining what data was considered sensitive, but rather on how data from specific servers was being used (in this case copied to USBs) by users.

RESULTS: By providing business leaders real-world information on how data was being used (or misused), Jabil was able to identify and classify their most sensitive data faster and more efficiently. This was a dramatic improvement over a more traditional discovery and classification approach.

> Within 30 days of DLP deployment, Jabil's security team gained visibility into all data access and usage across 52,000 workstations.

More Info

Read the full case study here.

A Leader In The Gartner Magic Quadrant

- "Digital Guardian offers one of the most advanced and powerful endpoint DLP agents due to its kernel-level OS integration. In addition to Windows, both Apple OS X and Linux are supported."
- "The Digital Guardian solution for endpoint covers DLP and endpoint detection and response (EDR) in a single agent form factor…"
- "…Digital Guardian [is one of] two vendors most frequently mentioned by clients looking for a managed services option."

Free Download

Gartner 2016 MQ
for Enterprise DLP

2017 Gartner Magic Quadrant For Enterprise Data Loss Prevention

Gartner 2016 Magic Quadrant for Enterprise Data Loss Prevention, 1 February, 2016 , Brian Reed and Neil Wynne.

60 MILLION TERABYTES

OF SENSITIVE DATA IS PROTECTED DAILY
BY DIGITAL GUARDIAN AGENTS

OVER
2.5 MILLION
AGENTS DEPLOYED WORLDWIDE

TRUSTED DAILY BY MORE THAN
450
OF THE LARGEST BRANDS IN THE WORLD

ACROSS
54
COUNTRIES

...ONE OF THE LARGEST AND MOST RESPECTED
COMPANIES IN THE WORLD HAS DEPLOYED OVER

300,000 **AGENTS**

INCLUDING...

7 OF THE **TOP 10** PATENT HOLDERS

AND **7** OF THE **TOP 10** AUTO COMPANIES

THE ONLY AGENT-BASED TECHNOLOGY COVERING

250,000 EMPLOYEES

USING A SINGLE MANAGEMENT SERVER

WE ARE THE **DATA PROTECTOR** OF **CHOICE** IN

ENERGY | FINANCIAL SERVICES | GOVERNMENT | TECHNOLOGY | HEALTHCARE & LIFE SCIENCES | MANUFACTURING

BECAUSE WE'RE FOCUSED ON PROTECTING
ONE THING: DATA

What DLP Must Do

Today's Data Loss Prevention solutions must protect against insider threats, external attacks, and outsiders posing as insiders. DLP must protect manufacturing IP no matter where it resides and how it is used. DLP technologies provide valuable context that can help manufacturers recognize the sensitivity of potentially compromised data, and then focus remediation and incident response efforts accordingly.

Success with DLP depends on setting reasonable data protection priorities, correctly evaluating vendor solutions, and selecting a deployment method. Presenting a compelling business case to business and technical executives will prevent the risk of delaying DLP initiatives. DLP can then be implemented using a simple framework that focuses on realizing "quick wins" to provide rapid return on investment and protect your sensitive data.

Data Loss Prevention is constantly evolving. We'll continue to stay on the forefront of data protection trends and technologies and keep you up to date with our web site, blog and resources: **www.digitalguardian.com**

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

(fta-dg-gd-0523-r1-79d)