FORTRA™

CASE STUDY (Digital Guardian)

Identifying and Blocking a Rogue Employee on Day One

About The Customer

The company helps organizations worldwide accelerate time to market and lower production costs through design and manufacturing services. The company operates from over 100 facilities around the world, employing over 190,000 dedicated individuals.

The Business Challenge

The company was a long time customer, using Digital Guardian's Managed Security Program (MSP) for Data Loss Prevention (DLP). With Digital Guardian installed on over 65,000 workstations, the company was confident that the DLP managed service was protecting their intellectual property as well as their customers. The CISO viewed this protection as a competitive advantage.

However, the CISO was aware of the changing threat landscape. In late 2014, hackers stole and released confidential information from Sony Pictures. In 2015, the federal Office of Personnel Management (OPM) had over 21 million sensitive records stolen. Cyberespionage by nation states was growing so quickly that in April 2015, a national emergency was declared to deal with "the increasing prevalence and severity of malicious cyber-enabled activities" originating outside the US.

Concerned about the growing threat from industrial espionage and the value of the IP they managed, the CISO decided to expand the company's managed security program with Digital Guardian to address advanced, external threats.

INDUSTRY

- Manufacturing

ENVIRONMENT

- 65,000+ endpoints
- 100+ facilities around the world
- Managed Service Program

CHALLENGE

- Integrate Endpoint Detection and Response without impacting endpoint performance
- Growing threat from cyberespionage
- Geographically diverse environment
- Integrated reporting

RESULTS

- ATP deployed globally to all endpoints in one day
- Malicious activity detected on day 1
- Activity blocked, full forensic investigation completed and rogue employee terminated within 3 days

Critical Success Factors

- Provide protection from advanced, external threats without impacting performance
- Fill skill set and resource gaps required to conduct Incident Response (e.g., Forensics and Reverse Engineering).
- Data protection expertise and resources to analyze and correlate events to surface threats immediately
- Integrated reporting with Data Loss Protection for a single management view to threats

The Solution

With Fortra™'s Digital Guardian® already installed on the company's endpoints, and configuration, monitoring, and reporting in place from DG's MSP, adding advanced external threat protection was simply a matter of adding Digital Guardian's Endpoint Detection and Reponse (EDR) policies to the existing agents' rule sets. The company could begin to defend against advanced threats immediately.

On the first day of the policy rollout, Digital Guardian's Advanced Threat & Analysis Center (ATAC) team alerted the company of suspicious activity. One of Digital Guardian's 200+ pre-built behavior-based rules identified a backdoor installed on multiple devices logging keyboard strokes, controlling microphones, and recording screen activity. Using DG's built-in Endpoint Detection and Response Scanner, the ATAC team remotely collected forensic data, including event logs, registry keys, and pertinent forensic artifacts from the affected devices to begin their analysis and build a timeline.

While the company's expectation was that advanced threats would originate from outside the company, this attack came from within. The data immediately showed that a business analyst at one of the company's sites had downloaded multiple hacker tools and technical books on coding. A few months later, the analyst began visiting various hacker and cybersecurity websites. Next, he began testing his skills by running various password dumping programs. He then wrote and installed a onto his work laptop leveraging the chat client Pidgin for issuing command and control orders, and the FTP protocol to exfiltrate data to a website he managed.

Digital Guardian's detailed forensics proved that the analyst installed his backdoor on over 25 devices in the company, collecting video through their laptop camera, recording their daily discussions, and logging their keyboard strokes.

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 Results

On the first day of the Digital Guardian EDR policy rollout to the existing agents, the rogue employee was identified and the ATAC team was able to build the timeline of events. Within 3 days, all affected devices were identified. With the undeniable forensic evidence of over a year of malicious activity in hand, the company confronted and fired the Analyst. The company is so pleased with the Digital Guardian service they have extended it worldwide to 300,000 workstations.

Evolution of an Insider Attack

2015

May
Hacker Tool Downloads

August
Installed Keyboard Logger on Personal PC

October
Compromised 5 Hosts

December
Compromised 3 Hosts

2016

May
ATP Installed

ATP Detection

June
Employee Termination

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

FORTRA™

Fortra.com

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.