VERDASYS
ENTERPRISE INFORMATION PROTECTION

INSIDER THREAT PREVENTION

An Inside Look at a Global 100 Company's Program

VERDASYS USE CASE

APPLICABLE INDUSTRIES

Manufacturing, Aerospace & Defense, Oil & Gas, Energy, Technology, Chemical, and Pharmaceutical/Biotech

BUSINESS DRIVER

Protect the Intellectual Property of a $30 billion global manufacturing company after a privileged insider stole trade secrets valued at $400 million.

BUSINESS NEED

Deploy an Insider Threat Prevention Program that mitigates the risk of data compromise without impeding innovation or collaboration among privileged users. Critical requirements included:

- Capture all IP data events by user in their complete transaction context
- Use real-time prompts to educate and warn users attempting risky behaviors
- Integrate tamper-proof activity forensics with existing investigative tools as an evidentiary-sound collection process.

The stolen trade secrets were valued at over $400 million. The perpetrator was a privileged insider, a foreign national who had worked for this multi-billion dollar global manufacturer for over 10 years. The Board of Directors vowed to prevent such an incident from recurring, and mandated the Chief Information Security Officer (CISO) to develop and implement a company-wide insider threat protection program immediately. It was the Spring of 2007.

At the time of the incident, the CISO led a security team who had deployed data loss prevention (DLP) technology at the network perimeter to meet regulatory requirements, but it could only detect keywords and phrases in emails. Clearly, that had not prevented the prior incident, but what kind of solution could stop a trusted user from misusing trade secrets? How could it identify irregular content like formulas and engineering designs? How would it tell an "insider threat" event from an authorized use? How could it capture evidence that proves malicious intent? Most importantly, how would it accomplish all this without blocking the business process?

The CISO turned to two partners for help: The FBI and Verdasys. The FBI was enlisted to help build a privileged user monitoring program that would recognize attempts by insiders to steal data; instruct the security team on how to properly collect event forensics; and define the policy controls needed to help achieve the program's objectives. Verdasys Digital Guardian was deployed as the company's enterprise-wide information protection technology platform. By combining the best people, processes, and technology the CISO was able to build an evidence-based insider threat prevention program upon four main pillars: data governance; employee education & accountability; forensic analysis, and business enablement.

Data governance began by designating a cross-functional team to assign data owners, create classification levels for intellectual property (IP), define acceptable use policies, and develop a strategy for employee policy training and awareness. Digital Guardian was used to provide accurate enterprise-wide visibility of where IP is at-rest and in-use; permanently tag it and track its uses; and analyze the risk of its transactions in both a policy and business context.

Employee education & accountability was to be the main driver of policy enforcement, as the governance team determined self-compliance would be the most cost-effective way to deter insider threats without necessarily restricting the business process. Digital Guardian was used to deploy real-time policy prompts to shape safer user behavior before a risky transaction occurs, and reminding malicious individuals their actions were being monitored.

Forensic analysis was the key recommendation from the FBI to better assure evidence collected during a data loss investigation incident could be accurately reconstructed and, if necessary, accepted in court. Digital Guardian's event logs were used to establish a continuous chain of custody connecting all enterprise transactions between users, files, systems, and applications in context, and ensure those forensic records were captured and secured using an evidentially-sound process.

Business enablement was the program's ultimate goal. The CISO's team had to implement a measurable information protection solution that: productively secured IP collaboration among privileged users; could evolve and expand to meet new business requirements; and prove that the company's data was not used beyond its acceptable risk.

Result: The data governance team was founded in January 2008, followed by the creation and communication of the first policies and procedures for insider threat prevention. By Spring 2008, Digital Guardian was deployed to 25,000 systems, and reached over 40,000 by year's end. Within six months of the program's launch, the team had established a baseline of enterprise data usage and permanently classified the company's most restricted IP. From there, educational prompts where created to warn users of higher-risk data transactions, like copying IP to USB devices and printing. Finally, Digital Guardian event logs were integrated with the existing forensics-collecting infrastructure using Digital Guardian's Case Management capabilities.

In the Fall of 2009, Digital Guardian detected a senior researcher violating numerous usage policies for trade secrets while working both on and off the network. The context of the transactions left little doubt this was an attempt to steal proprietary data, later estimated to be worth $800 million. Armed with a trove of incriminating forensic evidence from Digital Guardian logs the company approached the United States District Attorney with their complaint, who in turn issued an arrest warrant against the employee before he was able to abscond with the data to his native country.

Today, the CISO's insider threat prevention program is a fundamental component of the company's strategic planning.

CONTROL TYPES

Classification & Tagging

- Sensitive design files found or created on host systems
- Data exported from "sensitive" applications
- Any IP found on collaboration servers

Alerting

- On policy violation (Security Team)
- On repeat policy violations (Security Team & Employee's Manager)
- On IP transaction volume exceeding risk thresholds (Security Team & Employee's Manager)
- On IP email volume exceeding risk thresholds for offline use (Security Team & Employee's Manager)
- Any policy violation that invokes a blocking control (Security Team & Employee's Manager)

Education & Blocking

- Attaching IP to email (Educational Prompt)
- Copying IP to USB or DVD (Educational & Justification Prompt)
- Printing IP (Justification Prompt)
- Exporting data from sensitive application (Educational & Justification Prompt)
- Attempting to transfer IP to social media, webmail, or unapproved websites (Educational prompt & Action Blocked)

Forensics

- Capture all transactions related to policy violations
- Special event capture when a privileged user's role is changed or terminated
- Special event capture for IP email attachments sent to unapproved recipients

DATA LOSS INCIDENT INVESTIGATION

The investigation of the attempted insider theft in 2009 included the following forensic event data collected by Digital Guardian to successfully prosecute the individual:

- Email content showing the employee intended to resign for an "overseas" job, later determined to be at a foreign state-owned institution.
- Slide presentation that included plans for utilizing the stolen data to produce competing products in a foreign market within five years.
- Email attachments that included "hidden & embedded" trade secret data being sent to unauthorized recipients outside the company.
- Email content sent by the employee to his personal email account that included instructions on restricted production processes and a list of raw materials shipped to an accomplice.

PROJECT CASE DESCRIPTION

People: Scientist, Engineers, Research Scientists, Executives and IT Security Administrators

Data Type(s): Engineering CAD files, process and manufacturing designs, test results and chemical equations

Usage: Secure collaboration between R&D, engineering , manufacturing, and production teams across North America, Europe, and Asia

Key Differentiators

- Integrated data usage visibility, policy enforcement, and risk analysis across 44,000 host systems from a single technology platform
- Persistent and inheritable data classification using both a file's content and its sensitivity context (e.g. source application, database, network share, etc.) to permanently identify and monitor IP over its lifecycle
- Tamper-resistant agents and event logs that make it virtually impossible for a privileged user to kill or circumvent data protection or evidence capturing functions
- Integrated case management and forensics

BUSINESS VALUE

- Provides enterprise to forensic-level visibility and risk management of IP usage by trusted insiders through a single, integrated policy framework
- Continuously monitors sensitive data access and sharing among privileged users in their complete transaction context to help prove chain-of-custody and intent
- Real-time policy education and warning prompts raise user awareness of risky behavior; drive voluntary self-compliance; and assure accountability for transactions
- Reduces investigation and legal costs by integrating security, incident response, event forensics, and case management in an evidentiary-sound process

Report types

- Data at-rest reports for IP stored on privileged user endpoints and restricted project servers
- Trade secret egress report by USB, DVD, Network Printers and Local Printers; includes transaction context by classification type, system or printer location, time stamp, data volume, and user identity
- Email usage reports by body content, attachment content, file classification, encryption status, and destination
- Risk trend reports by data classification, user activity, and egress channels
- Employee exit reports with their most recent system file inventory and historical IP usage to verify compliance with data handling policies

VERDASYS

Corporate Headquarters
404 Wyman Street
Waltham, MA 02451 USA
info@verdasys.com
781-788-8180

www.verdasys.com

ABOUT VERDASYS

Founded in 2003, Verdasys provides insider threat solutions that are the cornerstone of our customer's global data security strategy. With over a million security agents deployed at over 200 of the world's leading organizations and Federal agencies, our solutions and services provide a strategic and comprehensive approach to information risk management.

© 2011 Verdasys, Inc. All Rights Reserved. Verdasys, the Verdasys logo, Digital Guardian, and the Digital Guardian logo are trademarks of Verdasys, Inc. All other logos are the property of their respective owners. The content of this document is subject to change without notice.