

Securing Sensitive Data in Outsourced Environments

CUSTOMER SNAPSHOT



CIGNA
A Business of Caring.

CIGNA is one of the nation's largest providers of workplace health and related benefits, including health care products and services, group life, accident and disability insurance.

► Website

www.cigna.com

► Industry

Health Care

► Problem

CIGNA needed a strong, flexible information security and data protection solution to support the company's growing outsourcing initiatives and in-house applications, in addition to achieving HIPAA compliance.

► Solution

CIGNA implemented Verdasys' Digital Guardian to ensure that users at its outsourcing partners do not inadvertently or intentionally violate CIGNA's information security policies. CIGNA receives alerts on any activity that could put data in jeopardy, such as cutting and pasting information into external web mail accounts or saving data to portable storage devices, while security agents on laptops, desktops and servers prevent these potentially dangerous actions in real time.

► Benefits

Adopting a point of use security strategy using Digital Guardian enables CIGNA to expand its offshore outsourcing to support its growing business. In addition, CIGNA has deployed Digital Guardian in a number of its business units and relied on it to achieve HIPAA compliance. With approximately 1,000 Digital Guardian security agents currently monitoring and controlling user activity around the world, CIGNA anticipates having 25,000 agents in use by the end of 2005.

As one of the nation's largest health and related benefits companies, CIGNA is on the front lines of information security. Each day CIGNA processes volumes upon volumes of sensitive data, from customer social security numbers, medical records and health care benefits information to employee payroll details and business application data, as a part of its business operations. The protection of that data is a bond CIGNA makes with its customers and employees – and it is vital for the company's long-term success.

CIGNA's commitment to information security starts with its senior executives, who have developed and implemented a range of proactive and thought-leading data protection strategies. While protecting its information assets from external threats is certainly a priority, a large percentage of CIGNA's effort is focused on preventing potential data misuse and leakage by authorized users such as employees, contractors and business partners.

"Nearly 70% of all security breaches are by employees or contractors who have been granted authority to access proprietary information," said Craig Shumard, CIGNA's Senior Vice President of information protection. "It's far easier to copy confidential data to a USB drive or paste it into email than it is to hack into a company's databases – yet, ironically, the majority of security products on the market are focused on the 30% of attacks that originate outside the company."

Outsourcing Creates New Business Opportunities and Security Challenges

When CIGNA contracted with a partner offshore to outsource a portion of its application development and maintenance activities, the need to protect company data in outsourced environments became a key priority. The company required a solution to prevent potential data leaks and enforce proper use of intellectual property such as source code. The company's executives, however, wanted to make sure that any security solution chosen would not get in the way of daily business operations. After examining various options available in the marketplace, CIGNA selected Digital Guardian from Verdasys.

Digital Guardian is an information security platform for the audit, control and protection of data where it is most vulnerable: the point of use. Through the real-time monitoring and enforcement of policies over how information is used on desktops, laptops and servers, Digital Guardian allows CIGNA to control which outsourced and internal users can access data and exactly what they can do with it – even from halfway around the world.

VERDASYS™

Data Security at the Point of Use

“Digital Guardian is a business enabler. For example, we wouldn’t be able to achieve the significant business benefits outsourcing offers without it.”

Craig Shumard, CIGNA’s SVP of information protection

“When you try to enforce information usage policies, the only real control you have is at the point of use,” said Michael McKenna, Assistant Vice President for engineering and standards at CIGNA. “Digital Guardian is the only solution that addressed our need to prevent loss or abuse of critical data by highly trusted users.”

Monitoring, Control and Compliance

The Digital Guardian system consists of a web-based management console and host-based security agents. After installing the Digital Guardian console at its information technology center in Connecticut, CIGNA deployed several hundred agents to its partner’s desktops, laptops and servers offshore.

Through the console, CIGNA defined and implemented a set of business rules representing the company’s information usage policies for enforcement. The same console also provides centralized agent management, audit and forensic activity queries, aggregate activity and violation trend reporting, and alert management.

The highly tamper-resistant Digital Guardian agents, which operate transparently to users, track all file, application, network, clipboard and printing operations. They enforce security policies in real time by taking action against activities that violate specific information usage rules. Agents log all user actions, filter and correlate the data to drastically reduce its size, then report back to the console, allowing CIGNA to integrate activity information into a single, enterprise-wide journal that makes it possible for the company to identify suspicious activity, track data usage trends, and generate forensic and compliance-related reports quickly and efficiently.

Digital Guardian enables CIGNA to protect its intellectual property by thwarting user actions that can put information in jeopardy. For example, the system prevents information from being copied to external network destinations via conduits such as email, webmail, IM or FTP. The same agents also keep data from being saved to portable storage devices such as USB flash drives, CDs, and even music players and digital cameras. CIGNA can also tailor Digital Guardian’s response to correspond to the level of threat presented by a particular user action. Enforcement can range from blocking a specific activity, to issuing a silent

alert to administrators, to generating on-screen warnings that educate users about the policy violation or ask for a business justification before being allowed.

The ability to enforce risk-appropriate controls provides CIGNA with the flexibility to balance security with business needs. The ability to handle numerous security functions with a single agent also eliminates the need for multiple single-purpose agents on each user device, which reduces overall cost and management efforts. The same agent technology can also be used to harden application, file and print servers as well as virtual sessions in Citrix and Terminal Server environments.

In addition, Digital Guardian’s reporting functions allow CIGNA to understand data flows to high-risk destinations throughout the enterprise. The reports offer insight into when and how policies should be adjusted as new security concerns arise.

“It comes down to intellectual property containment. We have a key advantage because of Digital Guardian,” said Shumard. “We now have the option to outsource a business process and have confidence that our intellectual property would not be compromised.”

Securing the Extended Enterprise

CIGNA’s success with the offshore outsourcing implementation convinced the company to expand Digital Guardian to other outsourcing partners as well as to in-house applications. For example, CIGNA now uses Digital Guardian’s capabilities to meet HIPAA compliance and reporting requirements. Digital Guardian agents log additions, updates and deletions to files, track application activity and generate reports on unusual actions, per HIPAA requirements.

From the initial deployment of several hundred security agents, CIGNA now has approximately 1,000 Digital Guardian agents in use within the company and at its worldwide outsourcing partners. The company anticipates rolling out Digital Guardian to its 24,000 employees by the end of 2005.

“With Digital Guardian, we can extend the reach of our security policies and best practices to our global enterprise,” said Shumard. “Whether intellectual property resides in-house or around the world, Digital Guardian allows us to maintain the security and data integrity we need to maintain our leadership position in our marketplace.”

ABOUT VERDASYS

Verdasys provides the first enterprise-wide security platform that protects data from loss or misuse at the point of use – on laptops, desktops and servers. Through the real-time control and comprehensive monitoring of information use at the host, Verdasys provides solutions that protect customer data, safeguard intellectual property, assure ongoing regulatory compliance and secure outsourced environments.

VERDASYS

950 WINTER STREET, SUITE 2600 WALTHAM, MA 02451
781-788-8180 TEL 781-788-8188 FAX
WWW.VERDASYS.COM INFO@VERDASYS.COM