MICRO FOCUS

Case Study

Security

Digital Guardian

Digital Guardian employs data recognition technology enabled by Micro Focus IDOL to enhance data safety and control.

Overview

Data breaches. Security infringements. Cyberattacks. These words alone cause trepidation among those charged with protecting classified information and intellectual property at the most secure organizations. Cyberattacks are inevitable as adversaries—whether outside or within an organization—become more skilled and better funded. Organizations also face threats from well-meaning employees who simply clicked on something that appeared legitimate and let in a breach.

Digital Guardian aims to halt data theft with its next-generation data protection platform. For more than 10 years, the Waltham, Massachusetts-based company has helped companies and governments worldwide guard their valuable data assets, which in turn, enhances their reputations and trustworthiness.

"If you want to protect your data, you must know what comprises your inventory of important assets. We rely heavily on the IDOL technology for helping us classify data. Our IDOL solution is a key part of the data protection puzzle."

MARCUS BROWN
Vice President of Corporate Business Development
Digital Guardian

Solution

The firm developed its data protection platform with the IDOL Information & Data Analytics solution to help customers see, analyze, and understand their data.

"Whatever we're trying to protect—personal information or intellectual property—we need to be in the right place to see what people are doing with that data," says Marcus Brown, Vice President of Corporate Business Development at Digital Guardian. "Our risk-based approach focuses on visibility."

The IDOL technology helps customers achieve that visibility by recognizing structured and unstructured files operating on multiple systems. Digital Guardian uses the software for scanning documents, recognizing terminology, and classifying structured information—such as credit card numbers, alphanumeric data, customer specifics, and patient/healthcare details. IDOL software allows Digital Guardian to assimilate and analyze multiple datasets.

"We can recognize regular expressions, such as a type of credit card or Social Security numbers," Brown explains. "We rely on the fact that

DIGITAL GUARDIAN®

At a Glance

- **Industry**
  Software & Technology
- **Location**
  United States
- **Challenge**
  Reduce the risk of data breaches by improving monitoring of sensitive information.
- **Solution**
  Use Micro Focus IDOL, ArcSight and SecureMail to analyze data, detect threats, and classify and encrypt email.
- **Success Highlights**
  + Eliminated as much as 90 percent of data risk and fostered user behavior changes by placing controls and rules in effect
  + Enabled analysis of structured and unstructured data preventing the loss of data and intellectual property
  + Helped organizations classify and guard their valuable data assets, which also enhanced their reputations and trustworthiness
  + Strengthened organizations' security risk profiles and security return on investment

> **"Get the visibility about users, data, and systems. Then leverage that visibility with analytics and tools so that you can profit from an automated kind of intelligence."**
>
> **MARCUS BROWN**
> Vice President of Corporate Business Development
> Digital Guardian

Contact us at:
www.microfocus.com

Like what you read? Share it.

IDOL supports hundreds of languages and many different subject areas. So, we're able to recognize much of what's written in text language using IDOL."

Results

Removing Security Blind Spots

Data recognition and classification are important steps in the process of guarding big data. Digital Guardian's platform monitors each movement of sensitive, top-secret information using customized endpoint agents on PCs, servers, and operating systems, along with network agents, sensors, and appliances on a network. The agents tag sensitive information, and the tag travels with the data wherever it goes. The endpoint agents warn users when they are putting information at risk and block transmission of classified information if a user tries to take it out of the company.

"Our agents sit right in the middle of a business process or application, enabling us to see what the user and application are doing," Brown says. "We're using IDOL, some of our technology, and our vantage point in the business process to figure out what the data is. We're on the end point, which is a blind spot for a lot of security organizations."

Without needing predefined rules or complex configurations beforehand, the platform produces practical risk and trend reports. Digital Guardian customers use the reports enabled by IDOL software in various ways, such as retrieving files and data that a resigning employee may have removed from the company. Or, customers may initiate controls and policy changes to lock down risks. By placing controls in effect, customers can eliminate as much as 90 percent of their data risk and realize changes in user behavior that reduce their data loss profile overall.

"After those controls are in place, within the space of a week you suddenly see the incidence of dangerous actions dropping dramatically," Brown notes. "Our customers experience a stronger security return on investment."

In addition to IDOL, Digital Guardian uses Micro Focus Security ArcSight Security Information and Event Management (SIEM) software. Brown shares that the largest enterprises, governments, and organizations use ArcSight. "ArcSight is the centerpiece of the security operation center. It's where all of the information from all the different security tools comes together, and operators and analysts and responders can work with that data to detect problems and respond to them," he says.

"It was key for Digital Guardian to integrate with ArcSight SIEM, which is very much the nerve center for so many of our customers in the security operations center. Our customers have really benefited from having the visibility of the end point and the network and the data that we provide. They're able to do a lot more in ArcSight around insider threat and around detecting advanced external threats."

Brown explains, "The main benefit our customers have seen from using ArcSight is that they've been able to zoom in and detect threats that are landing on an end point very quickly and respond to those threats automatically. Customers have become more secure by leveraging the visibility of data, users, and malicious processes on the end point, on the network, and bringing that into the SIEM to detect threats much faster and respond to them more quickly."

Digital Guardian also integrates with Micro Focus's Voltage SecureMail email encryption solution, providing customers with automated email classification, data loss prevention, and encryption. The integrated solution supports both onpremise and cloud versions of SecureMail, and helps enterprises simplify regulatory compliance and data protection deployments.

Digital Guardian's platform incorporates analytics, tools, and agents that come together brilliantly to improve the security posture of data-driven organizations. For enterprises that may be struggling with standard technologies on the end point that don't comprehensively identify and secure sensitive and intellectual property information, Brown offers this advice.

"Get the visibility about users, data, and systems. Then leverage that visibility with analytics and tools so that you can profit from an automated kind of intelligence."

Learn more at
www.microfocus.com/IDOL