identityfinder

Identity Finder Customer Case Study

University Finds and Protects Sensitive Data

Customer: University
Staff: 10,000
Students: 20,000
Industry: Higher Education

Profile: An established and renowned private University with many divisions and separate technology infrastructures.

Software:
- Identity Finder Enterprise Edition
- Identity Finder Management Console

"We found that Identity Finder was best in the marketplace because it offloaded the work to the end user in a friendly way."

- Security Specialist, Higher Education Customer

Identity Finder has helped hundreds of organizations find and protect personally identifiable information (PII). The following case study analyzes an actual business need and the subsequent technical evaluation and technology deployment of Identity Finder software. Per customer request, all references have been removed.

Business Need

A higher education University customer used Social Security Numbers (SSNs) in day-to-day processes to track students, but in 2007 it implemented a policy to replace this sensitive data with institution specific numbers. This policy would prevent usage of SSNs going forward, but the historic use of SSNs left instances of exposed data throughout the system. As such, the institution also needed to clean its existing machines.

The University instituted an initiative to protect students' personally identifiable information (PII) and prevent data breaches. Such incidents could typically result in costly, legally mandated, public disclosures.

Spearheading this effort was a division which has a technical and physical infrastructure spread out over fifty departments, some of which have their own IT infrastructure, supporting thousands of employees.

The division initially tried using open source and home grown tools, but encountered many challenges such as lack of: scalability, manageability, remediation capabilities, extensibility, ease of use, and centralized reporting. As a result of these requirements, the University initiated a one year product evaluation on an internal test environment to find an application that accurately and effectively allowed for identification and remediation of sensitive data.

Product Evaluation

Although interested in centralized reporting, the University specifically sought out the ability to empower its employees to identify and remediate PII rather than centrally performing this effort. It defined PII as:

- Social security numbers
- Credit card numbers
- Dates of birth
- Passwords
- Bank account numbers
- Other internally defined custom data types

The University had many evaluation criteria, including:

- Minimizing false positives
- Minimizing false negatives (missed valid matches)
- Maximing scanning performance
- Simplifying marking of false positives
- Maximizing file formats scanned

During its evaluation, they reviewed many commonly used tools and data leakage prevention products. The University set up a test environment with numerous files and file types that contained PII. They also forged data that appeared real but were not actually legitimate instances. In doing so, they could run applications and judge the performance against a known set of data.

Choosing Identity Finder

The University chose Identity Finder because its features met or exceeded their needs in each area. In addition, the ease of management was particularly compelling. They were excited that the entire solution was downloadable and installed by their IT staff within minutes.

Client Software Features

- Allows end users to sort, search, and control their own scan results
- Presents end user with remediation options within the tool itself
- Allows remotely searching of remote locations like databases, websites, and other desktops
- Supports multiple platforms (PC and Macintosh client)

Management Console Features

- Tracks installations and manages remote clients
- Provides centralized reporting to senior management
- Gives staff visibility into client usage

Impact

- Ease of use meant users actually acted on data discovered
- Requested features continued to be added during evaluation period (i.e. Redact PII)

Furthermore, the total cost of ownership was significantly reduced because the Identity Finder solution did not require them to purchase any additional hardware nor did it require any professional services for setup and configuration.

Deployment

The University installed the Identity Finder Enterprise Client on every staff and faculty's machine and installed a single Identity Finder Management Console. The Console was configured to perform aggregate data reporting but not collect PII matches because the administrators did not want to see actual user data. The console centrally reported on which machines had excessive sensitive data, what remediation actions users had taken, and how often they performed a search. They could then work with the data owners to reduce exposure.

Identity Finder's Management Console also allowed the University to produce a report card on the institution's exposure to PII. The trend reports over periods of time helped them understand how their policies were performing and whether they needed to become more aggressive in their remediation efforts.

Benefits

The University identified numerous side benefits from using the Identity Finder solution, including its:

- Ability to encrypt data matches, a feature which leverages native encryption for securing most file types
- Use of encrypted connections to the central server over port 80, minimizing firewall issues
- Ability to schedule scans
- Ability to automatically update
- Ability to seamlessly integrate into the organization's existing infrastructure
- End user wizard, practically eliminating need for any special training
- Integration capability with other client programs to open secured files

During incident response after a potential breach, the University also found it could use Identity Finder to quickly and accurately determine whether backup images of the data contained sensitive information and whether additional follow up actions or disclosures were necessary.

identityfinder