Masking Sensitive Data with Reflection Desktop

Most data-privacy violations are attached to someone you trust: The healthcare worker who is selling VIP details to the tabloids. An accounts payable employee who is inappropriately changing billing information. A bank teller who is passing stolen social security or credit card numbers to co-conspirators. These days, it can be hard to tell an upstanding employee from a crooked fraudster.

Reflection Desktop at a Glance

- **Connectivity:**
  Connect desktop and mobile users to host systems.
- **Ease of Use:**
  Make host apps as easy to use as Office apps.
- **Manageability:**
  Manage user configurations with ease.
- **Security:**
  Use layers of security to shield data in motion and at rest.

This product flyer tells how OpenText™ Reflection Desktop software can help you prevent data-privacy violations—without any changes to your host applications.

Why Malicious Insiders Get Away with It

Insider fraud is hard to detect. Traditional controls, focused on preventing attacks from the outside, are powerless against savvy insiders with legitimate access to confidential data.

Once a disgruntled or dishonest insider has the necessary access privileges, the risk of misconduct soars. In the most recent year on record, U.S. organizations lost $40 billion to employee theft and fraud. According to market research company Forrester, 46 percent of nearly 200 technology decision-makers cited internal breaches as the most common type of breach they experienced in the past year, and half of those respondents said malicious insiders were to blame.*

Why haven't organizations done more to protect themselves? The answer is simple: Changing entrenched host applications to make them more secure is difficult, risky, and expensive. Even if you're lucky enough to find an expert who understands mainframe platforms, it's dangerous to mess around with the business logic, written and augmented over time, that runs your company. The costs and disruption involved are prohibitively high.

An Easy First Step

The question is, how can you protect your customers and your company without revamping host systems and business processes that have taken decades to develop? How can you move your company into the new world of security?

Generally speaking, you want to add layers of security. It's a best-practice approach that you can carry out in phases. In the IBM mainframe and AS/400 world, there's an easy first step you can take. It's called data masking.

Data masking gives you the ability to prevent users from viewing sensitive data on a host screen, copying it to a piece of paper, taking a picture of it, printing it, or sending it via email. It masks the data on the screen, in real-time, so that employees can never see a full address, date of birth, credit card number, social security number, or any other private information. What they see is just enough to do their jobs. Period.

Reflection Information Privacy Technology

If you're a Reflection Desktop customer, you already have data masking capabilities

* *Keanini, TK. (2015). Why insider threats are still succeeding. Information Age. Retrieved January 25, 2016, from:* **www.information-age.com/technology/security/123459548/why-insider-threats-are-still-succeeding**

right at your fingertips.OpenText™ Reflection Enterprise Suite's data masking technology gives you the ability to easily mask any type of data on host screens—without making changes on the host side.

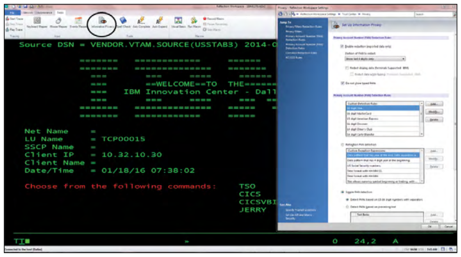
Reflection Enterprise Suite data masking is accomplished through the use of privacy filters and Primary Account Number (PAN) rules within the Reflection Information Privacy Tool:

- **Privacy filters**—You can create custom privacy filters that enable you to mask data on IBM mainframe and AS/400 application host screens. You can also apply different rules to these filters—enabling you to mask data as it's displayed, as it's being typed, and as it's leaving the screen (print screen, copy/paste, and screen scraping with API/macros).
- **PAN rules**—With PAN rules, you can configure Reflection to mask all or part of a credit card number on a host screen by checking the appropriate boxes. Reflection Enterprise Suite uses patent-pending technology to identify and validate PANs. It also uses the Luhn algorithm to ensure that all credit card numbers are hidden from view no matter where or how they are displayed. Users and administrators can choose a range of control options—from basic credit card recognition to complex customizations—to fit their business needs.

Here are some examples of what OpenText™ customers have been able to do using Reflection Enterprise Suite privacy filters and PAN rules:

- Mask an entire column of data.
- Mask personal financial data fields.
- Mask only the last six digits of a variable-length field.
- Mask a data field that appears in multiple places on the same screen.
- Mask data based on basic conditional instances (e.g., based on data fields or screen identifiers).
- Mask data based on complex conditional instances (e.g., using if, then, and else type conditions).
- Mask diverse PANs, including those with different lengths, prefixes, and dash positions.
- Mask data that is displayed between two separate values.
- Provide varying levels of visibility based on a user's role or job function.

Reflection Enterprise Suite's data masking capabilities are unmatched by any other terminal emulation client. They also provide a low-risk solution that you can easily implement. Learn more about setting up information privacy with Reflection Desktop at **https://docs.attachmate.com/reflection/16.0/info-privacy.pdf**.



```
 Source DSN = VENDOR.VTAM.SOURCE(USSTAB3) 2014-0

              =======   ============   ======
              =======   =============  =======
                ===       ===    ====  ======
                ===       ==WELCOME==TO  THE======
                ===    IBM Innovation Center - Dall
                ===       ===    ====   ===  ==
              =======   =============  =====   =
              =======   ============   =====

  Net Name    =
  LU Name     = TCP00015
  SSCP Name   =
  Client IP   = 10.32.10.30
  Client Name =
  Date/Time   = 01/18/16 07:38:02

  Choose from the following commands:    TSO
                                         CICS
                                         CICSVBI
                                         JERRY

TI■                         »                         0   24,2   A
```

Figure 1. Filters and rules are stored in files, which makes it easy for you to manage them by role or user group.

Changing the Threat Landscape

Every organization must face this disconcerting truth: Within its walls are people who may use their privileged access rights to commit damaging privacy violations. But traditional approaches to new threats perpetuated by increasingly sophisticated insiders no longer work. Your risk management strategy must evolve if it is going to be effective.

Reflection Enterprise Suite's built-in data masking capabilities provide a low-risk, easy-to-implement step in the right direction. Without requiring any host application rewrites, these capabilities will protect your data and facilitate regulatory compliance at the same time.

Learn more at
www.opentext.com

Connect with Us

Getting Compliant with PCI DSS

The Reflection Information Privacy Tool does more than mask data on host screens. Just by checking the right boxes, you can require encrypted connections on all networks, including wireless networks. You can track the viewing of credit card numbers by any user. And you can generate detailed reports as needed. In these ways, the tool helps to facilitate PCI DSS compliance. Learn more at **www.attachmate.com/library/docs/advance-your-pci-compliance-with-reflection-desktop.html**.