

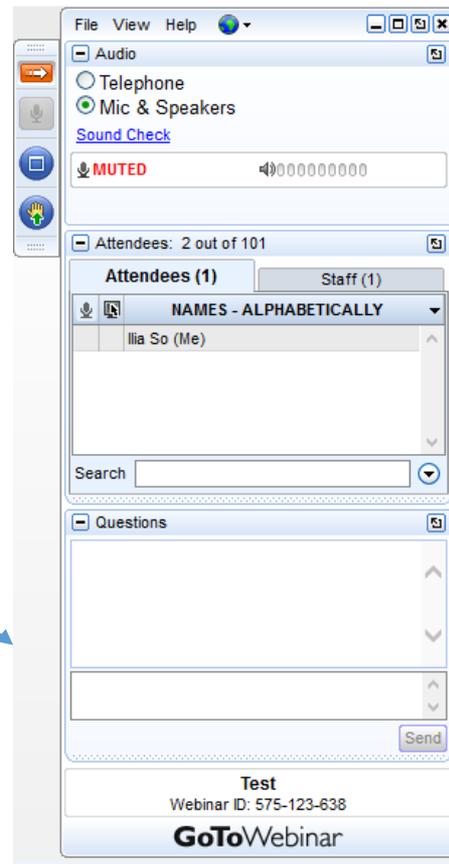
Mitigating the Threat of Data Theft by Departing Employees



Russell McDermott
Systems Engineer
Russell.McDermott@netwrix.com

How to Ask Questions

Type your question here



Click "Send"

Agenda

- Can departing employees really do it?
- Notorious data breaches
- Checklist: offboarding
- Be aware of what can happen
- 7 oddities in user behavior to keep an eye on
- Product demonstration
- Questions and answers

Can Departing Employees Really Do It?

- 30% of departing employees would take company documents and other information they haven't personally created
- 20% of departing employees would take data because of anger or dissatisfaction and would be more likely to pass it to a competitor
- 90% of employers did not have a policy or technology in place to prevent them from stealing data¹

Data at risk:

- Source code
- Patent filings
- Business critical data
- Customer data, including names, phone numbers, email addresses, bank accounts, etc.

¹ <https://www.entrepreneur.com/article/272319>

Notorious Data Breaches

2017 Facebook-ZeniMax

Ex-employees were accused of stealing the ZeniMax online code and using it for Facebook. Fine — \$500 M

2016 Zynga

Two ex-employees stole sensitive data during Independence Day. They tried to cover traces and delete 24,000 folders and documents

2016 The US Office of the Comptroller of the Currency

Before retirement, the employee downloaded more than 10,000 records about the regulator's activities

Checklist: Offboarding

IT Security Department

Done

- Notify systems administrators of account suspension and archiving
- Terminate all accounts (VPN, email, network logins, cloud services, specialized applications, company-owned social media site accounts, backup accounts)
- For departing privileged users, change all passwords to shared accounts, service accounts, network devices (routers, switches, etc.), test accounts, jump boxes, etc.
- Collect remote access tokens (two-factor authentication devices)
- Update access lists to sensitive areas (server rooms, data centers, backup media access, etc.)
- Remove employee from all the distribution lists and automated alerts

Checklist: Offboarding

Records Department

Done

- Ensure a departing employee returns all equipment, such as laptop, tablet, netbook, and smartphone.
- Verify returned equipment against inventory
- Ensure a departing employee returns any company-owned or controlled documents

Physical Security Department

- Collect identification badge, keys, access cards, parking pass, etc.
- Provide security debriefing

Checklist: Offboarding

HR Department

- Obtain forwarding mailing address
- Complete offboarding paperwork
- Notify organization of separation
- Reaffirm any IP (intellectual property) and NDA (non-disclosure) agreement

Done

-
-
-
-

Be Aware of What Can Happen



Sensitive data theft in order to blackmail the company or to sell it to the competitor



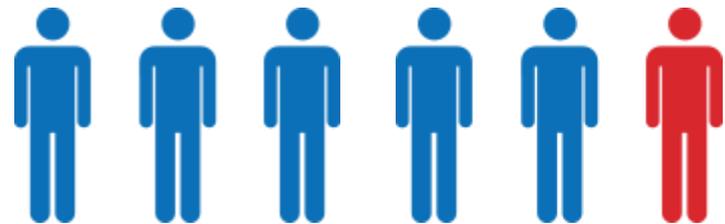
Critical business data deletion to wreak havoc in company's business processes



Credential and password changes to gain control over critical assets

Seven Oddities to Keep an Eye On

- Someone is **actively** accessing data
- Someone has undertaken too many **failed access attempts** to access data
- Someone is actively accessing **stale** data
- Someone is accessing data **outside business hours**
- Someone is trying to log in from **different endpoints**
- Someone has created **new user accounts**
- Someone is massively **deleting data**





Demonstration



About Netwrix Auditor



Netwrix Auditor

A **visibility** and **governance** platform that enables control over **changes, configurations, and access** in hybrid cloud IT environments by providing **security analytics** to detect anomalies in user behavior and investigate threat pattern before a data breach occurs.

Netwrix Auditor Applications



Netwrix Auditor for
Active Directory



Netwrix Auditor for
Azure AD



Netwrix Auditor for
Exchange



Netwrix Auditor for
Office 365



Netwrix Auditor for
Windows File Servers



Netwrix Auditor for
EMC



Netwrix Auditor for
NetApp



Netwrix Auditor for
SharePoint



Netwrix Auditor for
Oracle Database



Netwrix Auditor for
SQL Server



Netwrix Auditor for
Windows Server



Netwrix Auditor for
VMware

A large blue vertical bar is positioned to the left of the title. The title "About Netwrix Corporation" is written in a blue, sans-serif font.

About Netwrix Corporation

The text "Year of foundation:" is displayed in white, sans-serif font against a dark background of palm trees and a building.

Year of foundation:

The year "2006" is displayed in white, sans-serif font against a dark background of palm trees and a building.

2006

The text "Headquarters location:" is displayed in white, sans-serif font against a dark background of palm trees and a building.

Headquarters location:

The location "Irvine, California" is displayed in white, sans-serif font against a dark background of palm trees and a building.

Irvine, California

The text "Global customer base:" is displayed in white, sans-serif font against a dark background of palm trees and a building.

Global customer base:

The number "over 7000" is displayed in white, sans-serif font against a dark background of palm trees and a building.

over 7000

The text "Recognition:" is displayed in white, sans-serif font against a dark background of palm trees and a building.

Recognition:

The text "Among the fastest growing software companies in the US with 95 industry awards from Redmond Magazine, SC Magazine, Windows IT Pro and others" is displayed in white, sans-serif font against a dark background of palm trees and a building.

Among the fastest growing software companies in the US with 95 industry awards from Redmond Magazine, SC Magazine, Windows IT Pro and others

Netwrix Customers

Financial



State, Local Government/Education



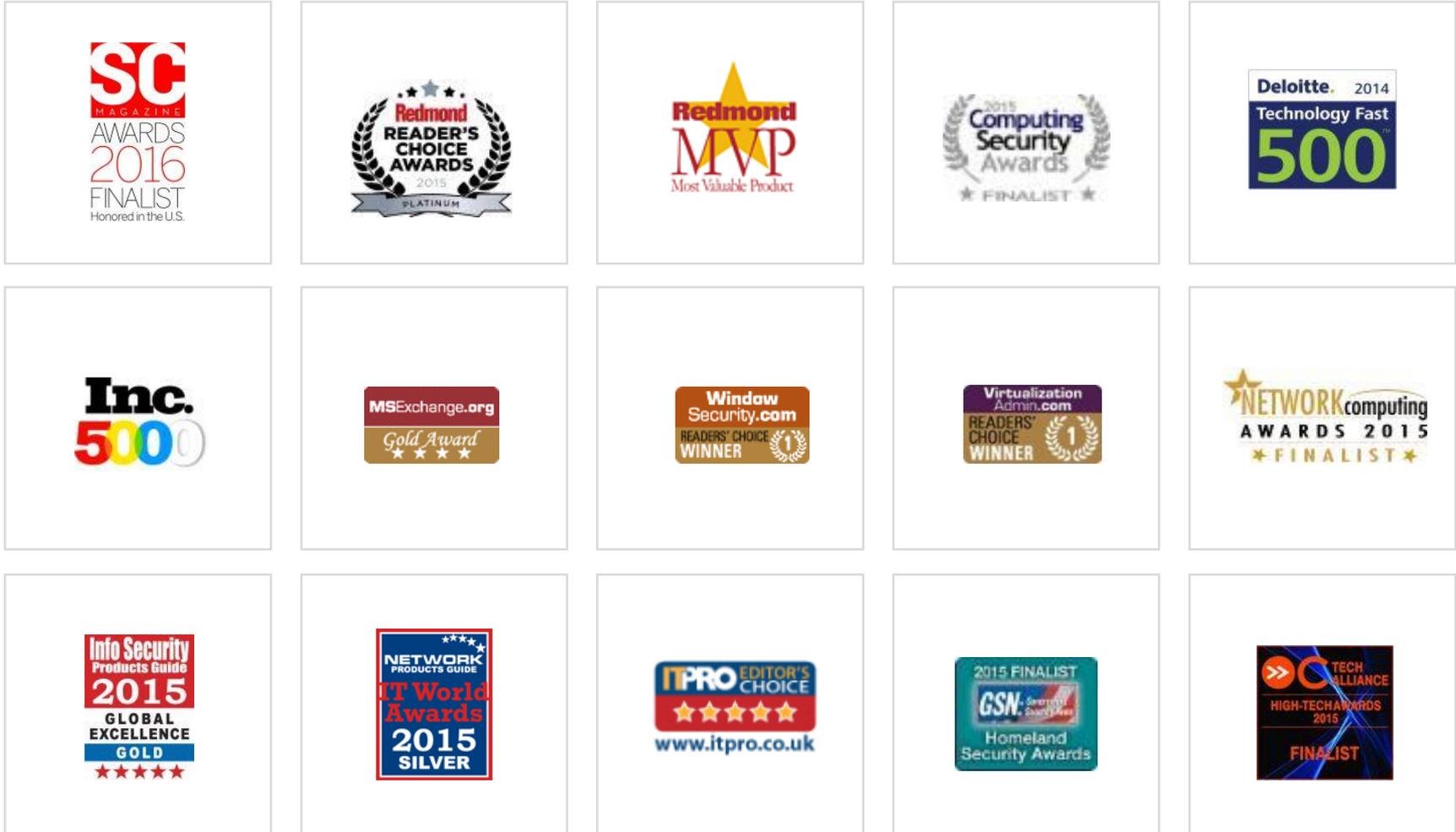
Heavy Industry/Engineering/Manufacturing/Transportation



Technology/Internet/Retail/Food/Other



Awards



Next Steps

Free Trial: setup in your own test environment:

- On-premises: netwrix.com/freetrial
- Virtual: netwrix.com/go/appliance
- Cloud: netwrix.com/go/cloud

Test Drive: virtual POC, try in a Netwrix-hosted test lab netwrix.com/testdrive

Live Demo: product tour with Netwrix expert netwrix.com/livedemo

Contact Sales to obtain more information netwrix.com/contactsales

Webinars: join our upcoming webinars and watch the recorded sessions

netwrix.com/webinars

netwrix.com/webinars#featured

Thank You!

