Remote Worker Accessing Sensitive Data

RISK

Insecure Public WiFi Networks

Dan from Finance attempts to use the free wireless network at a coffee shop to download sensitive business documents.

SOLUTION

Trusted Network Awareness

Dan is denied access and advised to use a secure VPN connection via a Digital Guardian real-time user prompt.

Incoming Phishing Email

RISK

Advanced Malware

Jen receives a phony email, seemingly from her bank, saying there's an account issue and providing an attachment to learn more.

SOLUTION

Malware Protection with Real-time Phishing Detection

Digital Guardian alerts Jen that the attachment is suspicious, blocks her from opening it, and alerts IT of the suspected malware attack.

Uploading Sensitive Data to a Cloud Application

RISK

Insecure Web Applications

Tricia attempts to upload sensitive files to her Dropbox so that she can access them from her own laptop at home.

SOLUTION

Web Applications and Cloud Storage Control

Digital Guardian recognizes that Tricia is trying to send sensitive data to an unauthorized web application and blocks the upload.

Systems Administrator Downloading Sensitive Files

RISK

Unrestricted Insider Access to Data

Joe, an IT administrator with root access, is leaving the company and tries to download sensitive design documents to take with him.

SOLUTION

Privileged User Control

Digital Guardian allows proper file access for the privileged user, but blocks his attempt to download the sensitive files and alerts staff of the incident.

Downloading Corrupted Web Software

RISK

Drive-by Malware

Susanne in Marketing searches the web for photo editing software. She visits a compromised website and is redirected to a malicious site that starts downloading malware to her machine.

SOLUTION

Application Control

The malware attempts to execute a variety of processes on its own. Digital Guardian detects this activity immediately and automatically blocks the malicious application from running.

Accidental Emailing of Sensitive Data

RISK

Emailing Sensitive Data

Kevin from Accounting attempts to send payment information via email and MS Outlook auto-populates an unapproved external recipient.

SOLUTION

Email Control & Encryption

Kevin clicks send and a real-time Digital Guardian prompt alerts him of the unapproved recipient and requests justification for the action.

Copying Engineering Drawings to a USB Drive

RISK

Insecure External Devices

Michelle from Engineering downloads a sensitive CAD file to her USB device to work on it from home later.

SOLUTION

Device Control & Encryption

Digital Guardian automatically encrypts the file prior to copying it to the USB. The file now can only be opened with a decryption key.

Malicious Insider Modifying Confidential Files

RISK

Malicious Insider Modifying Confidential Files

Bill is interviewing with a competitor, so he copies confidential information from a file on a shared network drive and saves it as a new file on his machine.

SOLUTION

Automatic Data Classification

Digital Guardian recognizes that the data was copied from a sensitive file and automatically applies the "Confidential" tag from the source file. This ensures that the new file is protected and can't leave the company.