Forcepoint Cloud Threat Assessment Report

PREPARED FOR ABC CORPORATION – OFFICE365 AND BOX

CONFIDENTIAL

10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin, TX 78759, USA

Published 2017

1 | Overview

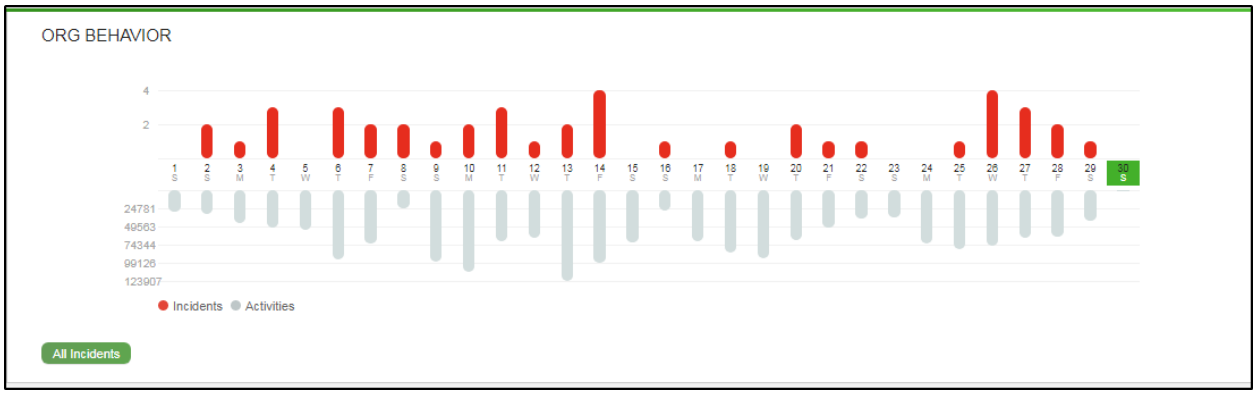
Forcepoint Cloud Access Security Broker (CASB) provides unrivaled visibility and control for cloud applications.

Forcepoint CASB delivers critical risk discovery for Shadow IT, compliance and security controls over sanctioned applications, and employs advanced cloud User Behavior Analytics (UBA) to detect and mitigate threats. With Forcepoint CASB, users get the applications they want and IT staff gets the control they need.

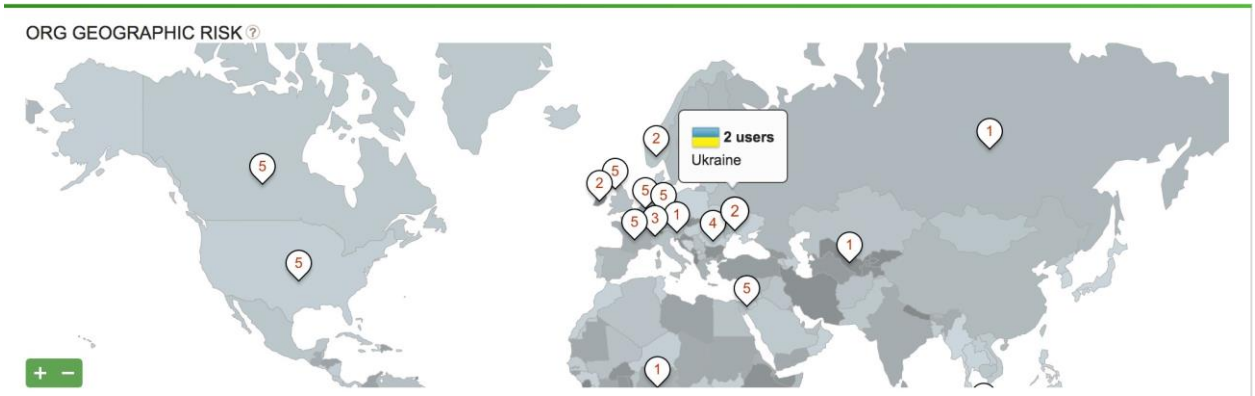
The following report contains analysis for ABC Corporation's use of Microsoft Office365 and Box.com. The analysis was performed during the period of Nov 1st to November 17th, 2017. During that period, the system analyzed over 598,287 user activities. Advanced statistical observations help establish the organization's behavioral benchmark and allow quick and automated detection of anomalous behavior or deviation from expected business flows.

The following provides specific examples of presented risks.

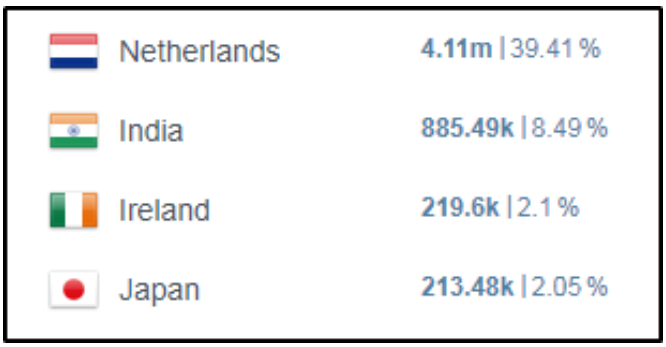
Overall cloud service usage pattern – for both benign and suspect activities (incidents)



Geographic analysis displays easy detection of business flow outliers from regional areas:



Top Active Locations



Least Active Locations

Cross referencing this information with understanding of the user activity will provides specific questions/observations. For example, why would an employee be accessing the Box administrator settings from the Ukraine when we have no users or presence there?

Privileged User Assessment

Twelve administrators were detected to be configured with Administrative privileges. Security best practices recommend **limiting** the number of such privileged users for cloud services. Here is the list of administrators detected:

- corinne.king@extremeguitars.net
- devin.eldred@extremeguitars.net
- sales@extremeguitars.net
- dorothy.wilson@extremeguitars.net
- corinne.king@extremeguitars.net
- devin.eldred@extremeguitars.net
- sales@extremeguitars.net
- dorothy.wilson@extremeguitars.net
- corinne.king@extremeguitars.net
- devin.eldred@extremeguitars.net
- sales@extremeguitars.net
- dorothy.wilson@extremeguitars.net

Dormant users

Four users have not logged in to the service for over 90 days. These dormant users cost your organization extra money and may also pose a security risk should they do not require this resource to perform their daily functions, yet still have access to it. The users are:

- corinne.king@extremeguitars.net
- devin.eldred@extremeguitars.net
- sales@extremeguitars.net
- dorothy.wilson@extremeguitars.net

2 | Top High--Risk Users

The following individuals were highlighted as top risks for your organization during the analysis period. These users conducted a pattern of usage which were detected as potentially suspect, anomalous, and thus have been recommended for analysis above all other users or incidents.

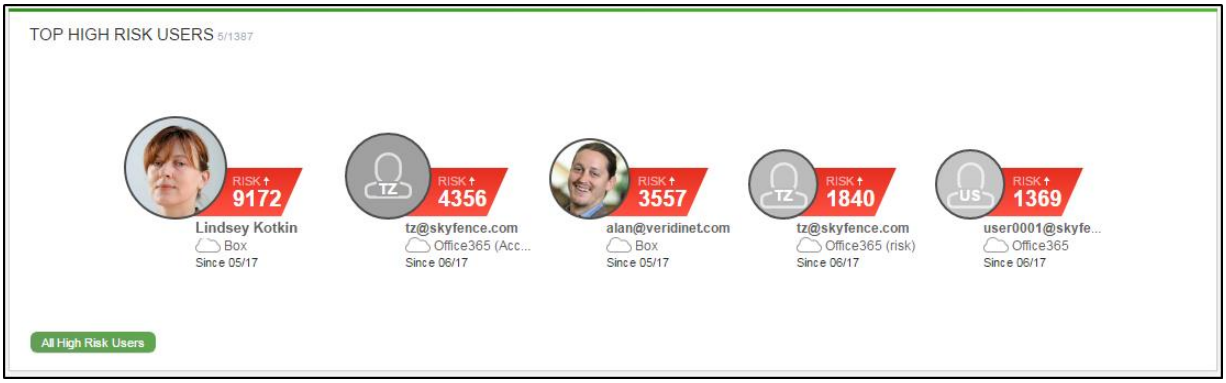


Figure 1 - Top Risk Users

Risk reports can also be presented for all users – Figure 2

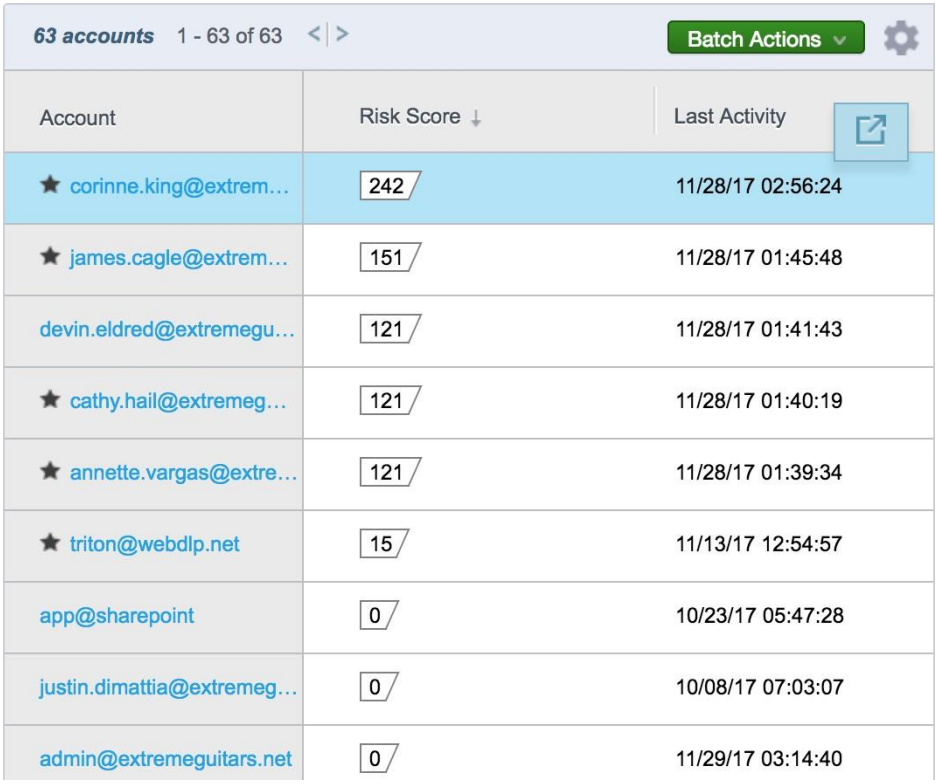


Figure 2

3 | Risk Analysis

This section contains detailed information about the behavior patterns of the top two users determined to be the riskiest to your organization.

Carefully review the behavior pattern by checking the activity (all user activity) and the incidents (user activity matched by the CASB anomaly rules) over the period of the analysis.

- Examine the incident timeline reflecting the anomalies and risky activity detected over time.
- Check the user typical locations and the devices used to access the system.

A typical behavior is detailed in the below image (Figure 3). This user typically:

- works from specific locations
- utilizes specific company issued and/or personal devices
- performs specific activities
- operational within specific time of the day
- conforms to peer activities (peer / OU data requires AD connectivity)

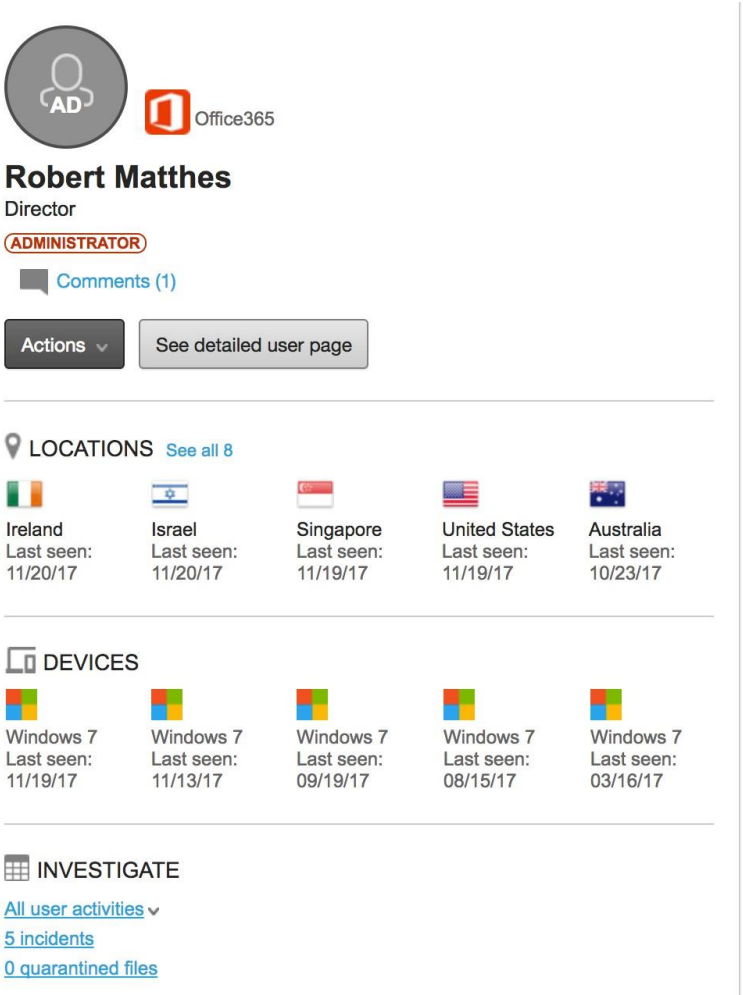


Figure 3

Easily seen from the timeline below, 27 incidents were detected in this account. These incidents contribute to this individual's risk score. The score is based on the severity of the activity, and **also** on the impact of a potential breach (e.g. if this user has an administrator account, sensitive data ownership, shadow IT consumption, etc) the potential damage is much larger than that of a peer user with different permissions or data ownership. (Figure 4)

Figure 4

These individuals as identified as owners of sensitive data stored within this cloud application and recommend closer analysis of appropriate ownership. (Figure 5)

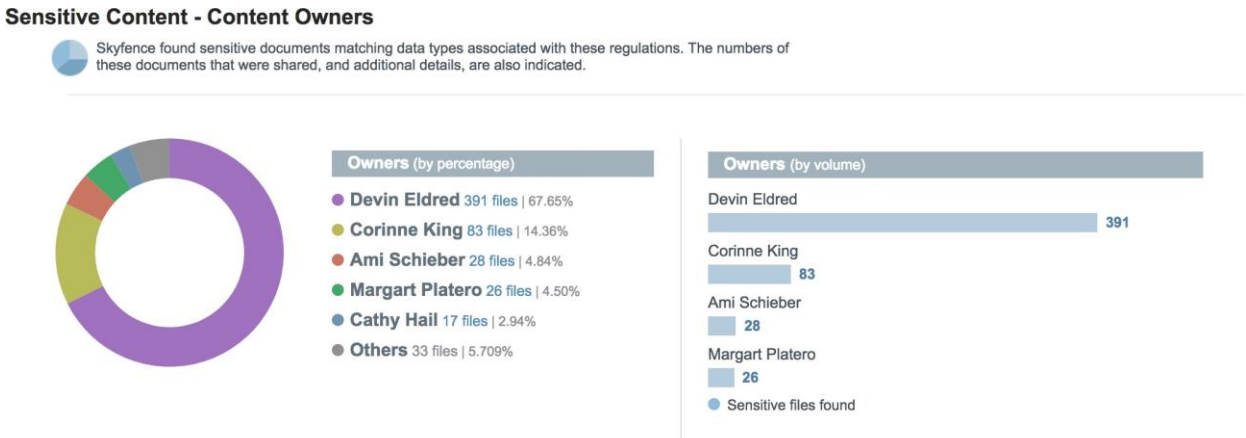
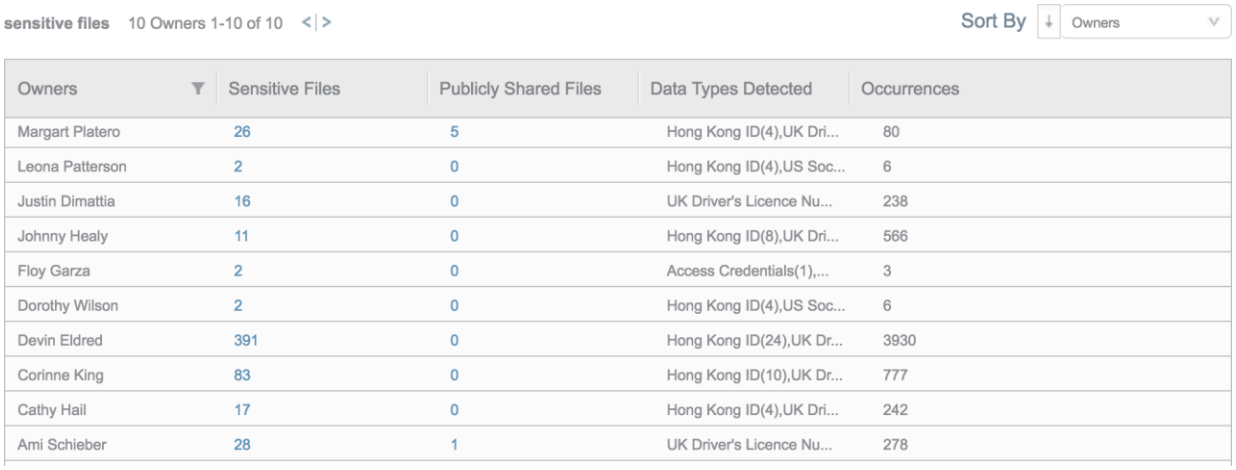


Figure 5

In-appropriate or accidental collaboration often presents the highest risk to organizations storing data in the cloud. We recommend a close examination of **Publicly Shared** files containing sensitive and regulated data. (Figure 6)



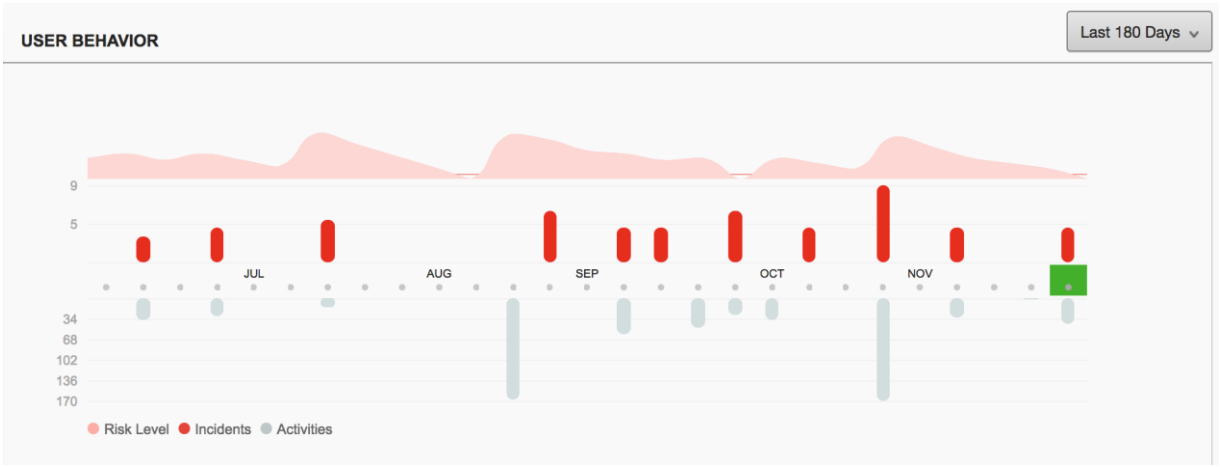
sensitive files 10 Owners 1-10 of 10 < | >

Sort By Owners

Owners	Sensitive Files	Publicly Shared Files	Data Types Detected	Occurrences
Margart Platero	26	5	Hong Kong ID(4),UK Dri...	80
Leona Patterson	2	0	Hong Kong ID(4),US Soc...	6
Justin Dimattia	16	0	UK Driver's Licence Nu...	238
Johnny Healy	11	0	Hong Kong ID(8),UK Dri...	566
Floy Garza	2	0	Access Credentials(1),...	3
Dorothy Wilson	2	0	Hong Kong ID(4),US Soc...	6
Devin Eldred	391	0	Hong Kong ID(24),UK Dr...	3930
Corinne King	83	0	Hong Kong ID(10),UK Dr...	777
Cathy Hail	17	0	Hong Kong ID(4),UK Dri...	242
Ami Schieber	28	1	UK Driver's Licence Nu...	278

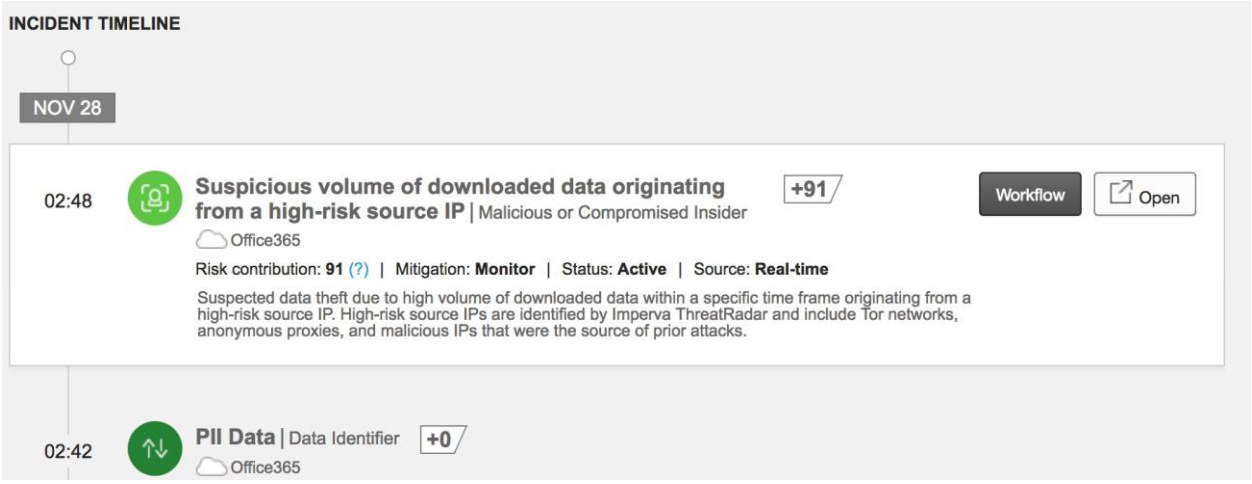
Figure 6

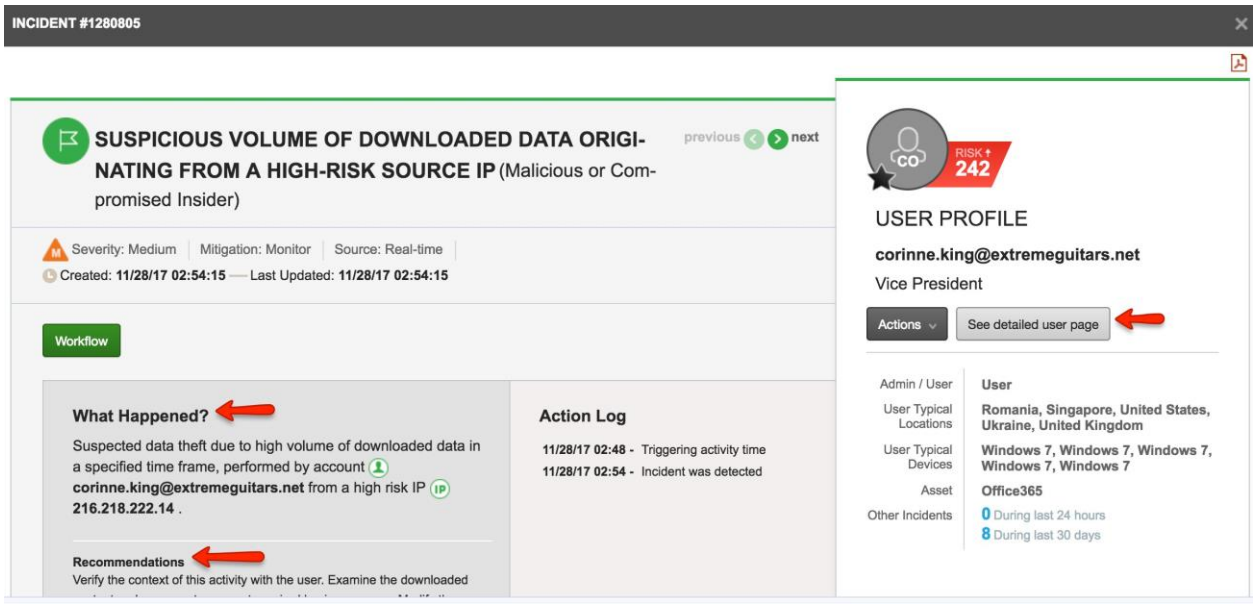
Reviewing user incident timeline also provides a detailed picture of what has occurred and the appropriate actions which should be taken:



These incidents represent threats detected during the analysis. Examine them carefully to understand the potential risks that Forcepoint CASB can detect.

Note the two interesting incidents below. Review the “What happened?” section to understand the nature of the threat to your organization and then read the “recommendation” section for a suggested response flow. Learn more about the alerts which are the source for this incident and understand the timeline for this single attack.





4 | Summary and Proposal

The explosive growth of cloud adoption, “cloud first” initiatives and BYOD have created security and compliance blind spots. As part of our human-centric approach to security, Forcepoint CASB helps eliminate those blind spots by giving you visibility into -- and control over -- your users’ devices and cloud apps, letting you understand the rhythm of your people and the flow of your data.

Forcepoint CASB not only lets you discover and assess risk from unsanctioned cloud apps, you can also control how sanctioned cloud apps are used, so you can prevent the loss of critical data and IP.

With the Risk Assessment successfully completed, it would be our pleasure to engage in discussion regarding a commercial proposal to address these findings.

Sincerely,

Your Forcepoint team

Protecting the human point is both Forcepoint's vision and the focus of our products.