



PROTECTING THE  
**HUMAN** POINT.

# Forcepoint Cloud Threat Assessment Report

PREPARED FOR ABC CORPORATION – OFFICE365 AND BOX  
CONFIDENTIAL

© 2017, Forcepoint  
All rights reserved.  
10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin, TX 78759, USA

Published 2017

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Forcepoint. Every effort has been made to ensure the accuracy of this manual. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

# 1 | Overview

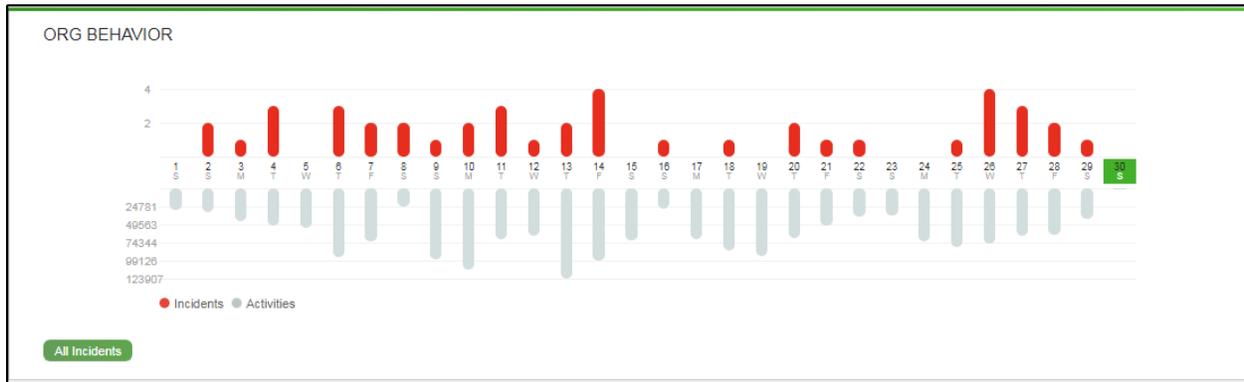
Forcepoint Cloud Access Security Broker (CASB) provides unrivaled visibility and control for cloud applications.

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.

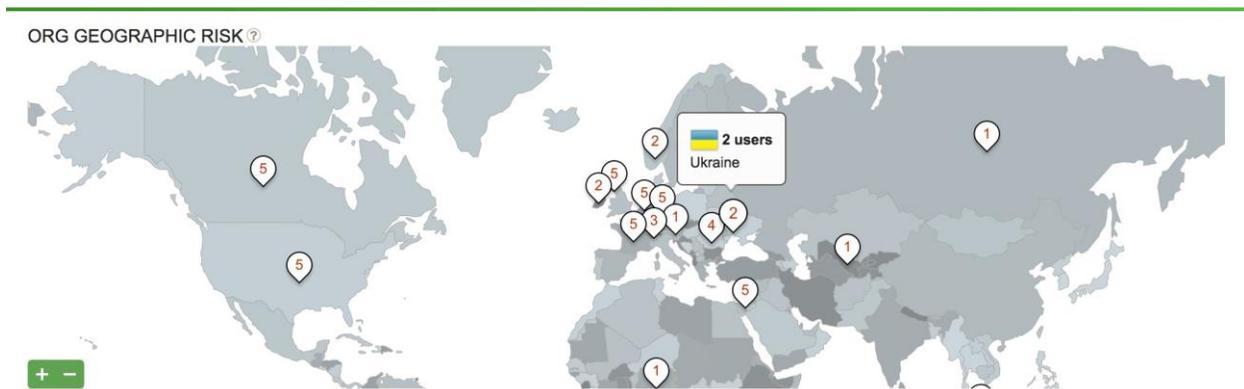
The following report contains analysis for ABC Corporation's use of Microsoft Office365 and Box.com. The analysis was performed during the period of Nov 1st to November 17<sup>th</sup>, 2017. During that period, the system analyzed over **598,287** user activities. Advanced statistical observations help 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

 Netherlands	4.11m   39.41 %
 India	885.49k   8.49 %
 Ireland	219.6k   2.1 %
 Japan	213.48k   2.05 %

### Least Active Locations

 Afghanistan	1   0 %
 Kyrgyzstan	1   0 %
 Georgia	1   0 %
 Cuba	1   0 %

*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.

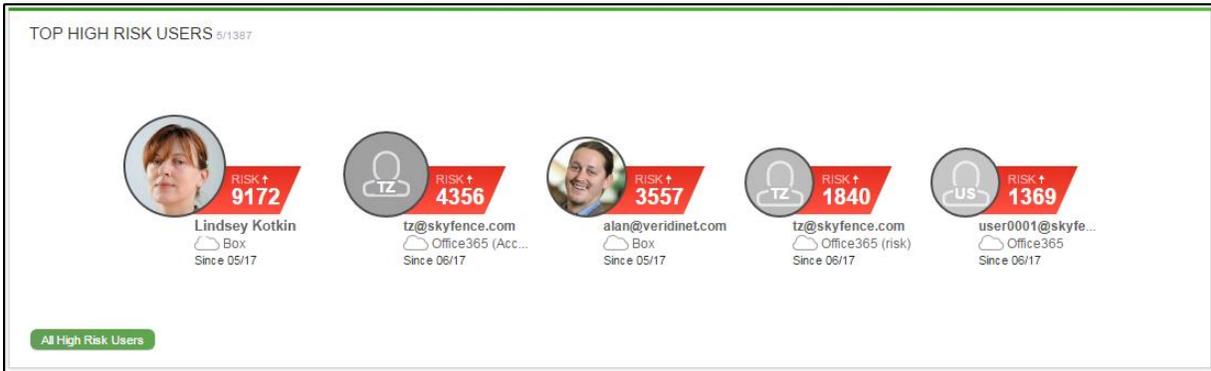


Figure 1 -- Top Risk Users

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

63 accounts 1 - 63 of 63 <   >			Batch Actions	Settings
Account	Risk Score ↓	Last Activity		
★ corinne.king@extrem...	242	11/28/17 02:56:24		
★ james.cagle@extrem...	151	11/28/17 01:45:48		
devin.eldred@extremegu...	121	11/28/17 01:41:43		
★ cathy.hail@extremeg...	121	11/28/17 01:40:19		
★ annette.vargas@extre...	121	11/28/17 01:39:34		
★ triton@webdlp.net	15	11/13/17 12:54:57		
app@sharepoint	0	10/23/17 05:47:28		
justin.dimattia@extremeg...	0	10/08/17 07:03:07		
admin@extremeguitars.net	0	11/29/17 03:14:40		

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)

The screenshot displays a user profile for Robert Matthes, a Director and Office365 Administrator. The profile includes a name, title, and role. Below the profile information, there are sections for 'LOCATIONS' and 'DEVICES'. The 'LOCATIONS' section lists five locations: Ireland, Israel, Singapore, United States, and Australia, each with a flag icon and a 'Last seen' date. The 'DEVICES' section lists five Windows 7 devices, each with a Windows logo icon and a 'Last seen' date. At the bottom, there is an 'INVESTIGATE' section with links for 'All user activities', '5 incidents', and '0 quarantined files'.

Location	Last seen
Ireland	11/20/17
Israel	11/20/17
Singapore	11/19/17
United States	11/19/17
Australia	10/23/17

Device	Last seen
Windows 7	11/19/17
Windows 7	11/13/17
Windows 7	09/19/17
Windows 7	08/15/17
Windows 7	03/16/17

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)

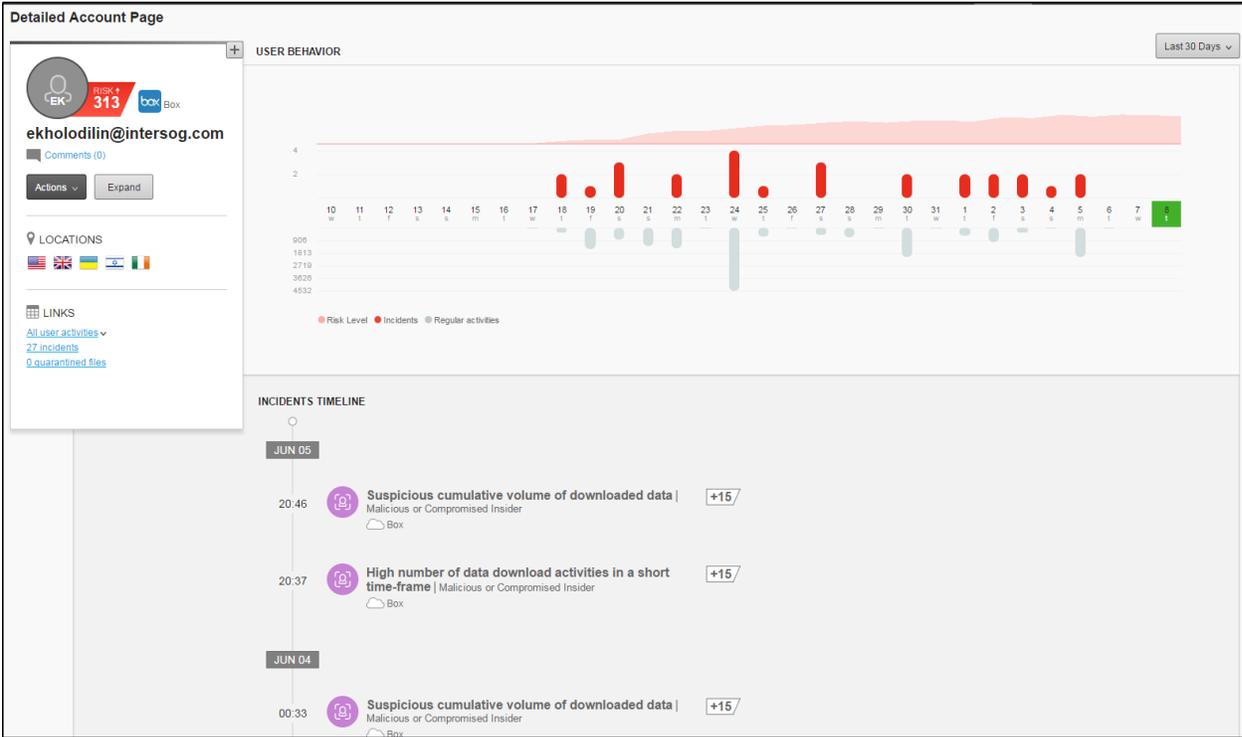


Figure 4

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

**Sensitive Content - Content Owners**

Skyfence found sensitive documents matching data types associated with these regulations. The numbers of these documents that were shared, and additional details, are also indicated.

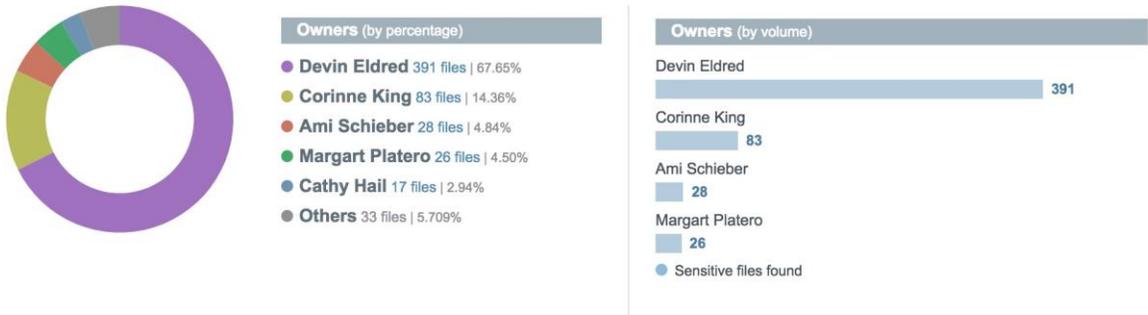


Figure 5

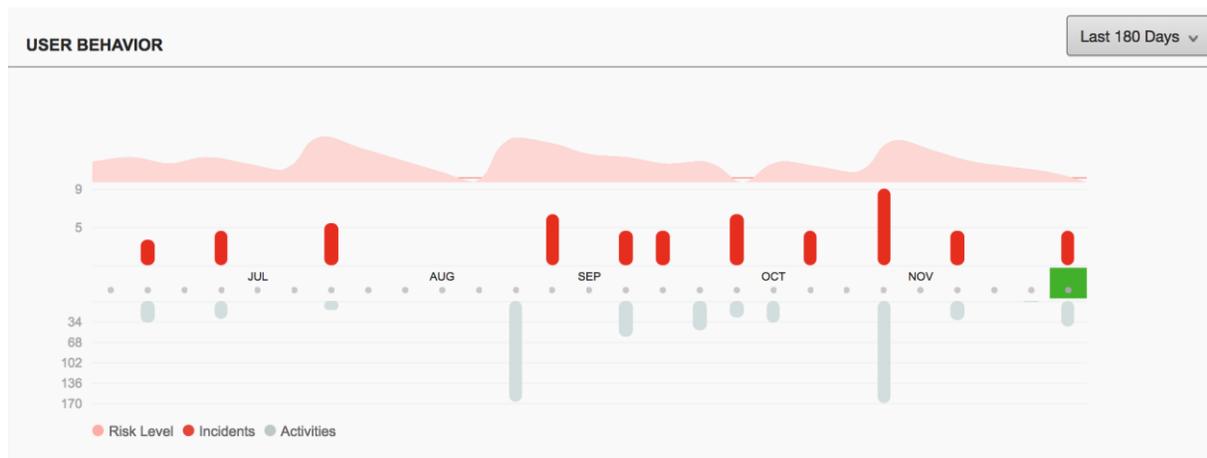
*In-appropriate or accidental* collaboration often presents the highest risk to organizations storing data in the cloud. We recommend a close examination of **Publicly Shared** files containing sensitive and regulated data. (Figure 6)

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.

### INCIDENT TIMELINE

NOV 28

02:48  **Suspicious volume of downloaded data originating from a high-risk source IP** | Malicious or Compromised Insider +91 Workflow Open

Office365

Risk contribution: **91** (?) | Mitigation: **Monitor** | Status: **Active** | Source: **Real-time**

Suspected data theft due to high volume of downloaded data within a specific time frame originating from a high-risk source IP. High-risk source IPs are identified by Imperva ThreatRadar and include Tor networks, anonymous proxies, and malicious IPs that were the source of prior attacks.

02:42  **PII Data** | Data Identifier +0

Office365

### INCIDENT #1280805

## SUSPICIOUS VOLUME OF DOWNLOADED DATA ORIGINATING FROM A HIGH-RISK SOURCE IP (Malicious or Compromised Insider)

Severity: Medium | Mitigation: Monitor | Source: Real-time

Created: 11/28/17 02:54:15 — Last Updated: 11/28/17 02:54:15

**Workflow**

#### What Happened?

Suspected data theft due to high volume of downloaded data in a specified time frame, performed by account **corinne.king@extremeguitars.net** from a high risk IP **216.218.222.14**.

#### Recommendations

Verify the context of this activity with the user. Examine the downloaded

#### Action Log

11/28/17 02:48 - Triggering activity time  
11/28/17 02:54 - Incident was detected

#### USER PROFILE

**corinne.king@extremeguitars.net**  
Vice President

**RISK +242**

See detailed user page

Admin / User	<b>User</b>
User Typical Locations	Romania, Singapore, United States, Ukraine, United Kingdom
User Typical Devices	Windows 7, Windows 7, Windows 7, Windows 7, Windows 7
Asset	Office365
Other Incidents	0 During last 24 hours 8 During last 30 days

## 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.