Reveille

Do You Know Who’s Accessing Your Sensitive Content?

With data security concerns topping the agenda of every boardroom, customers are constantly looking for ways to harden security, including at the application level. Traditional security efforts focus on locking down the perimeter and closely monitoring network traffic, devices, and points of ingress and egress for anomalies that need to be addressed. But insiders pose just a big a risk as hackers, with 50% of all breaches involving trusted insiders according to McKinsey.

Understanding whether documents are being improperly accessed, how users are using them and whether irregular login patterns are occurring is important for high-value digital assets. Recognizing this kind of user activity is essential not only to keep mission critical content apps running smoothly but to help organizations stay secure and prepare for compliance audits.

Understand User Behavior in Context

With Reveille customers gain deep, contextual intelligence about performance, access and user behavior surrounding high-value, business-critical content.

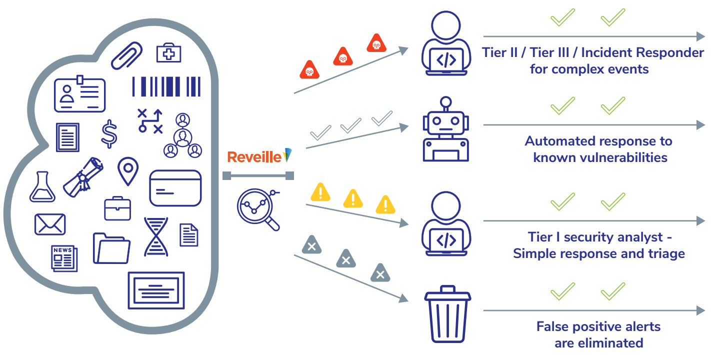
Reveille’s real-time user behavior analytics are included out of the box with deep content services platform (CSP) transaction context to:

- Stop Unwanted User Behavior and Access
- Protect High-Value, Business-Critical Content
- Audit Access for Compliance Reporting

Reveille’s user behavior monitoring helps detect, speed the investigation of and reduce the impact of a data breach by identifying suspicious access to content within your enterprise content management (ECM) / content services platforms (CSP). It can automatically shut down suspicious user access based on conditions set by the business to dramatically reduce the impact of a content breach from malicious insiders or hackers posing as your trusted insiders.

Reveille also provides audit and compliance reporting with details on who, what, and when sensitive documents are accessed as part of the regulated business process (SOX, GDPR Article 30: Records of Processing Activities, and others), providing clear answers to some of the toughest audit questions.

Content Security


Reveille
Tier II / Tier III / Incident Responder for complex events
Automated response to known vulnerabilities
Tier I security analyst - Simple response and triage
False positive alerts are eliminated

> Reveille’s user analytics are icing on the cake. Being able to report actual numbers up to management – who, that, when, how, and tie in the security aspect – is very powerful.
>
> – Steve Malik, ECM Solutions Manager, Turner Industries

See Beyond with Reveille

Detect content access anomalies in your ECM and CSP to identify and stop active breaches

Breach Detection

Cloud-based, agentless visibility into platform operations, user productivity, application adoption and user compliance to monitor for:

- Content access patterns indicative of a security anomaly
- Content use / misuse indicative of insider threats
- Irregular file access by privileged insiders
- Suspicious login attempts from both in-and-outside of the corporate network
- High volume movement of data to removable storage
- Irregular download/upload volumes

Remediation

As security anomalies are discovered Reveille notifies key stakeholders and can automatically terminate user access to content and/or apps based on pre-defined business rules.

Our API-level integrations with EnCase Content Security and Microsoft Defender ATP can be used to validate, speed investigation of and reduce the impact of a data breach by:

- Automatically creating alerts in these tools if users are improperly accessing documents or an irregular login pattern is detected.
- Initiating investigative workflows in these tools when suspicious activity is detected to accelerate response time.
- Restricting user application access or isolating a user machine from the Windows domain.
- Conditionally or automatically removing user access to the ECM or CSP application.
- Generating evidenced-based reports demonstrating compliance for audit requests.

Content security monitoring for:

OpenText™ Content Suite

OpenText™ Documentum

OpenText™ Intelligent Capture

OpenText™ InfoArchive

OpenText™ xPression

Microsoft™ SharePoint

Microsoft™ SharePoint Online

Microsoft™ OneDrive

Box™

IBM™ FileNet

reveillesoftware.com **+1 877.897.2579, #1** **reveille.sales@reveillesoftware.com**

Reveille
SEE. KNOW. PROTECT.

REVEILLE PROVIDES SOLUTIONS FOR THESE ENTERPRISE PLATFORMS

opentext™ box KOFAX IBM Microsoft