Interpreting Behavioral Analytics With Reliable Metrics

Identify potential insider threat behavior, flag possible legal liability issues, and observe behavioral patterns for lost productivity with report metrics.

Introduction

In your organization, do you suspect that an employee is visiting common job search sites or accessing personal cloud storage sites? Maybe it's a disgruntled employee who is dissatisfied with the size of his or her annual pay increase or bonus. Could there be a data breach occurring? Research indicates many significant data breaches are ultimately an "inside job." Insiders could be employees, contractors, business associates, or partners who pose the biggest risk to enterprise data, since they are allowed access to sensitive data. When an employee exhibits a pattern of behavior that includes visiting popular job sites, such as Indeed, LinkedIn, or Monster, the employee may be planning to leave the company. Perhaps the employee is also uploading confidential information to personal storage sites, such as Google Drive, Dropbox, and iCloud.

Enter behavioral analytics. Behavioral analytics focus on patterns of human behavior allowing management to understand what is normal and flagging anomalies that indicate insider threat. With employee Web-use behavioral analytics, the organization can set up a solution that ties Web requests to employees and performs Web categorization of these requests delivered in logging. Using this log data, report metrics in the analytics reporting feature assist IT, HR managers, and other department heads with identifying potential insider threat behavior, assessing trends for data breach exposure, and observing behavioral patterns for lost productivity. Interpreting behavioral analytics with reliable metrics also exposes abnormalities in user activity and flags possible legal liability issues.

There are many metrics available in behavioral analytics reporting, such as hits, visits, time online, bytes, download time, and denied visits, and more than one metric is necessary to provide meaningful insight into employee behavior to managers. The most important metric by far is visits that gauge the level of employee Web activity, but it is often confused with hits, so an explanation of these two metrics is provided below. But to recognize potential insider threats, compare trends, spot patterns of behavior affecting productivity, detect abnormalities, and determine whether legal liability is an issue, more than one metric should be examined as described below.

An explanation of hits versus visits

Based on an employee's visits to Web sites, an organization may need to determine whether the employee is planning to leave and whether the employee could be a potential insider threat. Confusion may lie in the fact that a visit is also a hit, and hits produce larger counts. Both visits and hits are determined in the Wavecrest analytics reporting feature. The following explanation distinguishes between the two and describes how they are meaningful.

Hits

A hit is any request to a Web server. Each time an employee downloads a page, clicks a hyperlink, views a graphic, or performs any other action on a Web site, a call is made to the Web server. The Web server records each of these requests in a log file. These requests are commonly known as hits, and the loading of a single Web page can amount to many hits, due to all of the elements it contains. Images, JavaScript, cascading style sheets, embedded objects, and other Web site elements all contribute to the Hits count.

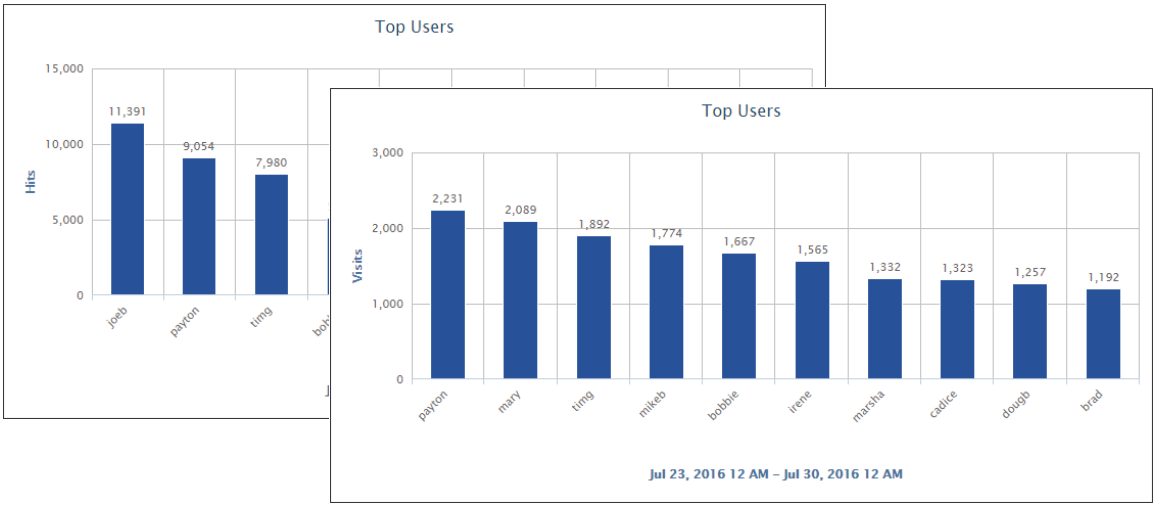
In other words, a hit can be defined as any visit to a Web site, plus any multimedia images and advertisements. Hits represent the number of requests for Web page elements that the Web site fulfilled. For example, a single page with 30 images, 1 JavaScript file, and 1 style sheet would be 33 hits, including the page as a hit in the total count, that is, 1 visit, but 33 hits. A hit can be a meaningful measure of how much traffic a server can handle.

Visits

A visit is a click action for the purpose of visiting a Web site. One click equals one request for a Web page. A visit does not include multimedia URLs, such as graphics or audio pages, banners and advertisements, or Web pages that were requested as part of a visit, that is, unsolicited. For most accuracy, Wavecrest provides a Visit Filter that is set to a reasonable time period so that the same URL visits are not counted more than once in reports in that time period. For example, if the Visit Filter is set to 3 seconds, all requests in this time period are considered hits, and the URL is counted as only 1 visit.

Visits represent the number of times a Web site was accessed. A visit is a meaningful indicator of the level and type of Web activity occurring in your network. In Wavecrest reports, visits can be delivered in several different perspectives, such as visits by category including legal liability and cloud service categories, by classification rating such as acceptable and unacceptable, and most importantly, by user.

In the figure below, the Top Users charts show the top 10 users with the most hits and visits for a specific time frame. Notice that the top user changes depending on whether the metric is Hits or Visits, and the Hits count is much larger than the Visits count for the corresponding top user, for example, payton and timg.



Hits Versus Visits

Wavecrest provides reliable metrics

As mentioned above, behavioral analytics rely on more than one metric to accurately interpret employee behavior. In addition to hits and visits, Wavecrest provides other reliable report metrics, including time online, bytes, download time, and denied visits. Briefly described below, these additional reliable metrics, along with hits and visits, deliver the most accurate results in Web activity reporting.

Time Online

To gain an understanding of time online, a description of “browse session” follows. Opening a browser generates Web traffic. This represents the beginning of a browse session. A session is a group of interactions that take place on a Web site within a given time frame. For example, a single session can contain multiple screen or page views, events, social interactions, and e-commerce transactions. The session is open as long as Web traffic is continually being generated. The session is considered closed once an amount of time passes with no Web traffic. A new browse session begins as soon as Web traffic is generated again.

Time online is an approximation of the time that a user spends on the Internet, based on the time stamps from Internet requests made as the user browses Web sites, the average number of minutes for reading a specific Web site, and the time spent reading the last Web site before the end of the browse session.

Bytes

The Bytes metric is used as a measure of bandwidth consumption and may be displayed in kilobytes, megabytes, gigabytes, etc. This metric allows you can view the bandwidth for your top consumers, that is, users and groups who are consuming the most bandwidth, as well as the bandwidth used by the top content categories, acceptability classifications, and Web sites. You can detect unexpected spikes that could indicate excessive bandwidth or Web use.

When interpreting behavioral analytics, you can also get the number of bytes read per hour, per top user, per top bandwidth site, and per Web request; and much more.

Download Time

Download time is the approximate or average time for a Web page to load in the browser, that is, the period between the time that a user clicks a hyperlink and the time that the page loads in the browser. As used in Wavecrest reports, the Download Time metric is derived by multiplying the smallest average amount of time required to download a typical Web page by the number of visits. For example, if the smallest amount of time to download a Web page is set to 3 seconds, and 100 Web pages were loaded, 100 multiplied by 3 seconds each = 300 seconds of estimated download time. Download time is displayed in a DD:HH:MM:SS format, where DD=days, HH=hours, MM=minutes, and SS=seconds, in reports.

Denied Visits

Another report metric that Wavecrest provides is the Denied Visits metric which indicates denied requests for a Web page. There are many reasons why a user may be denied access to a Web page. These include that the user may not be authorized to receive the page, the page may not have been found by the Web server, or the page may have been blocked for access. Besides being available in the Wavecrest audit reports, an entire report is dedicated to denied visits. It can be used to identify users who may be engaging in excessive attempts to visit inappropriate or unauthorized sites.

Conclusion

Behavioral analytics seek to answer the questions: Which users visited which sites? When did they do so? How often did they do so? What type of content were they seeking? How much bandwidth was consumed in the process? Were the visits in compliance with the organization's Acceptable Use Policy? Let Wavecrest provide you with the necessary and most reliable metrics to analyze employee behavior and answer these questions.

Wavecrest determines metrics, such as visits, hits, time online, and download time, that quickly give managers the detailed data that they need to get insight into how employees are using network resources. Activities, such as application usage in the middle of the night or on weekends, unusually large file transfers, excessive online searches, and more, can all be identified and flagged as abnormal behavior. Put in place a behavioral analytics solution with reliable metrics to protect your valuable assets, to spot insider threats, and to detect events that could lead to a data breach.

About Wavecrest Computing

Since 1996, Wavecrest Computing has provided business and government clients with reliable, accurate employee Web-access security, employee Web-use monitoring and analytics, and Cloud Access Security Broker (CASB) solutions. IT specialists, HR professionals, and business managers trust Wavecrest's Cyfin® and CyBlock® products to manage employee Internet usage with today's distributed workforce in mind–reducing liability risks, improving productivity, managing cloud services, saving bandwidth, and controlling costs.

Wavecrest has over 3,000 clients worldwide, including Blue Cross Blue Shield, MillerCoors, National Grid, Rolex, Siemens, Superior Court of California, U.S. Dept. of Veterans Affairs, and a growing list of global enterprises and government agencies. For more information on our company, products, and partners, visit www.wavecrest.net.

WAVECREST
COMPUTING

Wavecrest Computing
904 East New Haven Avenue
Melbourne, FL 32901
toll-free: 877-442-9346
voice: 321-953-5351
fax: 321-953-5350