The Human Factor: Implementing Employee Web-Use Analytics to Counter Insider Threats

Leverage analytics to manage the human factor, detecting and analyzing insider threats, increasing productivity, and providing more efficient employee investigations.

An organization's greatest vulnerability is its employees. Despite technical advances, such as firewalls, cyber attacks are still successful because the human factor isn't covered. For effective data security, humans have to be regarded as your true endpoints. Though employees constitute the biggest risk factor in the organization, they contribute the most important value for the company. The human factor is a constant, but neglected challenge for organizations when keeping IT systems and data secure. This paper is one in a series of papers that discusses managing the human factor in the workplace with employee Web-use analytics.

Introduction

As the latest buzzword in IT, analytics are increasingly crossing various components of IT systems. With IT requirements to gather analytics based on data, networks, and human behavior, there are endless possibilities for utilizing this information. In this paper, we discuss the need for employee Web-use analytics with a human focus, why these are important in any organization, and the key features of an employee Web-use analytics solution. What do we mean by employee Web-use analytics? By employee Web-use analytics, we mean user Web activity in your organization that is analyzed from many perspectives including security, network, and human behavior, to protect the organization from insider threats, lost productivity, and legal liability.

"Insider threat" can be a misunderstood term. The CERT Division at Carnegie Melon University defines it as "the potential for a current or former employee, contractor, or business partner to accidentally or maliciously misuse their trusted access to harm the organization's employees, customers, assets, reputation, or interests"–the human factor of cybersecurity. Now, you might be thinking that this could never happen in your company; you trust your employees, and "we're all good friends." But insider threats can be unintentional, that is, they can be comprised of employee mistakes, such as an employee clicking a link in an e-mail filled with malware. It is vital that organizations have an analytics solution in place to analyze user Web activity to mitigate the human factor risk.

Analytics have become an essential tool to perform forensic analysis after a security breach occurs. However, if executed properly, analytics can help organizations identify suspicious behavior, both internal and external, and proactively block potential threats before they can manifest, as well as provide early warnings against threats. In an analytics solution, detailed forensic reports deliver a comprehensive analysis of human Web activity including their visits, search terms, and inappropriate sites. From a security standpoint, Web content can be blocked to stop certain kinds of content from appearing on Web pages or from being downloaded. To also keep your network secure, analytics can inspect the secure sites that your employees are accessing so that this traffic can be examined for more accurate filtering.

From a network perspective, companies need real-time visibility into network bandwidth performance. An analytics solution collects, analyzes, and reports on data concerning what your network bandwidth is being used for and by whom. It can identify the top consumers in your network, as well as report on metrics such as the number of visits they made, amount of bandwidth used, and amount of time spent online. It can send real-time alerts to keep you informed on when thresholds are reached. It can provide insight into what cloud applications and services are being accessed. This is of tremendous benefit to IT personnel who are increasingly responsible for more and more applications and services traversing the network through an increasing number of locations and devices.

From a human behavior perspective, monitoring user activity and behavior has significant benefits including increased security against insider threats, increased productivity through insider intelligence, and more efficient and effective employee investigations. When you analyze human behavior, you focus

on patterns of behavior, comparing trends of user activity over time to detect anomalies. Monitoring Web traffic in real time is also a must to increase security and productivity, and to help IT properly prioritize the most concerning threats.

For companies struggling with visibility into their environments, employee Web-use analytics give you extensive visibility into the human factor. Organizations need to actively leverage these analytics and implement analytics tools for examining data and producing effective detection and response strategies. To keep organizations focused on their mission, they need the best possible insight into the security issues affecting their IT environment. To protect their networks, they need readily available employee Web-use analytics that can enable IT to overcome security, network, and human behavior issues.

The human factor of insider threats

A 2014-2015 SANS survey on insider threats indicates that organizations are starting to recognize the importance of protecting against the insider threat but struggle to deal with it. As one might expect, larger organizations are more likely to have provisions for responding to such threats compared to small companies.

Key findings include:

- **Insider threats are on IT's radar.** Almost three-quarters (74%) of respondents are most concerned about negligent or malicious employees who might be insider threats. The FBI and U.S. Department of Homeland Security agree that insider threats have increased and that such threats pose a serious risk.
- **Organizations fail to focus on solutions.** Survey respondents indicated that they recognize the problem but fail to implement solutions that effectively deal with it. This is not good news. This wide gap between threat priorities and resources available for budget and implementation is an ideal playground for attackers.
- **About a third of organizations know they've experienced an insider attack.** This is only the tip of the iceberg. Many insider threats go undetected, and some are only detected by accident.
- **Prevention is more a state of mind than a reality.** Over 68% of respondents consider themselves able to prevent or deter an insider incident or attack. Half (51%) believe their prevention methods are "effective" or "very effective." Yet 34% of respondents indicated that they have still suffered actual insider incidents or attacks, some of which were costly.
- **The financial impact is significant.** Almost one-fifth (19%) of respondents believe that the potential loss from an insider threat is more than $5 million; another 15% valued such loss at $1 to $5 million. Immeasurable costs include brand and reputation damage and related costs.
- **Spending on insider threats will increase.** One-fifth (20%) of respondents indicated they planned to increase their spending on the issue to 7% or more in 2016, demonstrating the growing awareness and focus on this area.

According to Gartner Research, "By 2018, organizations that monitor and analyze a broad spectrum of employee activities will experience 50% fewer insider data breaches than organizations that monitor internal communications only." Another SANS Survey indicates that organizations need to increase the variety and volume of data being collected. They need to collect as large a dataset as possible on their employees, such as cloud activity, security information, and events from user behavior monitoring tools, to gain insights into the human behavior in their infrastructure.

The research in a ZDNet article indicates that “most companies take over six months to detect data breaches.” A cybersecurity report conducted by the Ponemon Institute suggests that “the time it takes for businesses to detect a data breach once it occurs gives threat actors plenty of time to conduct surveillance, steal data, and spy upon victim companies.” So what can organizations do to detect potentially compromised systems sooner? By implementing an employee Web-use analytics solution, organizations can monitor and analyze human behavior, and utilize metrics that are focused on the human factor to help identify anomalies before a data breach occurs or just as the data breach is occurring.

Key features of an employee Web-use analytics solution

Given the heightened awareness of human factor risks and the consequences of not implementing a solution, companies need to act now to protect themselves and their employees with a comprehensive employee Web-use analytics solution. Some of the key features of employee Web-use analytics are listed in the table and further explained below.

Key Features of Employee Web-Use Analytics	
☑	SSL Inspection
☑	Web Traffic Trend Comparisons
☑	Identification of Top Users
☑	Detailed Forensic Reports
☑	Real-Time Web Monitor
☑	Bandwidth Usage Alerts
☑	Inspection of Content/Media Being Downloaded
☑	Cloud Activity Reporting
☑	Hits and Visits Metrics

Inspect secure traffic

No doubt, your employees are visiting secure Web sites, and thus you have SSL-encrypted (HTTPS) employee Web traffic in your network. This traffic should be analyzed for more accurate filtering and reporting to better identify and defeat security threats. SSL inspection is a process that analyzes employees’ encrypted Web requests (HTTPS traffic) to determine the specific type of content that the employee is seeking. Employee Web-use analytics properly categorize the traffic based on the most specific level of content-identification elements in the requested URL. These elements include the path and parameters, not just the domain name. The total SSL inspection process decrypts, analyzes, categorizes, and then re-encrypts the traffic. If categorization does not result in the request being blocked, the request is passed on to the Web.

Compare Web traffic trends

An important factor of employee Web-use analytics is the ability to compare trends in Web activity in order to recognize patterns and detect user anomalies. Using Trend Comparison charts, you should be able to compare the Web traffic of a user, group, content category, or acceptability classification, as well as denied traffic or allowed traffic, in a specific time period to that of a previous time period. Examples of time periods are yesterday, previous 24 hours, last 7 days, last week, and last month.

Provide metrics of top users in real time

If you suspect that excessive or inappropriate Internet surfing is affecting employee productivity, employee Web-use analytics can help you to monitor the Internet overuse or misuse by the employees in your organization. When the personal Internet usage of employees starts consuming the bandwidth meant for business purposes, a quick Top Users chart can identify the top consumers responsible with the number of visits made, amount of bandwidth consumed (bytes), or amount of time spent online (hours).

Perform forensic analysis

Should the organization need to identify and investigate employee Web activity, an employee Web-use analytics solution provides low-level, detailed forensic reports that can be used for audits, investigations of possible misuse of Web-access resources, forensic investigations, personnel appraisals, and other corporate purposes. These reports allow managers to get a comprehensive analysis of a single user's visits including the site's category and full URL, view search terms that users entered on popular search sites such as Google, view users who accessed sites that pose a legal liability risk, and see specific URLs to which a user was denied.

Continuously monitor Web traffic in real time

Unmonitored Web activity can impact productivity, lead to malware infections, as well as increase costs and potential legal liabilities. Therefore, an organization will want to continuously monitor live Web traffic as it is occurring in its network. A real-time Web monitor in an analytics solution can show Web activity in real time with information such as user ID, originating IP address, date and time, content category, and URL. It can display Web requests that were denied due to Web filtering and content type filtering. Its functionality includes allowing you to select and view only specific users, groups, or categories.

Deliver real-time alerts

Important to any organization is optimal network bandwidth usage that ensures mission-critical applications have the bandwidth that they need to keep running smoothly. When the bandwidth for your key business operations is being hogged and thresholds are reached, an employee Web-use analytics solution would automatically activate your bandwidth throttling policies, send e-mail alerts to keep you informed wherever you are, prioritize network traffic, and block nonessential categories or cap their bandwidth. As part of the solution, a real-time bandwidth monitor would display alert information such as the policy name and its associated threshold.

Inspect content/media being downloaded

Beyond blocking categorized Web sites, employee Web-use analytics determine whether the content of a URL is video streaming, audio streaming, images, and more. The analytics solution then blocks the data based on the content type, such as animation, audio, downloads, images, scripting, and video. It also can block based on file extension. With these capabilities, you can stop certain kinds of content from appearing on Web pages or from being downloaded.

Categorize and report on cloud activity

Today, as cloud adoption in the enterprise continues to grow, a number of cloud applications and services are being deployed by employees that help them do their jobs more quickly, easily, and with more flexibility. However, not all employee-introduced cloud services are sanctioned or even known to the IT department resulting in a human factor vulnerability. With employee Web-use analytics, these cloud applications and services would be categorized and their usage assessed through cloud service

reporting. This places the organization in a better position to determine which cloud services to keep, which to completely block, and which are desirable, but not enterprise-ready.

Determine hits and visits metrics

An essential feature of an analytics solution is its ability to determine and distinguish between hits and visits in Web traffic. Hits and visits provide the most pertinent data on human behavior in the organization, and it is important that managers understand these metrics in order to analyze employee behavior. Though more than one metric is necessary to provide meaningful information, the most important metric by far is visits, but it is often confused with hits. With its ability to separate hits from visits, an analytics solution can deliver accurate results in Web activity reporting.

Conclusion

Ultimately, how actual human users interface with the output of employee Web-use analytics will greatly determine if a solution or tool is adopted or deemed to produce useful information in a reasonable amount of time. Visualization of that data will greatly affect adoption of the technology. Analytics tools help manage the human factor and address common problems, such as how to use available Web data in a company's network to identify threats and attacks, and alert IT administrators when abnormal or malicious activity is in progress. Organizations of any size are potential targets.

The capabilities and benefits of employee Web-use analytics are many. Forensic analysis of data, inspection of content being downloaded, and SSL inspection help to block potential threats. The ability to identify the most active users in your network, be notified of bandwidth policies being triggered, and obtain insight into the cloud services being accessed helps to secure the organization's network. Useful information compiled from log file analysis, Trend Comparison charts of user activity, and live Web traffic monitoring increase security against insider threats and increase productivity.

Only by understanding employee behavior and the data employees are creating can organizations begin to address the human factor of data security. This data includes hits and visits which are highly important metrics used to interpret behavioral analytics that focus on patterns of human behavior. The next paper in the series will provide more detail about the use of metrics to analyze human behavior.

About Wavecrest Computing

Wavecrest has over 20 years of proven history of providing reliable, accurate Web-use management and Advanced Log File Analyzer products across various industries. Managed Service Providers, IT Specialists, HR professionals, Forensics Investigators, and business managers trust Wavecrest's Cyfin and CyBlock products to manage the human factor in business Internet usage–managing cloud services, reducing liability risks, improving productivity, saving bandwidth, and controlling costs. Wavecrest is trusted by large government and commercial organizations such as US-CERT Homeland Security, U.S. Department of Justice, USPS Office of Inspector General, National Grid, Johns Hopkins, and a growing list of global enterprises and government agencies. We are a proud long-term GSA contract holder. For more information on the company, products, and partners, visit https://www.wavecrest.net.

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