Wavecrest

THE CASE FOR A POLICY-BASED WEB-USE MANAGEMENT APPROACH

The

HUMAN FACTOR

White Paper Series

www.wavecrest.net

Executive Summary

Prompted by the explosion of employee Web use in enterprises of all types, this paper reviews policy-based Web-use management approaches. It first reviews their need and then describes how they can be implemented in a way that benefits all concerned.

> *By way of definition, a policy-based Web-use management approach integrates specific policy provisions (dos and don'ts) with semiautomated monitoring and auditing processes and follow-on management processes and actions. The terms "use" and "usage" refer to constructive, productive use of the Web as well as undesirable or unacceptable use.*

Internet usage is growing rapidly in enterprises of all kinds, such as business, education, and government. This rapid growth goes far beyond sales and research. It now extends to many core-business or mission-critical functions that depend on a number of cloud applications and services daily. As more and more dollars and manpower are invested in this effort, and as the dependency on network resources increases, these enterprises need to strengthen and improve the way in which they manage the use of this increasingly vital resource. In this regard, the paper urges managers to become considerably more involved in planning and controlling Internet usage. It goes on to point out that the best way to do this is through the use of policy-based Web-use management approaches.

A logical sequence of actions to follow is this: First, companies need to establish policies that encourage positive, safe Web use while simultaneously discouraging negative (personal or unsafe) use. Second, they need to put in place a policy-based solution to help ensure compliance with the policy. Policy-based solutions can automatically monitor, analyze, and document Web use, providing management with usable, reliable metrics that help identify problem areas and determine trends to properly manage the human factor. Third, management must invest the time and effort to use this information to adjust priorities, strategies, and schedules, and guide any necessary workforce-related actions, for example, assignments, training, or disciplinary action.

The paper concludes by pointing out that the integration of these three elements, that is, establishing a comprehensive policy, implementing a policy-based solution for reporting, and using the information in the reports to make strategic and tactical adjustments, constitutes an effective policy-based Web-use management approach.

Background

It is no secret that thousands of enterprises are increasing their use of the Internet at a phenomenal rate. Furthermore, their employees are using it for much more than simple online shopping and e-mail. Increasingly, they are using cloud applications and services for core functions of the enterprise, for example, front office, administrative, financial, marketing, purchasing, advertising, technical, training, and project collaboration activities. While this is all very exciting, many enterprises are discovering that it is a double-edged sword. On the one hand, Web use benefits the enterprise in many ways, that is, it typically results in improved communications, increased flexibility and agility, reduced turnaround times, increased profit potential, and so on. On the other hand, such extensive use results in your employees' increasing level of dependence on Internet resources, such as network bandwidth, and usage. Now Web-dependence is not inherently a bad thing. However, without proper management attention, such dependence can quickly lead to ineffective use of the workforce. To preclude this from happening, enterprises need to closely manage all aspects of Web-use activity.

Current Management Approaches

In some companies, most Web-use management efforts, if any, are aimed solely at preventing or minimizing use of the Web for personal reasons. Some enterprises do this by blocking access to undesirable sites, for example, those featuring pornography. This is often referred to as filtering. Another approach, which some enterprises employ, is the use of a very simple reporting system–one that identifies users and lists the sites they have visited. This type of simplistic reporting leaves it up to the individual manager to decide–after the fact–what is abusive and what is not. Without a reporting engine, also called a Smart Engine, which provides the analytics necessary for accurate, actionable reporting, sifting through this insurmountable data becomes an onerous task for managers.

The above simplistic approaches, while useful to a point, have several drawbacks. First, they focus solely on the negative aspects of Internet usage and do nothing to prompt or encourage positive, constructive use of network resources. Second, they can lead to a false sense of security, that is, they can never capture more than a modest percentage of unacceptable or undesirable sites.

Even if these two approaches were effective, mere minimization of abuse is no longer adequate in today's Web-intensive world. Today, companies need to protect their employees and networks from malware, phishing attacks, and other security breaches.

A Better Way

As with other company resources, management needs to plan and control Internet usage to ensure optimum results, including safety from hackers who target good employees. Unsuspecting employees can inadvertently click official-looking links on Web pages and e-mails that lead to malicious sites. To successfully control employee Web use, managers need to develop and implement policy-based Web-use management approaches. At a very fundamental level, a Web-use management approach includes:

- A strategy for Internet use.
- A policy for governing that use.
- A policy-based mechanism or process for monitoring and reporting on employee Web activity.
- A follow-through process for analyzing Internet usage and taking appropriate action on the basis of that analysis.

As you can see, the first, second, and fourth bullets represent human management functions. These functions involve decision-making responsibilities that cannot be performed by anyone or anything else–computers cannot do it all. On the other hand, the third bullet can be handled automatically by well-designed Web-use management products as seen later. All four bullets are discussed briefly in the following paragraphs.

Strategy for Internet Use

In any organization, network resources are absolutely crucial to the achievement of the enterprise's goals and objectives. In addition, it is no secret that they are extremely expensive. Consequently, to ensure cost-effective mission success, the enterprise should have a carefully crafted, clear strategy for the way these resources, such as network bandwidth, are to be used. In addition to gaining insight into security vulnerabilities and bandwidth consumption, the strategy should include acquiring an entire picture of employee Web use. The strategy should state the enterprise's goals and objectives in a clear, coherent way and should indicate the priorities to be employed, functions to be stressed, and so on.

Policy for Governing Internet Use

A sound, formal Web-use policy is needed to help implement the enterprise's strategy. In the context of network usage, an effective, thoughtful, and properly administered policy is a dual-purpose document. That is, it 1) encourages and guides all members of the workforce toward positive, constructive use of network resources, while 2) simultaneously helping to curb inappropriate or abusive use. To accomplish the first purpose, it should clearly reflect the strategy discussed above as it relates to network usage. In so doing, the policy should clearly state how, when, and why network resources should be used and when they should not. To aid the second purpose, it should clearly state what acceptable use is and what it is not, and it should clearly indicate the consequences of engaging in unacceptable use. The former should be emphasized more than the latter. In sum, a sound Web-use policy is more than just a litany of restrictions and penalties; it is the fundamental promoter and guideline for using network resources in positive ways to benefit the enterprise and all of its members and stakeholders.

Policy-Based Monitoring and Reporting

By definition, Web-use policy management strives to ensure that Internet usage conforms to both the positive and restrictive aspects of the enterprise's policy. Successful accomplishment of this objective requires implementation of some type of highly efficient monitoring, documenting, and reporting product that can provide the most pertinent data on human behavior in the organization. This information is needed to determine the degree to which network resource usage conforms to the enterprise's Web-use policy. To produce this information, enterprises can implement some sophisticated but easy-to-use Web-use management products that are currently in use in a number of industries. It is important that the product be policy-focused on the human, not on the unknown hacker or security threat, that is, human-based policy versus firewall security policy.

Follow-Through Process for Analyzing Internet Use

As indicated earlier, an effective policy-based Web-use management approach includes a follow-through process for analyzing employee Internet usage and taking appropriate action when deviations from policy are noted. Such action may be needed to bring network usage into conformance with policy, or to modify the policy and related plans accordingly. When this is the case, management can use the information provided by the reporting system to adjust priorities, strategies, and schedules, and guide any necessary workforce-related actions, for example, training. The reporting system would provide reliable report metrics focused on human behavior, that is, the human factor. The information can also be used to aid in establishing Web-access blocking regimens if management decides to include filtering in its overall approach.

Web-Use Management Products

Having stated the four elements of policy-based Web-use management briefly, below is a follow-up on the third one, monitoring and reporting, with a more detailed discussion of Web-use management products. Just what are Web-use management products, and why are they needed?

In the context of this paper, Web-use management products are solutions that analyze Web activity and supply different audiences in the company with information specific to their needs. These products may or may not be used in conjunction with filtering. Through various output reports, these applications provide information to managers for identifying relevant trends and making business decisions. More importantly, these products may or may not be policy-based.

"Policy-based" refers to an application that can be tailored to reflect–and monitor compliance with–the enterprise's own policy. While both types are useful, a policy-based product is much more advantageous than one that is not. A well-designed, policy-based Web-use management product utilizes Smart Engine analytics to monitor and report on employee Internet usage in a much more useful and efficient way than one which is not policy-based. The reasons for this are discussed next.

Nonpolicy-Based Products

If the product is not policy-based, it simply reports raw hit data. It does not analyze results or compare them with any standard. Without extensive manual analysis, this data does not answer the most important Web-related questions: Were the visits productive or abusive? What was the human behavior on the visited sites?

Policy-Based Products

Conversely, if the product is policy-based, it does answer the question: Were the visits productive or abusive? With its customized reporting capabilities, a policy-based product can offer Operational, Strategic, and Analytical reporting, and the Smart Engine analytics to answer this question and more. These reporting capabilities are discussed below.

Operational reporting shows activity that is happening now and is based on real-time data. With this reporting capability, IT can monitor current employee Web activity and system performance, and the data is updated frequently. In a policy-based product, Operational reporting components are designed to be viewed multiple times during the day, ensuring adherence to policies.

Strategic reporting provides information at set time frames, and its reporting tools, such as dashboard charts, are updated on a recurring basis at less frequent intervals. In relation to key performance indicators or metrics, Strategic reporting can show a snapshot of top consumer Web activity with drill-down capability providing the details of this Web activity.

Analytical reporting shows patterns of activity over time as well as comparisons of Web traffic. Its reporting tools may consist of trend and comparison charts as well as detailed audit reports, allowing you to analyze large volumes of Web activity data for long-term audits and investigations. With this reporting capability, you can quickly determine if Web-use trends are desirable or undesirable and compare trends to detect any anomalies in Web activity.

Smart Engine analytics provides the data for all reporting tools, ensuring that companies have adequate information to manage and control employee Web use. Smart Engine analytics affords detailed analysis, permitting the investigation of trends, policy violation, Internet misuse, and ultimately, human behavior. The Smart Engine is a necessary reporting component to get the best possible insight into the security issues affecting the IT environment and the human behavior occurring in the workplace.

Conclusion

Because of the burgeoning use of the Internet, it behooves enterprises of all kinds to strengthen and improve the way in which they manage the use of this increasingly vital resource. It is no longer enough to simply block access to pornographic sites, or to leave it up to individual supervisors to detect abuse via oversimplified site visit reports. To maximize the return on their Internet investment, managers need to become considerably more involved in planning and controlling Internet usage, and they need to develop and implement policy-based Web-use management approaches.

To achieve this objective, they first need to establish policies that encourage positive and safe–and discourage negative–use of the Internet. Secondly, they must support these corporate policies with a policy-based solution that automatically monitors, analyzes, documents, and possibly filters Web use, and utilizes Smart Engine analytics. Such solutions can provide management with usable, reliable metric information that helps identify problem areas and determine trends. Finally, management must use this information to adjust priorities, strategies, and schedules, and guide any necessary workforce-related actions, for example, assignments, training, or disciplinary action.

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