

HOW TO KEEP THE WEB SAFE & PRODUCTIVE FOR YOUR BUSINESS

■ ABSTRACT

Internet access has become a necessity for employees within the enterprise environment. Much of this access improves productivity by enabling cost effective access to Web-based applications and business partner extranets. The Web is also a tremendous tool for conducting research and tracking information for business purposes. Even for personal use, the Web can increase productivity by enabling employees to conduct banking and other consumer transactions without losing time leaving the office. Unfortunately, these productivity benefits can be outweighed by time wasting distractions. Furthermore, employee web surfing exposes countless companies to security risks which ultimately cost billions of dollars annually.

Criminal and other unscrupulous organizations now recognize Web vulnerabilities as an easy way to make money and they are doing so by taking advantage of serious flaws in Web browsing applications. A new approach is needed to keep enterprise use of the Web safe and productive, while keeping it cost effective. Complex software and hardware appliances solve some of the security problems but they fail the economic test because they are expensive to own and they divert valuable IT resource from more strategic business related objectives. This paper examines how ScanSafe's managed Web service can secure the productivity of Internet access for your enterprise, while freeing up your IT staff to concentrate on tasks related to your core business.

■ WEB PRODUCTIVITY

The cost to organizations of productivity losses from employee web abuse vary, depending on who you ask. Vendors of Web filtering solutions will tend to quote losses at the higher end of the scale, often stating 75 minutes of every work day is wasted, giving an annual loss per employee of about \$18,000 (at \$55 per hour). Most independent analysts will recognize that lost productivity due to Web use does result in significant quantifiable losses, although probably less than the numbers given above. ScanSafe believes that the losses are closer to analysts' more conservative estimates, and that it really depends on the company and work environment. When making loss estimates, each particular company knows their own culture best, and vendors should let their customers calculate their own numbers – it's an easy calculation to do. In addition productivity losses, ScanSafe believes it is important to identify other risks which companies may have greater difficulties in quantifying. Excess Internet use or abuse can mean costs or risks from:

- Bottlenecking of network resources resulting in lower business productivity and subsequent increases in capital investment for bigger infrastructure (which often can be avoided with Web bandwidth management)
- Behavior that constitutes harassment from a few individuals resulting in lawsuits and, more likely, less tangible damage to valued corporate reputation
- Criminal activities such copyright theft that can result in corporate liabilities and lawsuits
- Ordinary and innocent Internet use resulting in security breaches and costly damages

On its own, the fourth category deserves attention. Criminals and hackers now recognize that Web applications are full of vulnerabilities which make the Web a weak link in enterprise network security. The Web has changed the nature of threats; as well as actively targeting enterprise networks, they also target and infect websites which enterprise users visit. This results in the employee acting as part of the transport mechanism for the malware. The majority of this malware originates on a minority of mostly malicious websites. Clearly, avoidance of these websites is a basic component of good security policy. Given that risk management principles dictate use of risk mitigation where risk avoidance is not possible, the other component of good security policy is deployment of a proactive, Web traffic scanning service. ScanSafe's Web scanning service meets both of these security requirements. However, effective security does not begin with technology; it begins with good policy and a focus on people and process.

HOW TO KEEP THE WEB SAFE & PRODUCTIVE FOR YOUR BUSINESS

■ CREATING A CORPORATE WEB USAGE POLICY

Employee Web monitoring is a contentious issue. Employers have good, legitimate reasons for monitoring Web use. Web use outside of business purposes bogs down enterprise networks and can expose companies to liability issues. Some may believe that workers are entitled to privacy and that monitoring not only can infringe on privacy rights but also negatively impact the working environment and culture. Both viewpoints are valid, and there are some steps which can be taken to meet the concerns of both sides.

First and foremost, a corporate Internet Acceptable Use Policy (AUP) should inform employees about what constitutes inappropriate use of the internet. The AUP should always contain the following key points :

- The most important point is the need to reduce the employee's expectations of privacy by stating that company computer systems are for company related business. The parameters for personal use should be clearly stated.
- The policy should describe the penalties for violating Internet policies. It should be stated that abuse of the Internet will not be tolerated and can lead to termination of employment.
- All employees should be required to report any misconduct. With clear, visible rules, enforcement is everyone's responsibility.
- The policy should inform employees about the type of monitoring that will take place. Depending upon the perception of risk and corporate culture, monitoring can range from non-existent to complete logging and audit. Whatever the method, let employees know and state why Internet monitoring is being conducted.

The vast majority of employees understand that there are risks and liabilities for a company when Internet use is uncontrolled. Employers also recognize that permitting reasonable personal use of the Internet helps the day-to-day lives of its employees, thereby leading to happier working environments. Ultimately, each individual organization will have its own culture and this is what should dictate the tone of an AUP.

■ MITIGATE THE UNAVOIDABLE RISK

With a corporate AUP in place, enforced by a Web filtering service, much of the risk pertaining to both employee abuse and network security can be avoided by simply blocking inappropriate Web sites. However, Web filtering alone will not sufficiently reduce risk. Much Web-based malware originates on perfectly legitimate Websites which have been compromised by hackers and criminals. Web browser vulnerabilities also enable mobile malicious code (MMC) to penetrate the enterprise LAN via a compromised browser. The objectives of MMC can range from simple nuisances like pop-up advertisements, to more sophisticated spyware applications which track Internet surfing, and in doing so consume computing resources. It doesn't take long before multiple spyware applications have caused their PC hosts to slow down and even crash resulting in support calls and expensive fixes and reinstalls. Worse case scenarios involve criminal malware penetrating your network and stealing valuable information via covert SSL channels, which are very difficult to detect.

The long on-going list of Internet Explorer vulnerabilities have promoted some enterprises to install Mozilla Firefox as their standard corporate browser. As an open source browser, proponents claim that Firefox vulnerabilities are less common because the computing community is able to critique the code and pre-emptively remove vulnerabilities. Moreover, Firefox is less integrated into the host operating system therefore, when vulnerabilities are exploited they tend to be less damaging. Others claim that because Firefox isn't ubiquitous, it's a less favorable target for hackers. There is some truth in these comments, but the reality is that Firefox still cannot prevent Web-based security breaches. As Firefox becomes more prevalent, further vulnerabilities will be exploited. Recent vulnerability announcements in Firefox underline this argument. Moreover, many enterprises have decided that switching from Internet Explorer to Firefox is too costly a proposition, so they deploy patching solutions to remedy the vulnerabilities of Internet Explorer. While patching is an important part of the risk management process, alone it is not adequate. New threats can and do hit the Web well before any patches are available. An IT administrator cannot patch a vulnerability if the patch isn't even available. Furthermore, a number of studies and surveys have shown the majority of enterprises do not have their patching up to date.

HOW TO KEEP THE WEB SAFE & PRODUCTIVE FOR YOUR BUSINESS

This imperfect state of affairs is liable to continue for the foreseeable future. There is no silver bullet or quick fix. Instead, there are best practices involving tried and tested defense in depth strategies. The first and most effective strategy is to prevent malware from even reaching the enterprise host or LAN in the first place. Therefore, the first line of defense should include a Web filtering service which prevents users from visiting high risk, inappropriate websites. All necessary Web traffic should then be scanned for malware using multiple, best-of-breed antivirus (AV) tools. To guard against customized or innovative malware (having no available AV signatures) a proactive approach should be taken when examining inbound Web traffic. ScanSafe's managed Web service provides a Web filtering solution with advanced AV scanning using multiple, industry leading AV engines. To protect against cutting edge malware, ScanSafe's Outbreak Intelligence™ utilizes advanced techniques to quickly recognize and block malicious code. Outbreak Intelligence™ provides protection against customized malware and zero hour attacks – threats that appear before AV signature is available.

“The technology exists for carriers and others to provide network security services without customer premises equipment. This approach can increase the effectiveness and efficiency of security operations.”

A March 2005 Gartner Group whitepaper, “In the Cloud’ Security Services Will Change Provider’s Landscape”, John Pescatore

While the market is full of technological solutions, few of them meet the critical requirement of being cost effective. IT executives have limited budgets to spend on security. Spending too much money on one line of defence creates ineffective overall security because security is only as good as its weakest link. IT managers face the challenge of using their budget to cover as many areas of security as possible.

■ SECURITY IS A COST CENTER

Despite many assertions to the contrary, security is primarily a cost center. Some vendors will justify large investments in software and hardware solutions by quoting return-on-investment (ROI). ROI financials will claim that if your business doesn't buy a particular solution, it will suffer untold losses when compromised. This is an old argument and often based on some very subjective analysis. Instead, IT management should be asking, “How can I achieve more effective security for less?”

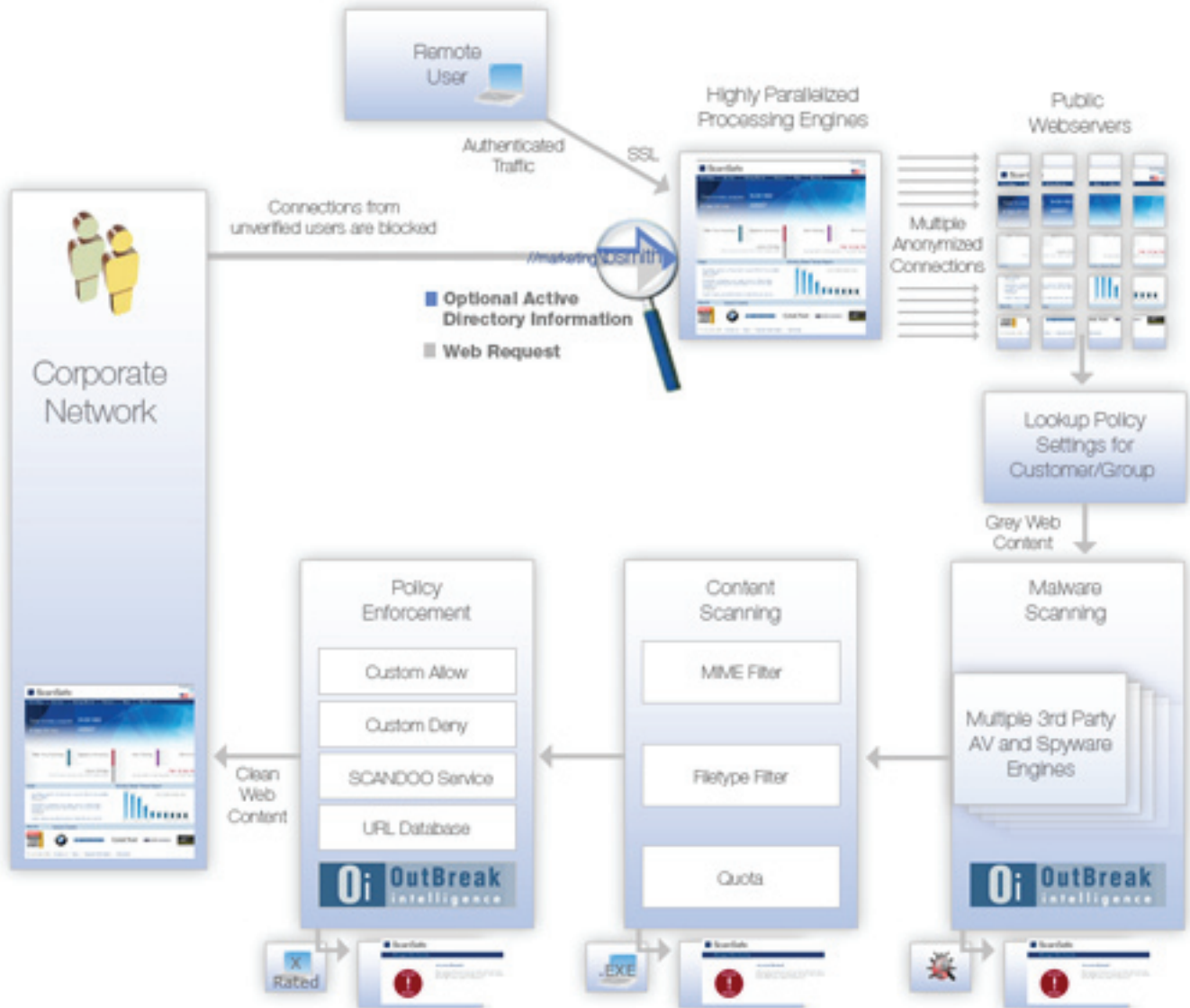
The other question IT managers should be asking is “How can I move my IT staff and resources away from cost centers like security, towards revenue producing centres?” IT staff are typically a limited resource. The opportunity costs of tying up your IT staff in security cost centers are large. These valued resources are required to boost your revenues by leveraging your enterprise's IT. Other industries, such as financial services or computer support have led the business world in outsourcing cost centers and the case for outsourcing functions aren't core to your business is well proven. This includes critical security functions including Web filtering, Spyware and AV scanning. Making this decision requires careful analysis of total cost of ownership (TCO) and an understanding of your opportunity costs.

“[A] Security group can reduce capital expenditure and total cost of ownership by reducing or eliminating CPE devices for detection and prevention.”

A March 2005 Gartner Group whitepaper, “In the Cloud’ Security Services Will Change Provider’s Landscape”, John Pescatore

HOW TO KEEP THE WEB SAFE & PRODUCTIVE FOR YOUR BUSINESS

SCANSAFE METHOD



HOW TO KEEP THE WEB SAFE & PRODUCTIVE FOR YOUR BUSINESS

■ VALUING THE TCO OF A SECURE WEB SOLUTION

Using Gartner Group's framework, TCO is a combination of two major categories of ownership costs: hard (direct or budgeted) costs, and soft (indirect or unbudgeted) costs. The cost of a customer premises based secure Web solution (e.g. Websense or SurfControl plus an additional AV gateway from another vendor like Symantec) can be estimated by applying the relevant line items as follows:

DIRECT COSTS

HARDWARE

- Upfront server(s) and/or appliance(s) costs
- Redundant, failover hardware
- Network connectivity for server(s)/appliance(s)
- Server, and/or memory and storage upgrades as capacity grows with organization
- Obsolescence due to capacity constraints (how fast is your company growing?)
- Obsolescence due to outdated technology (typically occurs within 2-3 years)

SOFTWARE

- Server operating system (OS) licensing
- Application (Websense or SurfControl + Symantec anti-virus gateway) upfront software licensing
- URL database subscription fees (annual)
- Anti-Virus subscription fees (annual)

SUPPORTING SYSTEMS MANAGEMENT (LABOR)

- Hardware installation
- Software/OS/application installation
- OS and application patching and upgrades
- Hardware maintenance, upgrades, and other troubleshooting
- Host security and AV protection and administration for application server
- Storage planning, management and backup for log and audit database
- Disaster planning & recovery

APPLICATION MANAGEMENT (LABOR) - LEARNING OF APPLICATION BY ADMINISTRATOR

- Web policy configuration
- Monitoring, reporting and adjustment

HOW TO KEEP THE WEB SAFE & PRODUCTIVE FOR YOUR BUSINESS

INDIRECT COSTS

DOWNTIME

- System planned downtime
- System unplanned downtime

With ScanSafe's managed service, all but three of these line items disappear:

APPLICATION MANAGEMENT (LABOR)

- Learning of application by administrator
- Web policy configuration
- Monitoring, reporting and adjustment

In addition, a fourth item is added to include the ScanSafe subscription fee (about \$4 per seat per month).

Clearly, a managed service does not have any hardware or software costs, and therefore none of the Supporting System Management costs are applicable either. Arguably, indirect costs are minimized because ScanSafe's managed service has much greater economies of scope and scale than a typical enterprise premises equipment (CPE) based solution, thereby avoiding any planned or unplanned downtime, which results in increased risk from unprotected Web exposure or loss of productivity. ScanSafe has an uptime track record to-date of 99.999% which is rarely seen by a CPE based solution.

[TCO study shows that a 1,000 seat organization will save \\$110,00 pounds with ScanSafe Solution over 3 years.](#)

A TCO case study for a 1,000 seat organization concludes that ScanSafe's managed service will deliver saving \$110,000 over the first three years when compared to a Websense or SurfControl product with an antivirus gateway appliance. More importantly, by outsourcing your secure Web solution to ScanSafe, you can free up valuable IT staff so they can focus on strategic projects that enable you to grow your core business.

■ ABOUT SCANSAFE

ScanSafe is the pioneer and leading provider of managed web security services at the Internet level. Our fully managed services provide a security layer around your enterprise, proactively defending your network and employees against Web threats such as viruses, spyware and undesirable content.

ScanSafe takes over the burden of managing web security allowing you to get back to business - no hardware, software, maintenance or updates are required. As the market leader ScanSafe currently processes more than five billion web requests each month, and counts N.M. Rothschild, BMW, National Express, Conde Nast and The Royal Society of Medicine as customers.

ScanSafe guarantees your protection fro web threats today and tomorrow.

CONTACT

US Office

ScanSafe Inc
1900 S. Norfolk St., Suite 350, San Mateo, CA 94403
Tel: +1 650-577-2355 Fax: +1 650-577-2356

UK Office

ScanSafe Limited
The Connection, 198 High Holborn, London WC1V 7BD
Tel: + 44 (0) 20 7959 0630 Fax: + 44 (0) 20 7959 0631