Centrally Managed Protection of Critical Business Content

Centralized management of a multi-level content security approach

Jon Collins and David Perry, Freeform Dynamics

April 2007

The last few years have seen a revolution in how organizations collaborate and communicate. While email has a long heritage, it has only more recently become acknowledged as a business-critical tool, to the extent that many companies would lose financially if it were unavailable for more than a few hours. Meanwhile, voice-enabled messaging tools such as Skype and Yahoo! have revolutionized interpersonal communications; things are not stopping there, as illustrated by the rapid adoption of social networking technologies such as blogs and wikis. As these capabilities continue to erode traditional, paper-based mechanisms, electronic content in the form of email messages, customer orders, service requests and other documents, is increasingly being integrated up and down the value chain, both internally and externally.

By embracing this brave new world of communications capabilities, and building applications that can take advantage of new ways of transmitting business related content, businesses can enjoy increased productivity and more efficient business processes through improved collaborative working environments, at the same time as strengthening supplier and customer relationships, and enhancing decision making through better access to information.

However, as more information is held and exchanged electronically, so organizations are subject to increased risk, for example from data leakage and malicious software such as computer viruses and spyware (malware). New, integrated approaches to security are required to protect both the content being transferred and the people and organizations concerned; also, organizations need to show how they are maintaining compliance when faced with the deliberate, ill-advised or unintentional behavior of their own staff.

This report focuses on content protection technologies, the role of which is to minimize such risks through the monitoring and management of both inbound and outbound content. A successful defense will depend on the ability of the enterprise to centrally deploy and manage content protection across the business environment, from the end points, at the gateway and indeed, inside the Internet cloud.

Table of Contents

New content delivery mechanisms are not without risks

In today's competitive business environments, organizations are under pressure to manage and protect content across multiple communication streams in both centralized and remote locations.

Unstructured content in all of its forms – from office documents and spreadsheets, to email messages and Web pages, may be passed from person to person in support of business activities. In addition, such information assets are increasingly subject to compliance legislation, both in the area of disclosure of financial information and in protection of sensitive customer data. Drivers that are increasing the reliance on such content include:

Email – a business critical communication tool. Only a few years ago, many organizations would have stated that email was a "nice-to-have" – it supported internal communications and customer interactions, but did not replace them. These days there is ample evidence that the balance has tipped: email is an essential element of both external and internal business communications, and it forms the backbone of collaborative activity. While email has indeed become critical to the business, its wide acceptance comes at a cost – in that it can be difficult to triage business communications from unsolicited messages, i.e. spam. Email can also be a transport mechanism for malware – malicious content such as viruses, spyware and other undesirable programs. Last but certainly not least, email can be the conduit for undesirable communications originating from the organization's own employees. There have been several high profile examples of this in the past year, such as 14 staff being sacked and 101 disciplined at the UK's Driver and Vehicle Licensing Agency (DVLA), for using email to transmit inappropriate (in this case, pornographic) content.

New communication streams. Mechanisms such as Voice over IP (VoIP), Instant Messaging (IM), file sharing and social networking sites such as blogs and wikis create new opportunities to extend the company's reach and support new working practices such as home working. However, they also create new information types and structures which need to be integrated with existing systems and applications. These new streams also represent potential information leaks: for example, instant messaging, left unchecked, can be used for insider trading in the financial markets, or file sharing tools could be used as a distribution mechanism for inappropriate or confidential content.

Integrated supply chains. With so much information to hand, and with the development of web-based content management systems, it becomes much easier for companies to reach out to their suppliers and customers, providing stronger linkages across the value chain, and delivering relevant information to the desktops of those who require it. However, as the underlying transport mechanisms become the same as those used for the wider Internet, they become subject to the same risks. It can be difficult to impose pre-defined restrictions on the web sites each individual is able to visit, as this can limit productivity and business agility. However, the removal of such restrictions opens up the organization to the threat of illicit content being hosted on corporate equipment.

Service Oriented Architecture (SOA) evolution. The development of applications based around SOA allows for the creation of much more dynamic and flexible modular applications, which can exchange information as data elements in messaging forms such as XML. This approach can enable more dynamic applications that take advantage of both external and internal functionality and content – consider the integration of Google Maps into corporate applications, for example. Again, however, such new communication paths offer new opportunities for unacceptable content to arrive inside, or to leave the organization, either through malicious intent or due to accidental leakage, for example because of a programming flaw.

The new types and flows of information bring with them numerous potential benefits, but an equal proportion of risks, particularly as organisations rely increasingly on unstructured content as a business tool. Organizations cannot afford to close the door to such capabilities – that would make them less efficient relative to the competition, and slower to deliver services to their customers and partners. An increased perception of risk can also lead to a reticence to take advantage of more forward-thinking working practices such as remote working. Organizations therefore need mechanisms to counter such risks, not just to resolve individual issues but so the business as a whole can move forward.

Meeting the content security challenge

As discussed above, challenges can be caused by content originating both inside and outside the organization. Content arriving at the organizational boundary needs to be verified, in case it poses a risk: it might in itself be damaging, or it could cause a legal or compliance issue. Similarly, content leaving the organization poses different risks, for example in terms of breaching confidentiality or damaging corporate reputation.

When building a framework to protect both business content and the mechanisms to support its transmission, organizations need to implement technologies that minimize the risks without having a detrimental effect on productivity or business flexibility. In addition, any such framework needs to be more than a short-term, tactical response to current threats. Given that we are discussing mitigation of risks around malicious, illicit, confidential or otherwise unacceptable content being transmitted in either the outbound or inbound direction, there are a number of places that such material can be monitored, checked and potentially blocked:

- **Internet level protection:** Content filtering at the service provider level can significantly reduce the burden of unwanted or inappropriate content before it even reaches the firewall. This level of protection does, however, lie outside the organization, so this approach may not suit all kinds of content (for example, confidential company information).

- **Gateway level protection:** Gateway protection, whether through software or an appliance, may be the simplest method of blocking inappropriate web and email content, as well as an important way of managing communication between corporate sites, and protecting from confidential data leakage.

- **Client level protection:** While protection at the Internet or gateway should reduce the vast majority of unwarranted content from reaching client machines, it is equally important to recognize that such content can arrive from other sources, including MP3 players, USB sticks and CDROMs. Client-level protection remains therefore an important defense.

These alternatives are presented in figure 1 below.

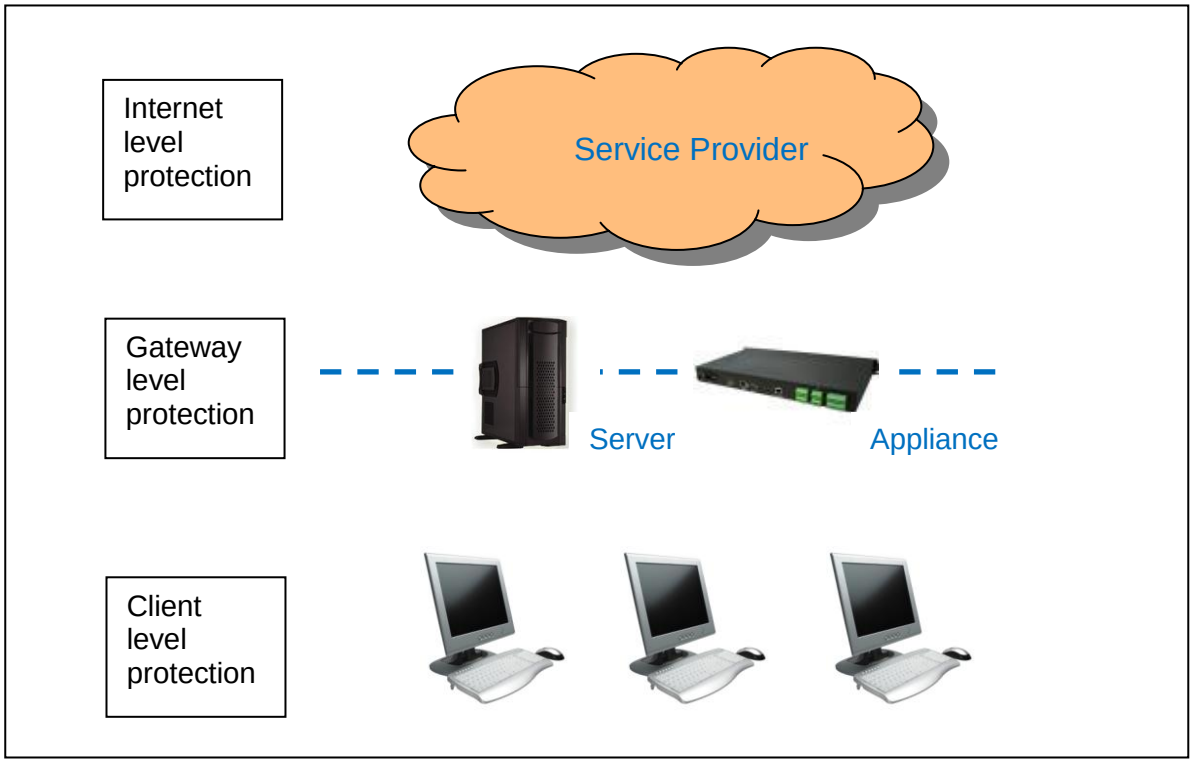

Figure 1: Alternative solutions for content protection

Each approach has its strengths and weaknesses, some of which are presented below. This section is by no means exhaustive, however it gives an indication of the criteria that should be taken into account when defining a suitable approach, relative to the unique needs of each organization.

Internet level protection

This is where content filtering and monitoring for malicious, illicit or undesired content takes place at the level of the Internet Service Provider (ISP), as service providers install and run the monitoring and filtering software on their own hardware platforms.

Benefits of Internet-level filtering include:

- **High-throughput, low-granularity spam filtering.** A lot of malware is propagated in the form of spam which itself is indiscriminate, so it is likely that a majority of unwanted content will take the form of bulk email sends to multiple addresses, including general ones such as "sales@", "support@" etc. Monitoring and filtering the bulk of malware at the service provider offloads what can be a resource-intensive process, offering a much more scalable, efficient targeting method than repeating the same filtering step at the gateway or desktop of every office or branch. By employing the resources of a third party, the company can focus resources and time on more specific, business-oriented content filtering rather than more general filtering for malware. Equally, the fact that traffic is stopped before reaching the customer's network is of particular benefit for organizations whose policies require all communications to be stored once they have crossed the organizational perimeter: requirements for collection and archiving are reduced, and available bandwidth is increased.

- **Cost savings due to third party hosting and management.** Internet level defense is, in fact, a form of service outsourcing. Service providers operate on economies of scale, in that they are managing the same service for multiple organizations, so they should be able to pass on the resulting cost savings to their customers. Also, they will be better able to ensure they have the right levels of technical expertise for the configuration, management and assurance of the underlying hardware platforms, as the levels and types of protection evolve.

- **Last line of defense for sensitive information.** Even if sensitive information has fallen into the wrong hands within the corporate network, content filtering in the cloud represents the organization's final line of defense against inadvertent loss of sensitive financial or other information from within. If there is a solid internal policy for the naming of documents for example, these can be explicitly called out in rules for content filtering. This example does not prevent the loss of encrypted data, or the renaming of sensitive files (though of course the file content could also be scanned), but in the latter case, the company has a defensible position in that there has been a deliberate intent to deceive as opposed to a problem with poor compliance policy.

- **Protection of intellectual property.** Many companies receive suggestions through various routes for product ideas and enhancements that may later be claimed to be ideas for original work that were adopted by the company, and so subject to royalties or damages. It is therefore important for companies to be able to demonstrate "prior art" when asserting their rights under patent or copyright law. To protect against such unsolicited communications, it is therefore important to have a demonstrable policy to block them. The most defensible place to do this is in the cloud, as it can be claimed that such information never actually reached the client network. To be effective, this rejection should be logged and an auto response sent to the sender indicating the reason.

At the same time, Internet level protection is not suited to all types of communication. As mentioned above, confidential information may be required to stay inside the firewall – this is as true for public organizations as private enterprises. Equally, many organizations prefer to keep control of their own IT environments and outsource only a minimum to third parties. Finally, it is unlikely that hosting companies and ISPs would ever be able to provide the depth of customization and configurability that is available if one is in full control of both the hardware and software.

Gateway level protection

Protection at the gateway may be achieved either through the use of gateway security software running on a server, or through the deployment of a security appliance. There are pros and cons for both platforms: the software solution does not mandate an extra piece of network equipment with its own power and space requirements, for example. An appliance, on the other hand, represents a preconfigured, discrete solution that can be swapped in and out, and which is isolated from other applications, reducing the potential for software conflicts and freeing up CPU cycles. Other advantages of an appliance include ease of deployment and reliability, though this can come at the expense of hardware configurability compared to a custom server build; it may also be possible to deploy and configure appliances from a central location, making them better suited to remote locations where it is impractical or costly for qualified technicians to visit.

In either case, benefits of gateway-level protection include:

- **Protecting the borders.** While sensitive documents must naturally circulate within parts of the organization, there should be appropriate restrictions on whether they may leave the firewall. Companies need to be able to establish policies on how information will flow outside the organization, and to enforce this at the boundaries of the network. Gateway content protection solutions enable IT managers to establish policy rules that govern the transfer of documents based on criteria such as travel between offices, communication with mobile devices and application software, and the delivery via web-based mail to unknown client PCs. Although the ideal situation would be for all content leaving the company to be encrypted, this is not achievable in a real world environment, especially where communications occur up and down the value chain with suppliers and customers. Gateway solutions must therefore be highly granular and functionally rich in order to protect all possible forms of communication flow, whether encrypted or not.

- **Customizable server-level handling of spam.** There is little technologically to distinguish between the filtering mechanisms that may be applied at the Internet level, or at the gateway level. However, given that the organization has more control over its own equipment, it can be more selective about how the mechanisms are configured. Both mechanisms offer significant benefit over executing anti-spam solutions as background processes on desktops: such an approach can mean a large cumulative hit in desktop processor cycles and therefore productivity, as well as licensing costs for the software. Since spam is indiscriminate, it is more effective to run content filtering processes as a server process. Indeed, spam at the client can be minimized or avoided altogether, if an anti-spam solution is deployed at the gateway perimeter.

- **Central quarantine.** Everybody is frustrated by the arrival of spam in their mail box. The problem is that as you get closer to the user, the exact nature of what constitutes spam, versus an opt-in activity becomes harder to define. For example, some users may be on several lists to receive what is often termed “selected information from our partners” and which can be important to their work. As well as avoiding hampering the performance of their desktop with content filtering software, a central repository of suspected spam enables the content to be stored away from the desktop or email server, but still gives business users the option to review and unblock quarantined email.

While the gateway solution has several strengths, not least the configurability aspects mentioned above, it is unlikely to benefit from the economies of scale that can be achieved by service providers. Similarly it requires direct monitoring and management, like any other server subsystem in the IT environment. This means that the organization will need access to the technical skills and experience required to keep the gateway solution up and running. Finally, gateway solutions can offer little protection if information is being siphoned off the corporate network directly from user desktops, for example onto USB memory devices.

Client defense

Personal desktop security is a necessary defense against malware targeted against users rather than systems: this is particularly true for viruses and other malware that are not always transmitted via email. There is a trade off between loading up a client machine with protection software, and the effect that it has on overall performance.

Benefits of client-level defense include:

- **Protection against social engineering.** One of the largest security headaches is the behavior of the users themselves. Some of this is due to poor education, but even the savviest employee can be taken in when under work pressure or distracted. For example, the controversy surrounding Sony's "rootkit" (a copy protection mechanism that hid itself in the core of the Windows OS) was discovered by a highly technical user, who nevertheless clicked "accept" on a user agreement, an act that enabled the software to install on his machine. One way or another, a piece of malware is going to make it onto a desktop computer, possibly from an IM conversation, or a personal webmail that will induce the user into an inadvertent slip. Even with up to date patch management and strong content protection elsewhere in the network, it's arguable that employees are more likely to fall prey to such an attempt, because ironically they may be less on their guard. Desktop protection against the arrival of malware is therefore of paramount importance.

- **Data leakage prevention.** Any organization should have strict policies to control the loss of sensitive information, some of which can be enforced on the desktop client. Data loss can occur when information is passed during a communication process, for example in an email as an attachment or during an IM session as a file transfer; it can also occur through the deliberate or inadvertent use of removable storage, for example a USB stick, or an external disk drive, or even as files on an unsecured laptop taken off company premises. The use of unsecured client PCs in uncontrolled areas (for example using hotel or airport wireless hotspots) are also at risk, for example, illegal "spoof" hotspots can upload malware onto a poorly configured PC. Policies for data leakage protection should therefore be comprehensively enforced, and vary according to the privileges of the user and the data in question, the user's location and the status of AV and patch software on the machine.

While it is important to protect clients for these and other reasons, many organizations recognise that keeping software versions up to date across the range of desktops can be a real headache; equally, it can be difficult to monitor the protection status at each client. As a rule of thumb then, organizations should be looking to putting the minimum necessary software on each desktop, and monitoring it accordingly. Equally however, it is very difficult to completely protect against inappropriate use of confidential data by a disgruntled or ill-informed employee. As discussed later in this report, technological solutions should be used in parallel with approaches such as staff training and vetting, risk awareness raising, and policy definition and enforcement.

Summary of benefits

The following table summarizes the benefits and downsides of each solution type.

	Benefits	**Downsides**
Internet level	High-throughput, low-granularity spam filtering Cost savings due to third party hosting and management Last line of defense for sensitive information Protection of intellectual property	Confidential information may be required to stay inside the firewall Outsourced solutions cannot be controlled as tightly as in-house solutions Lacks depth of customization and configurability compared with internally controlled solution
Gateway level	Protecting the borders Server-level handling of spam Central quarantine	Likely to be more expensive than hosted solutions Requires on-site monitoring and management
Client level	Protection against social engineering Data leakage prevention	Software maintenance, patch management issues and remote monitoring across multiple desktops

Specific choices will depend on organizational requirements and maturity

As discussed, each type of solution brings with it certain benefits, but no single option is suitable for all possible scenarios, so it is important to select the right configuration depending on the requirements of the organization. As well as the different approaches that each takes to content protection, criteria to keep in mind include:

- **Company size.** Smaller organizations are less likely to have the time or the wherewithal to proactively manage a content filtering solution, so a hosted, Internet-level solution becomes the more viable alternative.
- **IT governance.** The extent to which the more advanced facilities of content protection are employed depends to a large part on whether there are the right responsibilities inside the organization. For example, who is in charge of ensuring that the Acceptable Use Policy is applied?
- **Procurement strategies and funding options.** An appliance or server solution may be the best option for organizations that can free up funding for a capital outlay, whereas a hosted solution may be preferable for organizations that have access to smaller amounts of ongoing funding.

While each of the above mechanisms – Internet, gateway or client-level – has its own benefits, there are additional gains to be made by using them in combination. To do so enables a "defense in depth" approach to maximize risk reduction: for example, if an organization is suffering from heavy loads of spam, and wishes to implement local controls for web content protection, it may choose to use an Internet level protection for the former, and deploy an appliance for the latter. There is no single right answer.

However, the benefits can only be fully realized with the implementation of an integrated approach to content protection. Products are available that perform many of these functions, but the prevailing management approach is to overlay them onto an existing network and to manage them separately. This not only creates additional management overheads, it runs the risk of leaving gaps in content protection which can be exploited, for example if each mechanism (or the administrator in charge of it) assumes that the other is dealing with a particular requirement.

To achieve cost-effective, scalable and manageable data protection and compliance, companies should seek to move towards an integrated approach to security that maximizes the benefits of individual mechanisms, while ensuring they work together and minimize potential gaps between them. The following steps can help achieve this:

- Acknowledge the existing context and risk landscape
- Configure efficient content filtering
- Implement appropriate acceptable use policies
- Integrate with the wider risk management strategy
- Maintain a single point of management

These are described below.

Acknowledge the existing context and risk landscape

Each organization will have differing requirements when it comes to content protection, depending on their sector, market position, legal framework, business model and other factors. Equally, it is likely that the organization will have made security investments in the past, for example there are few companies today that have not invested in some form of desktop anti-virus solution. It is therefore important to understand the requirements of the organization and the risks it faces from a

business perspective, and compare these to existing content protection investments to determine the necessary steps to be taken.

While funding may be difficult to secure if mechanisms are expressed in purely technological terms, a business case presented from the perspective of business risk can garner more attention, particularly if there are compliance factors involved. Equally realistically, many companies will not be in a position to throw out their existing solutions and move wholesale to something new: instead, an approach that acknowledges the existing situation enables the organization to map out appropriate, yet realistic steps towards the strategic goal of improved content protection.

Implement Acceptable Use Policies

Every organization will have a different view on exactly what it considers to be acceptable use, based on both its own policies and the requirement to comply with industry-level and governmental requirements. While the extremes of unacceptable use may be generally agreed (for example, viewing of porn or releasing of confidential information), beneath this threshold organizations may wish to be more or less stringent; for example one organization may restrict web access to a very limited number of sites, whereas another may leave it down to the discretion of individual managers.

Once an Acceptable Use Policy is defined, it needs to be in some way implemented and monitored. If the policy is unenforceable, for example because it cannot be monitored, then it will quickly become worthless. Equally, it will be necessary to modify the policy over time. Both of these criteria lead to the requirement for a single point of management, for technologies that are used to monitor and enforce the policy.

Configure efficient content filtering

Organizations considering a content filtering solution should first establish the policy for filtering that they wish to implement bearing in mind all variables, from the acceptable use policy to the demands of compliance legislation. Using this pre-established framework they will then be able to make an informed choice of supplier and an appropriate approach to deployment based on the options available to them. Whatever solution is selected, IT staff should be able to push out a comprehensive set of content filtering rules to the appropriate network elements, both client, gateway and service provider from one management console.

Integrate with the wider risk management strategy

Content protection is an important element of IT security, but it is only one facet. Rather than treating it in isolation, organizations should consider content protection as part of their broader strategy, of understanding the risks faced by the organization as a whole, and implementing appropriate mechanisms to counter them. This is of particular importance when considering areas such as policy definition, employee risk management, staff training and external compliance.

Maintain a single point of management

In a large, multi-site IT environment, the management of security is a constant headache, due largely to the number of packages and devices that are in place. For example, informal surveys suggest that a typical branch office can have up to six gateway appliances managing a variety of functions such as threat management, routing and traffic management. The single biggest contribution to management of an enterprise security solution therefore, will be made by a single management platform.

Although the solution itself may be comprised of components at the gateway and through the service provider, if the company has established strong policies for its data flows and identity management, these can be applied centrally and pushed out to all the various elements of the content protection framework. For example, a new content filtering rule may be required based on a new class of commercially sensitive document. This can be pushed out to the multiple gateway and Internet level devices simultaneously, providing immediate, proactive content filtering protection, as shown in Figure 2 below.

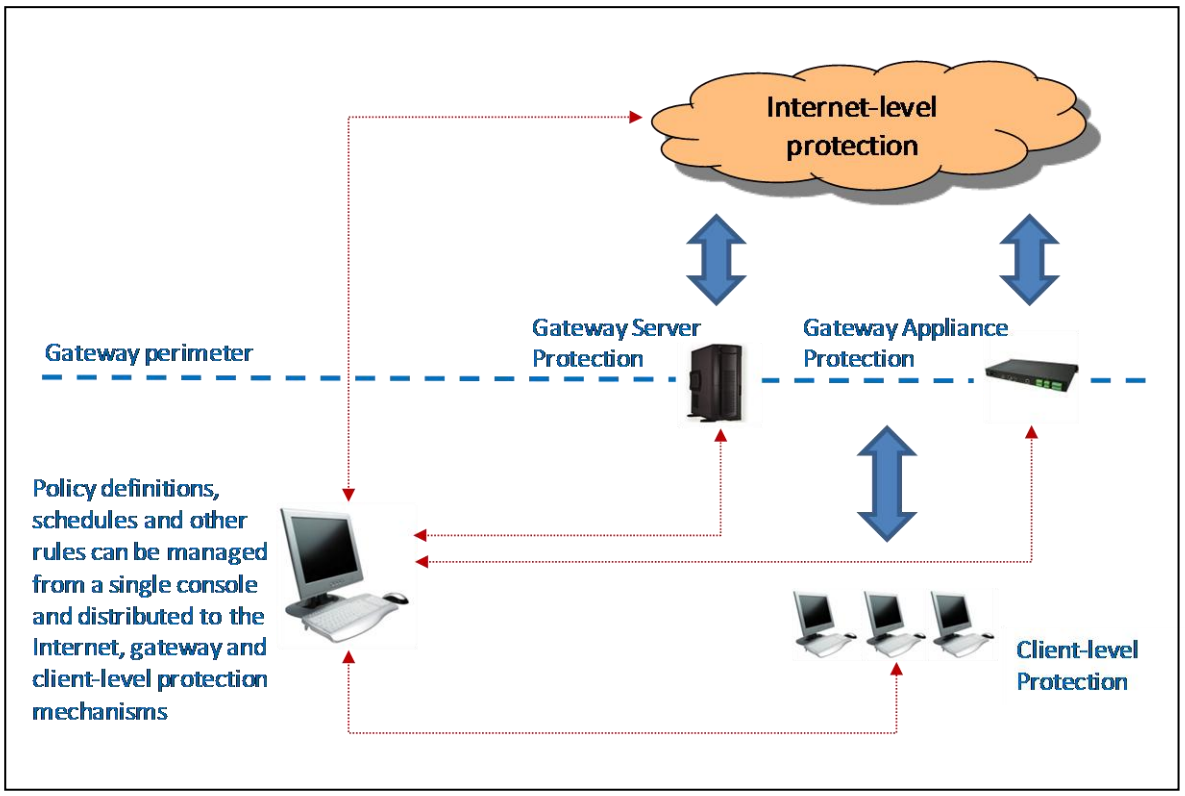

Figure 2: A central point of management control improves manageability and reduces risk

Conclusion

Content-related threats are not going away. Despite improved legislation in many countries, spammers continue to clog the Internet with nefarious requests, and each generation of programming students brings a new wave of individuals looking for their 15 minutes of fame. Meanwhile, inside organizations, individual lack of forethought can often make up for a lack of external malice, as employees access inappropriate content from their desktops, send confidential documents to third parties, and leave the door wide open to malware. Risks such as commercial espionage and unauthorized access can be mitigated to an extent through good training and other procedural mechanisms, but there remains the need for a centrally managed, configurable framework to enable the monitoring and protection of transmitted content.

Exactly what form such a framework should take will depend on the specific requirements of the organization: its size, maturity, specific acceptable use policy and so on. Alternative approaches, such as Internet-level or gateway-level solutions each have their own benefits, but it would be a mistake to consider them in isolation. Appropriate combinations of solutions will ensure that all requirements are covered and risks are mitigated. This does mean, however, that some kind of centralized management approach will be necessary; otherwise the resulting framework could quickly become unmaintainable.

In this domain more than many others, there can be no absolutes – risks need to be managed rather than avoided. By following an integrated approach, risks can be treated holistically which will stand organizations in good stead in both the short and longer term.

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in ITC strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.

About Marshal

Marshal is a privately-owned company with its worldwide and EMEA headquarters at Basingstoke in the United Kingdom and regional offices in Munich (Germany), Paris (France), Johannesburg (South Africa), Houston (USA), Atlanta (USA), Sydney (Australia) and Auckland (New Zealand). Marshal is a global vendor of Comprehensive Secure Email and Internet Management solutions that integrate content filtering, compliance, secure messaging and archiving, to protect businesses against email and Internet-based threats.

Forty per cent of the Global Fortune 500 companies use Marshal security solutions to secure their corporate messaging networks and web against internal abuse and external threats such as viruses, spam and malicious code. More than seven million users in 18,000 companies worldwide use Marshal's highly acclaimed MailMarshal and WebMarshal solutions to protect their networks, employees, business assets and corporate reputation and to comply with corporate governance legislation requirements.

For more information about Marshal visit www.marshal.com.

Terms of Use