



# SECURING YOUR BUSINESS From Internet Threats

---

This paper is intended for small and medium business (SMBs) managers and owners who are concerned about the dangers posed by Internet applications and websites. The intent is to give readers an idea of what hazards exist in cyberspace, and what the best protections, precautions, and cost-effective options are for SMBs.

---

## Risks in Cyberspace

Are you aware of what occurs when your computer accesses the Internet? Despite all the amazing services, applications, and knowledge found on the Web, what can happen is ominous. Unless properly protected, shortly after a computer connects to the Internet, automated scanning programs swiftly identify it and then begin to probe it for ports that are receptive to risky web applications or malware.

Malware is a computer application intentionally programmed to inflict damage by stealing data, denying services, taking control or performing other activities that can disrupt your business through lost working hours, dollars and even reputation. The list of these risky web applications includes spyware, botnets, Trojan horses and worms.

According to the SANS Internet Storm Center (ISC) in Colorado, the average time before a public-facing computer connected to the Internet becomes a target for a malware probe is less than twenty minutes. Considering how long most people's computers are tethered to the Internet, attended or unattended, that is a very short length of time.

The Ponemon Institute published a study in 2010 that found the average total cost of a 2009 breach in the US was over \$6M, with about two-thirds of that amount coming directly from lost business. Commerce today depends on the Internet and almost all businesses in the world have Internet access—but how many of them are secure from potential threats?

## Security in Cyberspace

So, what can you do to protect your business in a world where security threats constantly change, and time and resources are limited? The good news is there are solutions that can block most threats before they reach your systems, limit employee access to inappropriate websites, and restrict unauthorized transfer of confidential company information by deploying a defensive strategy with a strong perimeter security solution.

## The In-house Solution

A common solution is the in-house security model, where a business buys, hosts and manages all of the equipment and software they need to be safe from Internet harm. This method employs a substantial array of computer hardware and software programs that manage a centrally-monitored firewall, web filters, email filters, antivirus and antispymware programs with regularly distributed updates and intrusion prevention/detection that scrutinizes web traffic. Traditionally, self-managed security lives on a company's premises and is networked to client devices — desktop personal computers, laptops, tablets, mobile phones and whatever company property is attached to the Internet — that have an associated endpoint software security program installed on each of them. All company security is monitored, maintained and updated by a business's IT services group.

There are trade-offs, to be sure. There is something attractive about having a security solution in-house and completely under control — but, what about the financial burden? The evident downside of self-managed security is its expensive price tag. The in-house security solution requires a physical facility containing a multitude of expensive hardware devices and software packages, with internal experts to install, monitor, maintain and upgrade them. All of this activity can be a full-time role for one or more specially trained and certified employees.

Making a large capital expenditure and finding a way to physically and financially support it 24/7 is a serious concern. There can be no corner-cutting with it, as any amount of economizing may likely cause your security to suffer. If it does, and there is a security breach, your investment may have been in vain. For most SMBs, the capital expenditures and headaches involved with added human resources, floor space, and energy costs can place this model of Internet security out of reach. You must have Internet security, but with all the costs involved, you must also examine alternatives to an in-house model.

## The Outsourced Solution

Another solution is an outsourced security model, where Internet traffic is overseen by a security service provider with a wealth of expertise in managing a client's Internet security. The provider can manage the needed equipment and applications on your premises, which can deliver cost savings. Or, for greater cost savings, the provider can be a Cloud-based service, where all management activities are virtualized, hosted and managed

on the provider's premises. Outsourced security service providers take care of everything for their clients, 24/7 and every day of the year. This includes constant monitoring, upgrades, continuous updates for the latest dangers, firewall management, email filtering, intrusion prevention and detection and web filtering. Because these crucial activities can be performed for a fraction of the cost of purchasing and establishing your own security installation, key IT personnel will have time to manage other vital activities, floor space is saved and dollars for less resource-intensive purposes are available.

## Integra Telecom Solution: Cloud Firewall Service

An outsourced security solution, Integra Telecom's Cloud Firewall Service (CFS), delivers the protection your business requires without demanding a capital expenditure or a staff of Internet security experts. CFS provides a single point of control that monitors and protects your business from the harm of dangerous Internet incidents. It is available in several configurations that, depending upon your needs, can contain:

- An application-aware firewall
- Website filtering
- Antivirus and anti-spyware
- Intrusion detection and prevention
- File filtering
- Customizable reports
- A VPN client for remote users

These features are discussed in-depth below.

### Application-aware Firewall

An application-aware firewall (or next generation firewall) is considerably more sophisticated than basic firewall protection, which is prevalent in many in-house solutions. The CFS firewall provides both application visibility and application control. Application visibility gives you the ability to see applications being accessed by employees browsing the web. You can then determine if you need to restrict usage of specific applications to protect your network and boost employee productivity. Application control allows you to block high-risk web apps as well as high-risk behavior. The result is a highly-secure network with bandwidth preserved for business activities.

As an illustration, consider the risks that peer-to-peer file sharing websites expose your business to, such as broken



▲ Unlike legacy firewalls, Integra's Cloud Firewall Service offers filtering at the application level.

copyright laws, letting in spyware, or admitting a virus into your network. With the potential these sites have for transferring malware into, and confidential files out of, your network, you certainly do not want them to be accessible. Through an application-aware firewall, you can prevent access to these and all varieties of high-risk web-based applications that may be undermining employee efficiency.

## Website Filtering

The CFS website filter blocks access to or warns users regarding inappropriate websites. This component's filtering behavior safeguards your business from a spectrum of legal, regulatory, and productivity risks. As should be expected, this filter is constantly updated and maintained by Integra.

As an example of website filtering, imagine an employee who spends some nights and weekends competing at multi-player game websites. Should he attempt to extend his home playing time to his at work hours, CFS will block access to his favorite game sites. Working in conjunction with application-control and other components, like a blacklist of web addresses and a filtering database, the CFS website filter prevents him from visiting sites that jeopardize company security—and his job.

## Antivirus and Anti-Spyware

This feature blocks literally millions of malware variants from entering your network. Its vigilance includes stopping viruses and contaminants hidden within web traffic. Antivirus and anti-spyware defends your network from both unauthorized and malicious access that can result in lost time and money, and even loss of data.

For instance, a virus located in a seemingly safe website's HTML graphics enters the computer of anyone who connects to the site. However, when it reaches a business employing CFS, it is met at the gateway, recognized as malware, and rejected.

## Intrusion Detection and Prevention

CFS intrusion detection and prevention identifies and blocks network and application-layer vulnerability exploits, buffer overflows, denial-of-service attacks, and port scans. Similar to antivirus and anti-spyware, intrusion detection and prevention guards your system from dangerous unauthorized access. This can spare your business from costly network interruptions and lost data.

As a case in point, think about a business being hit with a denial-of-service attack in an attempt to make its website unavailable to users on the day the business launches a new product. Intrusion detection and prevention recognizes the strike and begins blocking the DoS attack, keeping the company network and website up and functioning as normal.

## File Filtering

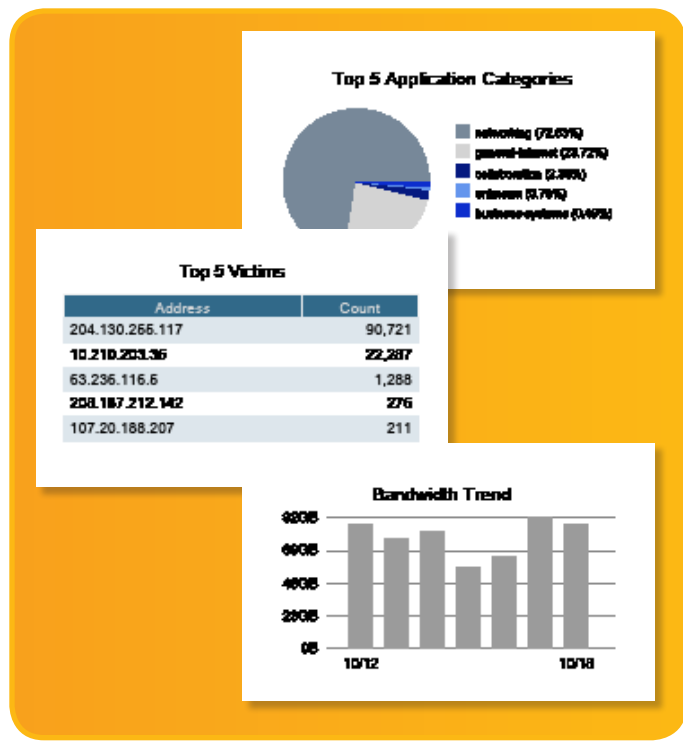
CFS file filtering oversees the file transferring functionality of individual applications. It allows a program to perform its duties, but it ensures that hazardous files transferred in or out via email attachments or downloads and uploads are discovered and denied.

For example, consider an employee who attempts to use their personal Hotmail email account to transfer spreadsheet files out of your network. The firewall may allow the use of Hotmail, but prevent it from uploading XLS files that could contain proprietary company information.

## Reports

CFS summary reports display top activity and threats. These reports include a change monitor, threat monitor, network monitor, top application report, and top high-risk application reports. The information is readily understandable and provides significant information to stakeholders, allowing quick status assessment of network security.

Custom reports and dashboards can also be created. CFS similarly allows clients to add, change, or delete policies for



▲ CFS Reports

all of the Cloud Firewall Service, so that you can implement Internet perimeter security policies that address your unique requirements.

As an example, you may want to see a comprehensive summary report but your CIO and CEO want to view a less-detailed report. CFS allows you to produce reports that work for all interested parties, with as many details as desired.

## VPN Client

It is the policy of most businesses to require remote users to utilize a VPN client in order to protect their laptops from malware. CFS provides a remote access VPN client for remote users with secure access to your local area network resources.

For instance, an employee working at home uses the VPN Client to access the company network. When he attempts to use what is identified as a risky application, that action is blocked. Had he not used the VPN Client, that action may not have been blocked and any malware in the restricted application could have infected the entire network.

# CONCLUSION

The state of the art elements that make up Integra's Cloud Firewall Service deliver a highly-secure perimeter around your business's Internet access. What has been touched upon here is a system designed to keep your business dramatically safer from the Internet's evolving threats. Because malware is constantly becoming more complex and evasive, businesses absolutely need to consider a security deployment that is robust and stays on top and ahead of ever-changing malicious attacks. CFS is a comprehensive outsourced Internet security service that can be utilized for a fraction of the cost of in-

house security solutions. You can rely on Integra to thoroughly oversee and update these services and relentlessly defend your network from all Internet threats.

Please contact Integra, or your agent, to learn more about our Cloud Firewall Service. For additional information, please visit [integratelecom.com](http://integratelecom.com) for more information.



## About Integra Telecom

Integra Telecom Inc. connects business by providing business-grade networking, communications and cloud solutions to thousands of business and carrier customers in 11 Western states, including Arizona, California, Colorado, Idaho, Minnesota, Montana, Nevada, North Dakota, Oregon, Utah and Washington. The company owns and operates a nationally acclaimed best-in-class fiber-optic network consisting of a 5,000-mile high-speed long-haul fiber network and a 3,000-mile metropolitan access network including more than 1,700 fiber-fed buildings.

## Contact Us

Integra Telecom  
 1201 NE Lloyd Blvd., Suite 500  
 Portland, OR 97232  
 1-866-INTEGRA  
[www.integratelecom.com](http://www.integratelecom.com)