www.gficloud.com

GFI Cloud™ white paper

Antivirus management in the cloud: Award-winning malware defense for small businesses

Contents

Introduction

IT administrators for small- and medium-sized business (SMBs) are busy people who are expected to accomplish a lot on thin budgets. Managing antivirus solutions is just one of their many tasks, and while users may have a "set it and forget it" perception of antivirus, the reality is quite different. IT administrators face the challenge of protecting users and networks 24/7, without hindering employee productivity or negatively impacting business operations in any way. That's a tall order when one considers the limited IT budgets that most SMBs have.

Large enterprises, on the other hand, generally have the resources to dedicate one or more servers to host a centrally-managed antivirus solution, as well as a team of skilled personnel to operate it. That's a different story for cash-strapped SMBs that do not have the IT infrastructure or skill sets to do so and often rely on user-dependent, non-managed endpoint products to scan PCs, laptops and workstations for malware. Meanwhile, SMBs that already use a centrally-managed antivirus solution would benefit if they could reduce IT costs associated with managing their antivirus on premise.

Antivirus management frustrations

Managing antivirus technology is a complex task that requires proper planning and effective execution. Administrators have to set and manage scan and update schedules, taking into account network loads and employee productivity to determine the best time of day for each task. New viruses, Trojans, worms, spyware and other malware are unleashed constantly, while existing ones morph and evolve to evade detection. Even if IT administrators religiously keep up with virus definition updates, there is always a chance an unknown virus can slip through due to unsafe user practices. This threat is compounded for small businesses that do not have a centrally-managed antivirus solution with the controls, settings and policies in place to protect users from themselves. Users in the office, traveling or telecommuting can unwittingly launch infected email attachments or contract viruses through their laptops. Though well-intentioned, inexperienced users can create security breaches with bad decisions such as disabling their antivirus or being fooled by a clever phishing email.

The smallest, most cash-strapped businesses often eschew automated network-wide antivirus deployments in favor of individually installed endpoint products, often pre-installed on each PC they purchase. These products do not protect servers or provide other essential security capabilities. They also are not the most cost-effective solutions available for businesses with multiple users, forcing business owners and IT administrators to manage multiple one-off licenses from different vendors expiring at different times of the year. Additionally, in these environments, users are effectively given responsibility to perform antivirus scans and updates, which are time-consuming and become one more thing they must remember to do. Complicating matters even more, users sometimes change settings, which can lead to machine infections that prevent an employee from working. This creates a hardship for SMBs, which typically don't have extra PCs for emergencies.

Moreover, some users fail to comply with company policies, while others turn off their computers when they are scheduled for updates and scans. Sometimes scans and updates fail, or the antivirus server may have trouble communicating with a specific machine for whatever reason, leaving it vulnerable to malware infection. And considering the non-discriminatory tactics employed by cybercriminals and malware developers, reliable, efficient and proven antivirus is just as critical for small businesses as it is for Fortune 500 companies. All this underscores that centrally-managed antivirus is the most effective solution. However, with the average server costing thousands of dollars and skilled IT security professionals demanding high salaries, it's clear why SMBs traditionally have had fewer options for keeping their systems virus-free.

The solution is the cloud.

Why the cloud?

Cloud-based antivirus solutions are scalable and affordable, requiring minimal in-house antivirus expertise, and as such, they are tailor-made for budget-conscious businesses. Other benefits include:

- Centralized management accessible from any browser
- Easy, quick client deployment
- Automated tasks
- Predictable per-user cost structure
- No hardware or software to buy, manage or update

Budgeting and management

Cloud computing democratizes access to centrally-managed antivirus solutions. The affordability, elasticity and flexibility of cloud solutions make it possible for even the smallest businesses to enjoy robust antivirus options, complete with server protection and network firewalls. What traditionally would have required one or more servers to deploy and manage antivirus now becomes accessible through the cloud. Through a web browser, setup is simple and quick. Upfront capital expenses, along with the associated tax implications and depreciation, are eliminated because there is no outright purchase. Companies instead pay for a subscription, renewable on an annual basis, as an operating expense. And, of course, the need for highly skilled staff to run the technology disappears, enabling them to focus time and resources on more strategic, business-building initiatives.

Regulatory compliance

Multiple federal and state regulations have placed strict requirements on businesses large and small – especially in the legal, financial and healthcare fields – to protect sensitive data from leaks and breaches. Laws such as HIPAA (Health Insurance Portability and Accountability Act), GLBA (Gramm-Leach Bliley Act) and the Sarbanes-Oxley Act mandate strict protection for data in use, in transit or in storage.

Compliance is best achieved through effective, robust security systems that automate tasks, centralize management and generate auditable reports. Automated cloud-based antivirus solutions help small businesses achieve compliance through standardized, documented processes. In addition, a centrally-managed antivirus solution will generate reports in various formats, listing threats that are identified and contained, as well as issue alerts where there are cases of noncompliance with security policies.

Cloud-based antivirus matures

Despite the cloud's many benefits, antivirus vendors have struggled to find the right balance for how to leverage the cloud for the delivery of their services. Consequently, users have experienced several drawbacks with some cloud-based solutions. The first among them is limited functionality resulting from slow, disrupted or unavailable network connections.

The primary issue with cloud-based antivirus so far centers on network performance. Solutions that run scans and host virus definitions in the cloud can bog down networks and ultimately degrade the ability to accurately detect threats. To the chagrin of users, there have been cases of spikes in false positives, which create extra work. In other cases, solutions have missed some threats when running scans and failed to entirely remove the threats they detected. The cause for these issues is vendors trying to compensate for network performance degradation by removing some capability from their solutions, impacting their precision and performance in the hopes of creating the false impression that their solutions are faster. So far, these solutions have only created weaker defenses and more headaches for SMBs.

The solution to many of these issues is to keep antivirus scanning on the endpoint – utilizing an antivirus engine with a small footprint and low resource consumption – and migrating the management component to the cloud.

The GFI Cloud™ approach

Security vendor GFI Software addresses the shortcomings of cloud-based antivirus tools with GFI Cloud. To avoid bogging down networks, all scanning is performed on the endpoint, eliminating the need to transfer files back and forth to the cloud. To avoid performance problems, GFI Cloud's Antivirus service deploys an agent at the endpoint, where all scans take place, with minimal impact on system performance thanks to very low resource consumption inherent in GFI Cloud's Antivirus engine. From a browser-based dashboard, administrators manage all their protected endpoint devices and servers, scheduling scans, easily identifying infected machines and setting and managing policies. Scans take place on all devices regardless of Internet connectivity status, so if a computer is not online, the task still runs. As soon as the device is back online, it will immediately receive the latest definition updates and communicate its status to the cloud-based management portal.

Antivirus is one of a full complement of cloud-based security and infrastructure services offered through GFI Cloud™. GFI Cloud centralizes the management of security, networking and monitoring services – sold together or separately – on a subscription basis without the need for investments in additional IT infrastructure. GFI Cloud empowers SMBs to easily deploy and manage
an array of IT solutions which, especially for the smallest businesses, may have previously been out of their reach.

A busy IT administrator, who is also responsible for IT support and other day-to-day operations, now can leverage the full power of an enterprise-class solution without manually running servers and pushing definition updates on a regular basis. Deployment and management all take place through the GFI Cloud.

To get started, an administrator needs to only deploy the GFI Cloud agents to user machines across the network and manage the whole process through the web via the GFI Cloud platform. For organizations without the capabilities to deploy the agent from a central server, users can be provided with an agent download URL via email. Once the GFI Cloud agent is installed, it is as simple as a mouse click for administrators to begin managing antivirus from the cloud.

When an administrator logs into GFI Cloud, he or she gets a comprehensive view of all their services, such as Antivirus. They instantly know the status of every device they manage in one easy view. This centralized management approach simplifies client deployment of GFI Cloud's Antivirus agent on all servers, PCs, laptops and workstations. All configuration tasks, such as setting scan schedules, rebooting computers and setting policies, are accomplished through the GFI Cloud console.

Conclusion

Running antivirus is a complex task for administrators and, when left to users to manage, time-consuming and risky. The cloud alleviates these issues and makes antivirus management more affordable, but solutions that run scans in the cloud bog down networks and aren't always effective in detecting and fixing threats. GFI Cloud's Antivirus improves on this by scanning at the endpoint and centralizing management in the cloud, making it possible to deploy, monitor, manage, report and automatically address threats via a single dashboard. With Antivirus in GFI Cloud, smaller businesses gain the same level of protection against viruses, worms, Trojans and malware that the enterprise enjoys.

To learn more about Antivirus in GFI Cloud, visit gficloud.com.

About Antivirus in GFI Cloud

GFI Cloud's Antivirus service, gives IT administrators control of their company's network security, in minutes, with real-time threat protection against viruses, spyware and other malware.

Optimized to scan for security threats without hogging system resources or slowing down PCs – even during scans and updates; Antivirus installs and scans on the endpoint, so no sensitive data leaves your network for security checks.

Saving IT's time with automated scans and customizable group based policy management, its easy-to-use, web-based dashboard enables IT administrators to protect all their servers, workstations and laptops on the move, from one central point of control; anytime, anywhere.

About GFI Cloud

GFI Cloud gives hard-worked IT admins control of their company's IT, whether workstations are on or off the business network. Within minutes, its simple, web-based interface offers patch management, antivirus, asset tracking, workstation and server monitoring and remote control from one unified platform.

For busy IT admins GFI Cloud is the easy and affordable way to stay on top of their company's IT. With a single management console to secure the network, catch problems early and fix them fast, GFI Cloud streamlines IT operations, saves time and cuts costs.

GFI Cloud is the platform within which GFI delivers an expanding range of its award-winning software services.

For hands-on experience with GFI Cloud, you can register for a free 30-day trial from https://www.gficloud.com/freetrial

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

gficloud@gfiusa.com

33 North Garden Ave, Suite 1200, Clearwater, FL 33755, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

gficloud@gfiusa.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

gficloud@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

gficloud@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

gficloud@gfiap.com

For a full list of GFI offices/contact details worldwide, please visit **http://www.gfi.com/contactus**

www.gficloud.com

GFI 2013 April10