GFI White Paper

Managing security in a device-driven Windows environment

The increasing portability of computing devices, coupled with the rampant growth of mobile devices and portable storage means that organizations are faced with a growing number of threats. This white paper examines the landscape that is developing at a rapid pace and outlines the major areas of concern for the administrator.

GFI®

Contents

Introduction

The traditional desktop PC is dying in the workplace[1], and has been for a considerable period of time. A quick look across most small or medium sized businesses will quickly reveal that recent IT purchases have favored more mobile and technologically lightweight devices such as laptops, netbooks, smartphones, tablet computers and thinner clients[2].

The traditional model of the desktop computer – a bulky base unit, dedicated monitor, separate keyboard and mouse – is becoming more and more unusual in the workplace, much as it is in the home. However, this move away from immobile, tethered computers with fixed locations and fixed users has created a number of challenges for the IT department in terms of asset management, device security enforcement, network management and lifecycle management.

Things have been complicated further by end-user device creep – the growing trend for users to bring their own devices into the workplace with the expectation of interfacing them with workplace IT facilities such as email accounts, wireless connections and VPN services[3].

This means the IT department is challenged with managing the most diverse array of end user technology ever, while still having to maintain an efficient and available network. At the same time, IT must ensure these devices have adequate security measures running to prevent malware, vulnerabilities and ill-configured devices from compromising network safety and data protection.

To do this, IT departments are taking a device-centric view of security, ensuring that any device, rather than just the user, that comes onto the network is appropriately screened, secured and, if necessary, quarantined or limited to ensure that anything contained on the device that may be a risk does not contaminate other devices and data stores. This is in addition to ensuring that said devices are not used as a means to make unauthorized copies that could be lost, stolen or otherwise compromised.

Securing a Windows computing environment

Using a Windows operating system and application environment brings with it the benefit of access to a broad range of built-in and third-party solutions that can be called upon to address endpoint security.

With a single point of account administration available in the form of Microsoft Active Directory, third-party solutions can leverage a single Windows account and user profile to impose additional security controls based on overall policy, individual and workgroup exceptions, role-based rules and exceptions, and device exceptions where necessary, while retaining the ability to log, quarantine and push security agents onto new Windows-based hardware connecting to the network for the first time. Doing this without having to create parallel user and workgroup profiles within the endpoint security application not only saves time, it reduces the administration overhead and ensures that changes to access and operating privileges can be made swiftly and accurately[4].

Deploying a dedicated endpoint security solution will provide the IT department with important functionality to monitor and limit a number of PC-based activities that could pose a risk to overall IT security, including:

- **The creep of consumer devices into the enterprise** – Despite clear policies within most organizations about the use of approved and non-approved devices interacting with organizational systems and data, the creep of extremely powerful and capable end-user devices into the workplace has become commonplace. This scenario dates back to the early days of the Palm Pilot PDA, which achieved significant initial business penetration due to end users purchasing the devices themselves, then making the case for the IT department to support and service the devices, as well as enable data silos such as email available to them.

- **Control use of USB ports on endpoints** – I/O ports such as USB, FireWire, eSATA, Parallel and Serial pose a challenge for organizations trying to limit device access to network resources and also trying to prevent the storage of sensitive data on devices that can be easily removed from the workplace and from outside the scope of a monitoring solution. USB ports pose the most substantial risk, which is why it is important to have a solution in place that can not only monitor what peripheral devices are being connected to the PCs under management, but can also limit what can and can't access expansion ports. This can help prevent external hard drives and other flash storage devices from being used to store and remove copies of valuable, sensitive and potentially damaging data files.
- **Block transfer of particular file types** – Endpoint security goes beyond the ability to limit hardware use, but can also control data flow at the software level. If imposing limitations on hardware and peripheral storage use is not practical or too disruptive, an endpoint security solution can be used to limit file transfers by file type. As well as preventing sensitive files from leaving the network, this approach works also prevents certain file types and known high-risk attachments from leaving the endpoint and heading back in to the network where they could infect other machines with malware or where malicious code could exploit Windows or application vulnerabilities.
- **Encryption for mass storage devices** – if external storage devices are to be used legitimately in the workplace, endpoint security solutions can ensure they are used in the safest way possible. By imposing storage encryption on USB and other external storage devices, the risks posed by removable storage being lost or stolen while it contains sensitive data is reduced considerably, as the data will be encrypted and unreadable by unauthorized users.
- **Pushing antimalware protection to devices** – With the ability to push management and querying agents to devices as they join the network, an endpoint security solution will also have the ability to limit the impact of malware, ensuring clients are protected and scanned to minimize the threat from malcode that may be tracked into the network from the device having been used in untrusted locations or being used for transporting untrusted data.

Although it is possible to carry out some of these functions at the BIOS level, for example blocking portable and removable storage devices such as CDs and floppy drives, this approach is seldom convenient and is impractical when applying software or network upgrades. For example, a new software or device installation would require the administrator to physically visit each machine, an activity which is both a time-consuming and costly.

Tamper-proof endpoint security is extremely important, but difficult for the IT department to deploy and enforce. A high proportion of end users have administrator level account privileges on the Windows devices they use in the workplace. However, there are numerous measures now being offered within endpoint security solutions to aid the IT department and ensure that users can't circumvent controls, even if they have administrator accounts.

While a determined user can hack a BIOS to circumvent a BIOS-level security measure altogether; endpoint security agents can be more robust, with many featuring anti-tampering and self-repair features in order to prevent and recover from a destructive attempt or registry edit intended to remove the agent and regain access to blocked features.

Endpoint protection agents can also enter a locked-down mode in the event that communications with the management console is not established for a prolonged period, or if fake (hacked) management console information is sent to the endpoint in an effort to change permissions or disable the agent altogether.

Managing on-site and off-site devices and users

With the array of devices now requiring access to the corporate network, the process of managing these manually and trying to set appropriate policy is impractical at best. Endpoint security solutions not only tackle important frontline security concerns, but also provide important reporting, monitoring and device management tools.

Endpoint security can provide valuable insight into who is using the network, how they are using it, what devices they are using and what activities they undertake while logged in with those devices, for example:

- **Asset management** – Endpoint security solutions will need to index and identify the devices connecting to the network in order to push the appropriate agent to them, authenticate the devices and apply the appropriate policy limitations. That means generating asset discovery reports and logs, often in conjunction with whitelists of known and approved devices, while also maintaining blocklists of prohibited devices such as certain consumer technologies that you want to keep off the network at all costs. The ability to update and manually expand the database of supported devices with custom entries will allow IT administrators to customize the solution to the specific device needs of the organization.
- **Policy creation and management** – Access and device logs provide essential visibility of what is being used on the network and what tasks are being performed. This data, stored in logs and detailed visual reports is valuable intelligence for refining IT security policy so that it keeps pace with changes in technology, user habits, emerging security threats and the requirements of legal and industry regulation regarding data security and access management.
- **Activity management and reporting** – When taking a device-centric approach, it is critical to understand what the technology is being used for. This is particularly important in hot-desking environments or transient environments such as schools, libraries and municipal public buildings, where the providers of Internet connections and networks have a duty of care to ensure that users are not at risk and that the IT resources on offer are not being used for criminal, illicit or otherwise undesirable activities.

Extending security to mobile devices

With so many different mobile devices in use today beyond conventional PCs, there are clear risks associated with allowing many of these to connect to business resources such as Internet connections, VPN tunnels and other office computers directly for the purposes of syncing, charging and for use as an external storage drive.

With many of the non-Windows platforms used on devices such as smartphones and tablets being effectively closed systems, pushing an agent to them is not always a practical or preferred method. Unapproved mobile devices can pose a potentially significant risk to the organization, as well as potentially compromise productivity through disruption and incompatibility with enterprise applications and services[5]. Therefore, it is essential that any endpoint solution can provide detailed monitoring and reporting of what devices are connecting to the network, and what devices are connecting through the Windows PCs – the main endpoints – that are, in turn, connected to the network.

Detailed reports on mobile device use provide essential insight into which devices staff are using, and how they are using them. From these reports, the IT department can quickly build a picture of how these devices fit into the day-to-day workflow, and what threat they pose to IT and data security. From there, policies can be augmented to limit access and exposure. For example, USB ports can be disabled on desktop computers for all but essential devices such as keyboards and mice, preventing business computers from being used to sync and interface with unauthorized devices.

Devices that can't have an agent pushed to them can be quarantined, so devices such as tablets that connect to office Wi-Fi networks can be isolated from the core network – for example, allowing them access to the open Internet but not to file shares and public folders – as a way of balancing the user's desire to keep their device useable in the workplace and the organization's need to protect systems and data from unacceptable risk.

The popularity of USB 3G modems and Internet connectivity via tethered smartphones has created a significant challenge for administrators. If a user is able to connect their own inexpensive and driverless Internet connection device to the endpoint, it can effectively render useless the investment in a gateway security solution. Unrestricted Internet access via a 3G modem in the workplace, while the endpoint is still connected to the corporate network, creates significant risk. Users can browse the web and exchange files without the normal restrictions and web filtering controls, raising the risk of malware infection, data loss and theft, legal and regulatory infringement and of course a potential loss of productivity.

However, portable Windows devices equipped with 3G modems can have access to these disabled while on the corporate network, preventing users from running external Internet connections on their devices as a means to circumvent gateway level controls and access limitations on the corporate network.

Summary

The increasing portability of computing devices, coupled with the rampant growth of mobile devices and portable storage means that organizations of all sizes need to have clear policies and technologies in place to ensure that systems and data are not at risk from theft, malware and other forms of mishandling brought about by users bringing unauthorized and unmanaged computing devices into the workplace and connecting them to the enterprise network.

With a sizeable number of workers using portable computers and working in the field, having a solution in place within the core workplace that can ensure up-to-date security agents are pushed to Windows devices as they connect to the network for the first time is essential. Doing so will automate the application of key safeguards, such as a default blocking policy to prevent the transfer of hazardous code until security measures and antimalware tools are up to date and the IT department are confident that the device does not pose a risk to data, other users and other systems connected to the IT infrastructure.

Along with centralized monitoring of what is connected to the network and to devices on the network, plus the ability to manage I/O port use, the end result is a robust, cost-effective and easy–to-manage solution that ensures security is maintained regardless of what Windows computer is used and what storage device is connected to it.

1 http://www.guardian.co.uk/technology/2011/aug/17/pc-shipments-fall-tablets

2 http://www.gartner.com/DisplayDocument?id=1871420

3 http://www.computerworlduk.com/in-depth/infrastructure/3287249/enterprise-is-being-overrun-with-consumer-devices/

4 IDC Market Analysis: Worldwide Endpoint Security 2010–2014 Forecast

5 http://searchconsumerization.techtarget.com/news/2240034835/Mobile-endpoint-security-and-management-Best-practices

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

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

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

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@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

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

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

GFI 2646 jan12