

I D C E X E C U T I V E B R I E F

Portable Policy Management: Taking Control of Today's Extended Enterprise

August 2006

By Fred Broussard and Al Gillen

Sponsored by FullArmor Corp.

Introduction

There is little doubt that mobile computing is the next big wave in the evolution of business information technology. With benefits such as enhanced employee efficiency, greater overall productivity, and improved customer service and satisfaction, the demand for extensible enterprise networks that support remote and mobile users will surely grow stronger. However, a fluid computing environment that includes mobile, embedded, and disconnected devices creates significant management challenges for enterprise network administrators. This Executive Brief examines the business drivers for extending today's enterprise networks, the challenges of this computing environment, and the benefits of implementing key policy-management technologies to gain control.

Business Drivers for Enterprise Policy Management

The business market is becoming increasingly in need of mobility. Workers are requiring greater flexibility in how and where they do their jobs, including needing mobile access to their company network. Improved wireless networks, a broader range of mobile devices, easy virtual private network (VPN) access for remote workers, and other advances are motivating companies to increase the mobility and location flexibility of their workers. With benefits such as enhanced employee efficiency, greater overall business productivity, and improved customer service and satisfaction, many organizations are pushing to implement mobile and remote workforce solutions within their enterprises.

This trend is creating greater challenges for IT professionals to manage and secure the extensible infrastructure that is today's enterprise network. IT departments are judged primarily on their ability to support users of all kinds — local and remote — as well as keeping the network and IT systems up and running continuously. Successful organizations, regardless of size, must deliver high-quality services through policies that quickly adapt to changes in

users' locations and must enforce these policies on machines using the corporate network.

Computing Environment Challenges

However, managing the machines that "float" in and out of contact with an enterprise network presents significant challenges when the users are remote and not necessarily directly connected to the office infrastructure. These challenges include the following:

- Remote users possessing multiple machines needing to be managed
- Non-corporate users, such as temporary employees, contractors, vendors, or customers, that need access to corporate networks
- Remote users logging onto a corporate VPN where policy is not immediately updated and enforced
- Intermittent connectivity means that updates may not be distributed to all machines at any one time
- Personalized desktops for different lines of business within the enterprise are proliferating, where individual users modify their own settings, creating nonstandard configurations that are collectively harder to manage
- Malicious actions may occur to remote machines through the use of removable storage devices or devices that may connect directly to the remote machine

As a result of these challenges, IT administrators can be forced to abandon management of these mobile and remote users, risking security violations of the network, as well as failing to provide necessary support and services to existing employees.

IT administrators need the capability to manage and enforce remote systems' settings as they arrive on the network. They also need to keep the network safe through inadvertent action from end users. This security enforcement includes the capability to lock down the desktop from users using USB storage devices.

Within a short time, a computer can be rendered almost useless to a subsequent user because of changes made by previous users. Likewise, the accidental introduction of spyware, viruses, and other malware can degrade system performance and reduce the privacy and security of the next user's personal information that may be entered into a legitimate Web site.

Technology Solutions

The Windows server operating environment offers the following technology to manage and enforce security and usage policies:

- **Active Directory** — A hierarchical directory service that is LDAP-compliant and built on the Internet's Domain Naming System (DNS). Workgroups on an enterprise network are given domain names, just like Web sites, and any client can gain access to the domain. Active Directory can function in a heterogeneous enterprise network and encompass other directories, including NDS and NIS+.
- **Group Policy** — A software that provides centralized management of computers and users in an Active Directory environment. Group Policy can control a target object's registry, NTFS security, audit and security policy, software installation, log-on/log-off scripts, folder redirection, and Web browser settings. The policy settings are stored in Group Policy Objects (GPOs). Group Policy can be used as the basis for managing a group of technologies, which relate to the administration of disconnected machines or roaming users, and include Roaming User Profiles, Folder Redirection, and Offline Folders.

Within the framework provided by Active Directory and Group Policy, network managers can take advantage of third-party technologies that augment the native Windows technology and enable the management and enforcement of remote systems' settings as users arrive on the enterprise network. There are Web services-based technologies, for example, that let network managers automatically enforce Group Policy settings on machines that are temporarily or permanently disconnected from Active Directory. This functionality enables enterprises to maintain the security of their network's endpoints by extending directory-based policy management over the Internet.

Similarly, there are policy-setting tools that empower network managers to create and maintain standardized desktop configurations that aren't available in the native Windows environment.

Benefits

The capabilities of Active Directory and Group Policy, enhanced by third-party policy monitoring and management technologies, provide the following important benefits to organizations:

Reduced Cost and Complexity

- One way to control network ownership costs is to decrease the number of domains managed; another way is to lower the number of servers and standardize desktop configurations —

both of which lead to a reduction in the overall man-hours required for management, troubleshooting, and support.

- Administrative tasks that are often tedious and time-consuming, such as computer configuration, can be simplified and automated by leveraging Group Policy settings. Help desk calls can be reduced by ensuring proper configuration of the basic end-user operating environment, as well as business-critical applications.
- Disconnected and intermittently connected computers that previously presented management headaches can be brought into the system-management fold.

Security and Availability of Key Business Services

- Enterprise policy management enables device lockdown, including granular control of USB storage devices. Other security-related management includes control of local administrator group membership, as well as control of local administrator passwords.
- Enterprise network managers can be assured that configuration changes to endpoints, such as desktops and laptops, do not create vulnerabilities in the network. They have the ability to maintain the security settings of remote and home computers, as well as of computers temporarily disconnected from the network, or those computers or non-corporate users that may be outside the network domain.
- Using third-party Group Policy management technology, remote and home computers connecting to an enterprise network over a VPN can have the latest security and configuration policies immediately applied, correcting past policy violations.

Regulatory Compliance and Best Practices

- Government and industry regulations are putting unprecedented pressure on organizations handling sensitive or personal information. Policy management plays a key role in ensuring that only authorized users can gain access to information stored on mobile computing devices.
- When the proliferation of nonstandard desktop and other client-computer configurations can be prevented, compliance with regulatory and corporate policies is more easily enforced.
- As new devices and computing endpoints are added to an enterprise network, economies of scale can be achieved by forcing strong lock-down policies on individual users. Leveraging the Windows server operating environment and third-party tools will make this task easier to manage.

Conclusion

The fluid networking environment compelled by mobile and remote computing places enterprises at greater risk for security breaches, compliance violations, and increased IT costs. The extensible infrastructure that is today's enterprise network must deliver high-quality services through policies that quickly adapt to changes in users' locations. Moreover, network administrators must be able to enforce these policies on any machine or "endpoint" anywhere on the corporate network.

The Windows operating environment provides important foundational technology in Active Directory and Group Policy for managing usage and enforcing security policies, but it lacks the capability to monitor, enforce, and audit policies on machines that "float" in and out of contact with an enterprise network. IT managers need to take advantage of third-party tools that augment the native Windows technology and enable the management and enforcement of systems' settings as mobile or remote users arrive on the company network.

IDC believes that, with the continued rise of mobile and remote computing, the need for portable policy management for enterprise networks has never been greater. It behooves IT managers to investigate solutions that will help their organizations ensure endpoint compliance with corporate security and configuration standards.

COPYRIGHT NOTICE

The analyst opinion, analysis, and research results presented in this IDC Executive Brief are drawn directly from the more detailed studies published in IDC Continuous Intelligence Services. Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. Contact IDC Go-to-Market Services at gms@idc.com or the GMS information line at 508-988-7610 to request permission to quote or source IDC or for more information on IDC Executive Briefs. Visit www.idc.com to learn more about IDC subscription and consulting services or www.idc.com/gms to learn more about IDC Go-to-Market Services.

Copyright 2006 IDC. Reproduction is forbidden unless authorized.