

Desktop Security:

Protecting Against Malware and
Securing Data Access with Thin Clients



May 2004 was the fifth-worst month on record for virus, worm and Trojan attacks, according to the U.K.-based mi2g Intelligence unit, which has been tracking and analyzing security events since 1995. Worldwide damage totaled between \$16.2 and \$19.8 billion, thanks mostly to the spread of the Sasser worm and its variants to millions of PCs worldwide.

August 2003, a.k.a. the “August Can of Worms,” was another record-setting month. Thousands of systems were hit with the one-two-three punch of Blaster, Nachi and SoBig.F. Blaster managed to do over \$750 million in damage, according to Computer Economics, even though it exploited a Windows vulnerability that Microsoft had issued a patch for months before.

MyDoom, which hit in late January 2004, spread even faster than SoBig.F, first infecting users of Kazaa, the popular peer-to-peer file sharing network, then quickly moving to email. Millions of users clicked on its suspicious attachment, despite warnings and explicit corporate policies against such practices. MyDoom’s damage will add up to \$4.5 billion, according to Computer Economics.

Malware has become a depressing fact of life for just about every organization, with the constant risk of losing thousands or millions of dollars in productivity, reputation and revenue from a single event. Companies often struggle to get their systems up and running again after an attack, only to be blindsided by re-infection from an unprotected notebook or telecommuter system. And it doesn’t look as if the situation will improve anytime soon. In June 2004, mi2g raised its estimate of the probability of a catastrophic global malware attack, with damage surpassing \$100 billion, from 1 in 40 (2.5 percent) to 3 in 10 (30 percent)

As if malware weren’t enough of a threat, computer and data theft are also very serious problems for most organizations. In November 2003, thieves stole three computers containing personal and financial data on thousands of customers maintaining line-of-credit accounts with California-based Wells Fargo. In August 2002, the U.S. Department of Justice announced that between October 1999 and January 2002, more than 400 computers had been lost or stolen from the FBI, Immigration and Naturalization Service (now known as U.S. Citizenship and Immigration Services), Drug Enforcement Administration, Federal Bureau of Prisons and U.S. Marshals Service.

At about the same time, U.S. Customs & Border Protection reported that it had lost 2,251 computers between 1999 and 2001. Many of these systems contained classified data that would be very useful to criminals and terrorists. Brigadoon Software’s 2003 BSI Computer Theft Survey, which interviewed 676 respondents worldwide, found that 44.5 percent experienced computer theft or worked for an organization that had experienced computer theft. Ninety-nine percent reported that the thief was never caught. The value of data on those stolen computers averaged a whopping \$690,759.61 per system.

Aside from damage to revenue and reputation in the U.S., new regulations such as the Graham-Leach-Bliley, Sarbanes-Oxley and Health Insurance Portability and Accountability Acts add a new dimension to the risks companies face. Now corporations can incur steep fines or even criminal prosecution if it’s determined that they are not taking the proper measures to protect customer data or to store and secure certain other types of information so that it can be retrieved quickly.

In fact, data protection compliance legislation is growing all over the world. All 25 member states of the European Union are bound by the EC Directive 95/46/EC, which lays down strict standards of data stewardship for organizations that hold information on its citizens. It also gives almost half a billion EU citizens the legal right to see all information any organization has on them. If a citizen exercises this right through a court, it costs an organization, on average, \$90,000 per request to provide the information.

Today’s companies are getting the message. Market research firm International Data Corp. (IDC) projects that worldwide

TOP TEN SECURITY BENEFITS OF THIN CLIENT COMPUTING

1. Thieves cannot access data from a stolen thin client, since thin clients don’t store data or applications locally.
2. Thin clients don’t need personal firewalls or anti-virus agents.
3. No need to back up thin clients.
4. Users can’t disable anti-virus agents or install their own applications, services, unauthorized peripherals or data devices on a thin client.
5. No residual data left on a thin client after an application or Web session.
6. No data travels over the wire to and from a thin client on a wireless or wired LAN. Control and verification happens at the network level.
7. No need to spend time reinstalling applications on new client systems if thin clients are lost in a disaster.
8. Thin clients can be redirected in minutes to a second server with replicated applications and data if primary location experiences an outage.
9. Fewer service calls means fewer opportunities to introduce security problems.
10. Centralized field maintenance through Wyse™ Rapport® Device Management Software enables tighter network security.

spending on security and business continuity will grow twice as fast as total IT spending over the next several years, reaching more than \$116 billion by 2007. Forty percent of nearly 1,000 IT managers surveyed by IDC in July 2003 rated security their highest priority.

SECURITY: IT'S ABOUT MANAGEMENT

There was a time when security meant simply protecting the network's gateway to the Internet. Today's attacks, however—including the ones mentioned above—often breach the network through unprotected desktop, telecommuter and road-warrior PCs and notebooks, as well as PDAs. Companies struggle to ensure that all of these network endpoints, with their sometimes uncooperative users, are kept up-to-date with the most recent firewalls as well as anti-virus, spyware and operating system patches. But it's not always possible.

For example, a user's notebook may become infected by a virus or worm during a business trip. Then, if the user reconnects the notebook before a patch can be applied, the infection will likely spread to the network. Also, many users disable their anti-virus agents to increase system performance, or they may install new hazardous applications (such as peer-to-peer client software) without the knowledge of IT. Telecommuters sometimes even give their children access to the systems they use for work.

And even if all systems are somehow kept up-to-date, new application-level attacks for which patches have not yet been released can infect thousands of networks in a matter of hours or even minutes. For many companies—particularly those with very sensitive security issues—the management of desktop and notebook security can be overwhelming and very costly.

THIN CLIENTS TO THE RESCUE

The truth is that it doesn't have to be this way. There is an alternative to PCs that vastly simplifies the management of security and business continuity with little or no sacrifice by PC users: server-based computing, also known as thin client computing.

In a network running a server-based computing solution, users have access to the same Windows and other applications as their PC brethren. But instead of running locally on thousands of desktops and notebooks, these applications run and store their data on centrally secured and managed servers. Housed within a secure data center, these servers typically run Microsoft Windows Terminal Services or Citrix MetaFrame, allowing for multiuser access to Windows-based and Web-based applications.

Users access their applications and data over the network with thin clients, which look and act very much like PCs. However, thin clients store no data and run few or no applications locally—other than a lightweight thin client operating system, a terminal emulator and perhaps a Java-equipped Web

browser and/or media player. No data traverses the network, only mouse movements, keystrokes and screen updates.

For those who think that a thin client is nothing but a throwback to the disco days of dumb green-screened terminals, think again. Thin clients provide access to the same applications and graphical interfaces that traditional PC users run. With today's high-speed networks and powerful server hardware, thin client performance is the same or faster than running the applications locally. The only thing they are not good at is high-end graphics, such as CAD, or gaming applications that rely on a local application connected through a high-speed bus to a high-end graphics card. Thin client computing makes particular sense for companies whose users already spend much of their day accessing Windows office productivity suites, browser-based applications such as ERP or CRM and legacy green-screen applications that need terminal emulation.

Server-based, thin client computing is much less expensive and resource intensive to manage than typical PC computing. But for high-security environments, the security and business continuity benefits of thin client computing are particularly dramatic.

Take hardware theft, for example. Since no data is stored locally, the theft of a thin client has no real security implications. The thief can't access any corporate data or applications. Instead, both are protected on highly secure servers located in fortified data centers. Theft is far less likely to occur in a secured data center environment—where Internet access can also be carefully controlled and monitored—than in the office or on the road.

Thin client systems from Wyse are easily equipped with strong password protection and advanced authentication methods such as smart cards or biometric devices. So even if the thief somehow manages to get near the network with a stolen thin client, he's unlikely to be able to use it to connect to those servers.

With thin clients, the thorny management headache of client backup becomes a thing of the past as well. That's because all up-to-date information is by definition stored on a few servers or network or SAN storage devices, whose regular backup is more easily managed than that of thousands of widely distributed PCs. Data required for the fulfillment of regulatory obligations is always current and centrally located, where it's much easier to secure and access.

THE CURE FOR PATCH-MANAGEMENT HEADACHES

Patch management, an exercise that often feels like herding cats, is another security management problem that thin client computing solves. With thin clients, there's no need to protect thousands of clients with personal firewalls and anti-virus agents, as there is no place for malware to reside on the client. Rather than



finding a way to distribute security patch updates to hundreds or thousands of widely dispersed PCs, efforts may be concentrated on the few servers running user applications. If a new virus hits, it can be contained and eradicated much more easily on a few servers than if it spreads to thousands of user PCs.

Companies also don't need to worry about uncooperative users bringing new risks into the network. These users can't disable anti-virus protection, because thin clients don't need it. They usually can't install their own applications or introduce infected media, because thin clients generally lack hard disks as well as floppy and CD drives. And since applications only run on the server, it's relatively easy to restrict or block use of peer-to-peer and instant messaging networks, which are easy entry points for malware and other attacks.

A dramatic reduction in service calls is another benefit of thin client computing. There's rarely a need to troubleshoot a thin client since it has few moving parts, runs few or no applications and provides very few opportunities for user-induced problems. Fewer service calls means fewer opportunities to introduce security problems either accidentally or intentionally.

Finally, since they store nothing locally and have much higher mean-time-between-failure rates than PCs, thin clients make sense for insecure public-access environments. Users no longer have to worry about others accessing residual files or data left on a machine's hard disk from their use of the Internet or other applications. Further, the thin client's Web browser can be run from the server, so no residual data resides in client memory; or client browsers can be set to delete residual data from memory automatically.

MOBILITY AND DISASTER RECOVERY

It may seem as if server-based computing would limit user mobility, but that's usually not the case. Thin client telecommuters and business travelers can access the network remotely with the same virtual private networking connections that PCs use. Since no data passes over the connection, performance is relatively speedy, even over a 56K dial-up connection.

The fact that client sessions run on the server instead of the client has actual advantages for both user mobility and business continuity. For example, a user can start an application session on one system, and then move to another machine down the hall, across campus, or even at home. Once logged in, the user may continue that application session exactly where he left off—a mobility feature that typical PCs can't provide. The server stores all the user's system preferences, so the session looks and feels exactly the same on any client system.

Imagine what this means for disaster recovery. It's easy to replicate server data and applications periodically throughout the day to servers at another location—even across the country. If one server location is shut down by a fire or other natural disaster, client systems can be redirected seamlessly to mirrored or clustered servers, allowing users to continue working without even noticing the disruption.

Thin clients also offer "desktop disaster recovery" capability—something PCs really cannot offer. If thin clients are damaged or destroyed, a hot spare can be installed very quickly and will automatically configure itself within minutes without any IT support, ensuring continued access to server-based applications and data. This unique capability of thin clients means that an organization's disaster recovery capability can run from the hard disk all the way to the keyboard. This capability can also be used if employees have to work from another location, such as their home, in the event that the office cannot be accessed. This is useful for non-disaster events that still effect business continuity such as weather or transport disruption.

Newer wireless thin client solutions are a boon to security as well. As with PCs and laptops, wireless thin client users can access their applications as they move with their system from room to room. But unlike with PCs, no data is passed across the wireless LAN—again, only keyboard, mouse and screen updates. Thin client traffic is also typically encrypted within its robust ICA/RDP protocols. Hackers, therefore, have little to gain by attempting to sniff the wireless LAN—a surprisingly easy undertaking in the PC world.

There are indirect security benefits to server-based computing as well, as the significant management savings from reduced PC visits for troubleshooting and maintenance can be redirected to security efforts.

CONCLUSION

Security continues to be an urgent, widespread concern among today's organizations, which are struggling to keep PCs and their users up-to-date with the latest protection methods and patches. For many of these organizations, server-based thin client computing provides a very viable, lower-cost alternative to the chaos of PC management.

By centralizing applications and data on a few servers instead of hundreds or thousands of PCs, server-based thin clients also make securing the network from the latest attacks much more manageable and less expensive. In turn, this allows IT staff to focus on *improving* the business, rather than simply defending it against intrusion or disaster.

Sponsored by Wyse

Copyright© July 2004 Ziff Davis Media Custom Publishing. All Rights Reserved. Reproduction in whole or in part in any form or medium without express written permission of Ziff Davis Media Inc. is prohibited. The information contained herein is accurate only as of the date of publication, and is subject to change without notice.