

5 SECURE REASONS FOR THIN CLIENTS

IF YOU NEED JUSTIFICATIONS FOR ADOPTING THIN CLIENTS, LOOK NO FURTHER.

BY PAUL A. STRASSMANN

ACCESS TO WEB APPLICATIONS IS TYPICALLY the most frequent use of a personal computer. Whether this should be done by means of a “fat” computer or by the increasingly available “thin” client is a question on many enterprise agendas.

The fat solution offers mainframe-like—as well as stand-alone—capabilities for the desktop, making it attractive from the user standpoint. The thin approach has demonstrably lower operating costs and significantly lower security risks, both of which favor a corporate point of view.

The security side of this equation is what enterprises should weigh most heavily. The following are five security justifications that underscore why enterprises should adopt thin-client models.

1. ZOMBIE PREVENTION

By far the greatest damage an adversary can inflict on an enterprise is capturing its PCs and turning them into zombies. A zombie is a PC infected with a Trojan—an application that gives hackers unfettered access. Zombies linked together in a network are often referred to as a botnet, which can be used to attack other networks. All it takes for a zombie to get in is an unsuspecting operator who downloads a malicious file, despite regulations prohibiting that.

One advantage of thin clients is their inability to become zombie hosts. Their operating systems are closed and have no disk drives. This means zombies have no place to insert malicious code, at least at the endpoint.

Thin clients depend entirely on applications hosted on servers that typically have more secure computing power, defenses, operator attention and software configurations than the average fat client.

2. THEFT DODGING

Stories abound about stolen laptops containing thousands of confidential records ending up in unauthorized hands. Although some enterprises have policies that require sensitive data to be encrypted on laptops, this level of protection is rarely implemented—and even if data is encrypted, users often compromise encryption applications by applying weak passwords to the cipher key. Another advantage of thin clients is they do not have disk memory, rendering a stolen thin client useless to a thief. It cannot be used except on an authorized and better-protected hosting server. The tradeoff, obviously, is that thin clients lack mobility.



3. FILE MANAGEMENT

Most IT policies restrict sending gigantic file attachments because they clutter disk files. For instance, several versions of a 100-KB PowerPoint presentation can expand to anywhere from 20 GB to 100 GB. In a thin-client environment, an originator posts the source file on a shared server. This makes it possible to track all attachments and to store only a single archival copy as a reference.

Thin clients should be initially restricted to environments that call for well-defined functions, such as confidential communications or highly structured tasks. Thin clients may have limited use in dealing with graphic-rich

applications. Within limited choices the extraction of redundant attachments should be easy.

4. SOFTWARE CONTROL

IT management is reluctant to permit users to install unauthorized software—particularly software published by unknown sources. This is more than a licensing issue; applications downloaded from Web sites often contain Trojans and other malicious code that open back doors or leak data. While it's possible to configure a fat client to prevent the installation of software, an IT department has much greater control over application installations and configuration management in a thin-client architecture.

5. PERSONAL USE LIMITATIONS

Company-owned PCs are often used by employees for personal purposes, such as online shopping and travel planning. It's not feasible to block personal access to every conceivable Internet location. Besides, users will always find ways to circumvent blocks put up by IT departments. In a thin-client architecture, enterprises have much greater control over the applications and Web sites users can access.

Obviously, thin clients aren't best for every enterprise or every class of user. But for enterprises with a large number of stationary, non-power users, thin clients may present the best option for secure, cost effective and ease of management. ◀

PAUL A. STRASSMANN IS A FORMER TECHNOLOGY EXECUTIVE AT GENERAL FOODS, KRAFT, XEROX, THE DEPARTMENT OF DEFENSE AND NASA. SHARE YOUR EXPERIENCE WITH THIN-CLIENT ARCHITECTURES WITH HIM AT EDITORS@BASELINEMAG.COM.