Microsoft Solutions

Recognizing security threats and putting solutions in place to prevent them is a key responsibility of today's IT departments. Some of the challenges IT professionals face in their mission to provide more secure and reliable services include:

Preventing the introduction of viruses and malicious content. If allowed onto the corporate network, computer viruses can cause havoc on computing systems; disrupting operations, infecting data and even enabling theft of valuable company assets. Regardless of how computer viruses sneak onto a network, the result is often devastating and expensive.

Keeping the network running, available and accessible. As a core IT service, the network must be available and accessible. With so many different systems and devices on the network today, access control can be complicated and inconsistent. Solid security tools can simplify this complexity and increase security without compromising access.

Balancing access and security. Distinguishing between threats to your network and legitimate access requests is a key challenge. The most secure system in the world is the one no one can access, but it is also practically useless. Therefore, security threats must be recognized and neutralized without a disruption in service.

Key elements of more secure network services include:
• Firewalls
• Secure Remote Access
• Antivirus Capabilities
• Patch/Update Management

Establishing an optimized and more secure network can benefit your organization by:
• Ensuring a more stable and secure infrastructure.
• Providing standards for policies, which provide a more consistent environment.

• Rapidly and reliably delivering security updates to address targeted vulnerabilities in software assets.
• Establishing security layers at the perimeter, server, desktop and application levels to provide a controlled, robust environment able to withstand malicious attacks.

Firewalls

ISA Server 2006 is an integrated edge security firewall that helps protect IT environments from Internet-based threats while providing users fast and secure remote access to applications and data. It provides value to IT managers, network administrators and information security professionals who are concerned about the security, performance, manageability or reduced cost of network operations.

ISA Server 2006 enables organizations to make their Exchange, SharePoint and other Web application servers accessible in a more secure way to remote users outside the corporate network. By pre-authenticating users before they gain access to any published servers, inspecting even encrypted traffic at the application layer in a stateful mannerand providing automated publishing tools, ISA Server 2006 makes it easier to provide security for corporate applications accessed over the Internet.

Secure Remote Access

Microsoft's Intelligent Application Gateway (IAG) 2007 with Application Optimizers provides secure socket layer (SSL) virtual private network (VPN), a Web application firewall and endpoint security management that enable access control, authorization and content inspection for a wide variety of line-of-business applications. IAG also enables IT administrators to enforce compliance with

PROSYS

application and information usage guidelines through a customized remote access policy based on device, user, application or other business criteria.

Key benefits include:
• A unique combination of SSL VPN-based access, integrated application protection, and endpoint security management.
• A powerful, web-application firewall that helps keep malicious traffic out and sensitive information in.
• Reduced complexity of managing secure access and protecting business assets with a comprehensive, easy-to-use platform.
• Interoperability with core Microsoft application infrastructure, third-party enterprise systems and custom in-house tools.

Antivirus

Microsoft Forefront Client Security provides unified malware protection for business desktops, laptops and server operating systems. Microsoft Forefront Security for Exchange Server and Microsoft Forefront Security for SharePoint help businesses protect their Microsoft Exchange Server 2007, Microsoft Office SharePoint Server 2007 and Microsoft Windows SharePoint Services 3.0 environments against viruses, worms, spam and inappropriate content.

The benefits offered by Microsoft Forefront Security include:
• Unified protection from viruses, spyware and other current and emerging threats.
• Simplified administration through central management so you can protect your business with greater efficiency.
• Visibility and control through insightful, prioritized security reports and a summary dashboard view so you have visibility and control over threats.

Patch/Update Management

Microsoft Windows Server Update Services 3.0 (WSUS 3.0) enables information technology administrators to deploy the latest Microsoft product updates.

By using WSUS, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network.

Phased Approach

We take a phased approach to your Networking and Security projects, with set milestones based on best practices. These phases are based on Microsoft's proven approach to technology projects, the Microsoft Solutions Framework (MSF). This is how it works:

Assess: Help identify your business drivers, review your current environment and develop an initial logical design for the new environment. The phase concludes with a milestone where you approve the vision and scope, based on the business case.

Design: Our experts work closely with your staff to refine the design for the new environment. At the end of this phase we re-examine the business case to ensure the design aligns with the desired goals.

Plan: Once the infrastructure design is complete, our team guides your staff through the implementation options and documents the detailed plans.

Build: With the plans completed, we help test the infrastructure design, implementation strategy, systems management design and operations plan in a test lab.

Stabilize: Our team helps define a detailed release-management plan and sets up a pilot environment to further stabilize the final solution.

Phased Project Approach

ASSESS
DESIGN
PLAN
BUILD
STABILIZE
DEPLOY
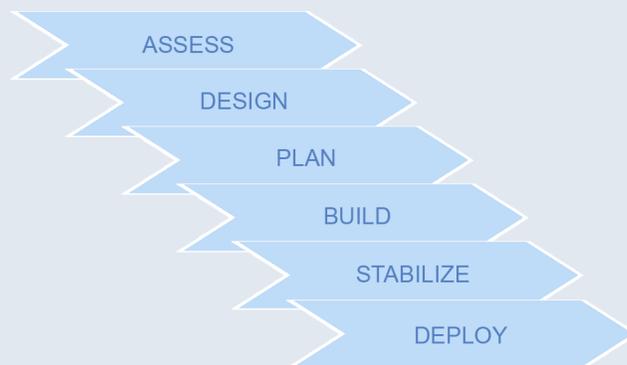
Deploy: The core technology and site components are deployed and the project is transitioned to operations and support. After the deployment, the team conducts a project review and a customer satisfaction survey.

Not Sure Where to Begin?

Let us help. We can assess your current environment, help map strategic business goals to the capabilities offered in our Microsoft Solutions for Networking and Security and help establish your end-state vision for implementation. For more information contact us at mssolutions@prosys.com or contact your local ProSys representative.