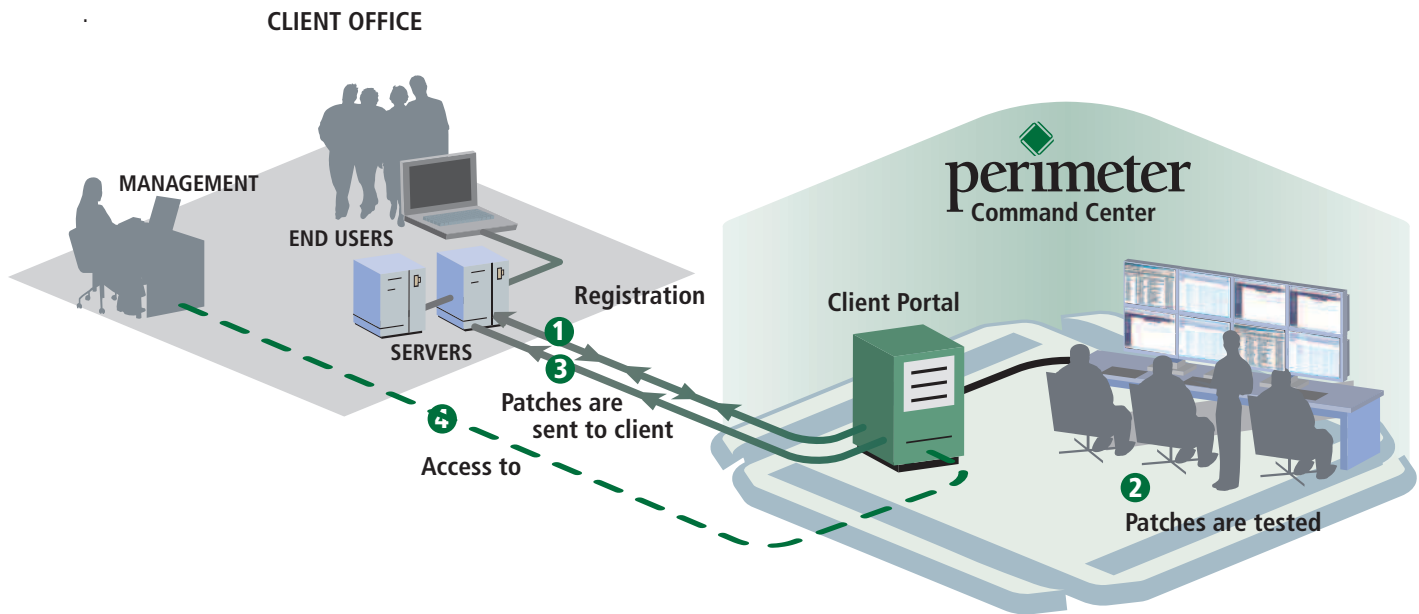


Patch Management Service

Service Overview

While patch management is critical to the security of your organization, the process of effectively researching, deploying and maintaining patches is an incredibly costly and complicated endeavor. In the time that it takes for a patch to be issued and deployed, your business is vulnerable to security breaches, mass outages, productivity reduction and ultimately the loss of customer confidence. The deployment of patches is a complex process - it can take days of researching, testing and deploying for every patch when there are hundreds of patches issued each day. Without a dedicated team to ensure that the accurate patches are deployed quickly and correctly in your environment, you may be exposed to some of the most severe attacks.

Perimeters' Patch Management service ensures that corporate risk tolerance, security vulnerabilities, configuration/change management, IT infrastructure inventory, and functional and business issues affecting a company's information systems are addressed in a timely, efficient and cost-effective manner. Perimeter's Patch Management Service enables businesses to quickly and confidently implement patches to maintain a stable and secure networking environment.



Service Highlights

Perimeters' Patch Management Service is designed to seamlessly integrate a robust patch management process into your daily IT operations. Our security professionals take a comprehensive and top-down approach to patch management, and utilize industry best practices such as ISO 17799. The process is also based on applying business and technical requirements, including those for change management, security policies, network infrastructure, and operating systems inventory. Perimeter is uniquely qualified to deliver Patch Management Services because of the strength of our Microsoft, Security, and Network and Systems Management consulting expertise, and our successful track record of solving management challenges in complex enterprise and regulatory environments.

Key Features & Benefits

Feature	Benefit
Automated assessment of patch status	Discover security issues with current server infrastructure
Monitoring & evaluation of new patches	Ensure that patches to be deployed are applicable and clean
Initial deployment of patches to sandbox	Test patches for smooth operation in client's unique server infrastructure prior to full deployment



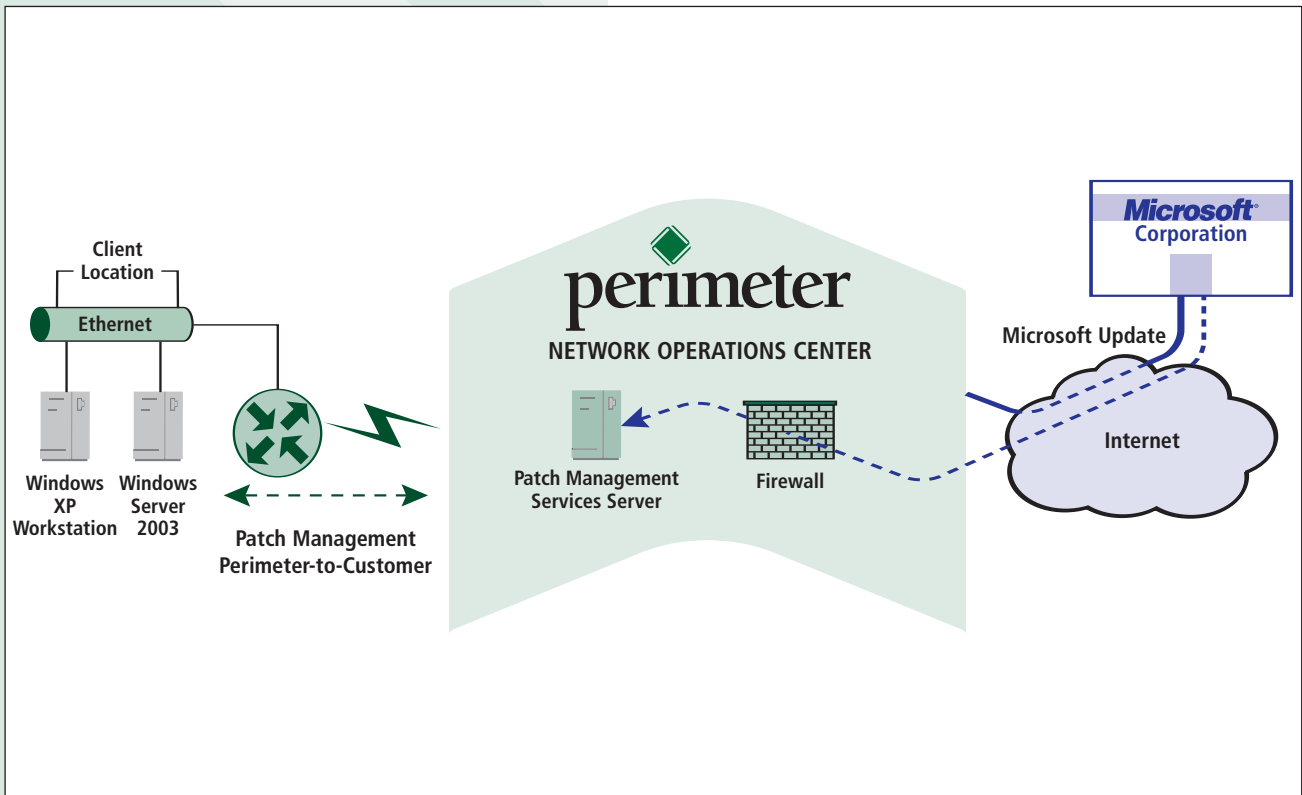
Problems Addressed

Perimeter's Patch Management Service assists organizations in updating Microsoft Windows systems to address the following problems:

- Security issues including internal and external exploits, worms, and trojans.

- Performance and other functional enhancements released by Microsoft to improve server operation.
- Bug reports addressed in periodic Service Pack releases as well as Hot Fixes released for critical problems.

Workflow Diagram



Technical Overview

Perimeter's service maintains a Patch Management Services server logically inside the Client's firewall to distribute patches to licensed Microsoft Windows XP and 2000 workstations and 2000 Server & Server 2003 systems in the Client's location. The customer's systems are registered as "downstream" to Perimeter's "upstream" patch management server, which communicates periodically with the Microsoft Update Web site to discover relevant patches and service pack updates. New patches are first tested and evaluated by Perimeter's engineering staff and then made available to the customer. The customer can first deploy them in a "sandbox" environment in their data center and then approve them for release to all or groups of servers and workstations in the Client's network infrastructure.

Technical Dependencies/Limitations

Windows 2000 Server/Server 2003	Service is limited to these supported servers.
Windows XP & 2000 workstations	Service is limited to these supported workstations
Licensing and registration.	Servers must have valid license documented by Microsoft, and servers must be registered as downstream to Perimeter's upstream server.

