



VULNERABILITY SCANNING

Internal, External, & PCI Scanning Services



PERIMETER E-SECURITY

- ▶ Providing a single, complete source for all your security needs since 1997
- ▶ Constant, around the clock monitoring with over 150 security personnel analyzing information 24/7/365
- ▶ Continuous third party assessments including an annual SAS 70 Type II and Cybertrust security audit
- ▶ Three redundant data centers and seven offices nationwide
- ▶ Servicing over 2,000 financial institutions in the United States

PERIMETER E-SECURITY VULNERABILITY SCANNING OVERVIEW

Vulnerability Assessments are critical in securing an organization's network. Most organizations perform these assessments annually or quarterly at the most. The difficulty with this level of frequency is that new network vulnerabilities are discovered daily. Since networks often change due to patching, new machine installations, and many other reasons, your vulnerability posture can change just as often.

Also, many regulatory bodies recognize the value of vulnerability assessments, including the PCI Council which published the PCI-DSS regulation. With so many reasons to scan, it makes sense to consolidate all these scans inside one easily accessible location that includes scan scheduling, report review, and remediation recommendations.

THE PERIMETER E-SECURITY VULNERABILITY SCANNING SERVICE

We have built our Vulnerability Scanning service to be as robust and thorough as possible. We have incorporated several best-of-breed scanning tools to ensure an extremely accurate assessment. Perimeter E-Security offers many scanning services to best fit your needs. Scanning services are divided into the following types:

- **External** - this vulnerability scan uses hardware outside of your network to scan the outside of your network for vulnerabilities. The same web-based portal is included for easy service management and reporting with this service as is included in the Internal service.
- **Internal** - this option allows you to turn any supporting hardware into an internal scanner that searches for vulnerabilities within your network. The same web-based portal is included for easy service management and reporting with this service as is included in the External service. As an additional option our scanner can be installed on a virtual machine.
- **PCI** - this external scan is customized to include the required Statement of Attestation and Self-Assessment Questionnaire. In addition to the management and reporting portal, this option provides additional reporting options including an overview of your PCI compliance status and more insight into any areas that may fall

Our managed solution provides the optimal solution for your scanning needs, bringing our scanning and security expertise to you. We will configure and schedule monthly scans for you. Our security experts will then review the outcome, discuss the findings and provide insight to solutions. Additionally consulting is also available to for your unique situation upon request.

Call Us Toll Free: 800.234.2175

[C](#) [W](#) [S](#) [D](#) Sales Sheet



VULNERABILITY SCANNING

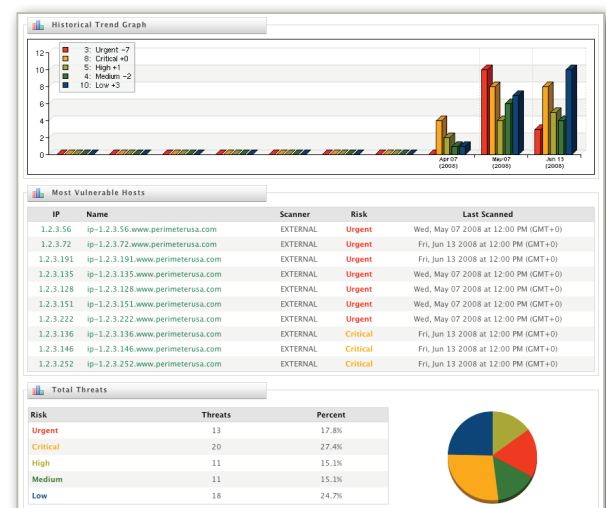
Internal, External, & PCI Scanning Services

THE BENEFITS OF PERIMETER'S VULNERABILITY SCANNING SERVICE

Key Features	Benefits
Meets Regulatory Requirements	As an Approved Scanning Vendor (ASV) , Our PCI scanning service is specifically designed to help you become PCI-DSS compliant. However, other regulatory bodies (including FINRA, SOX, GLBA, and HIPAA) all require scanning as well. Our scanning services can help in achieving compliance with these regulations
Simple, Single Interface	All reporting and service management is accessed through one portal with a simple, customizable interface
Self-Updating Threat Database	Every 12 hours the threat database is updated to reflect the latest exploitable vulnerabilities
Unlimited Scanning	The service offers unlimited scans, as frequently as you'd like (for the On Demand versions)
Experts Ready to Assist	Our security experts will plan and schedule the scans with you and will provide remediation guidance after the scan is complete to rid your network of the discovered vulnerabilities (for the Managed versions)
Flexible Scan Scheduling	"Restricted times" can be scheduled when scans will not run

PORTAL DASHBOARD

The dashboard shows executive level summaries for previous scans, historical trends, most vulnerable hosts, total threats, and several other scan reports. Depending on which services are subscribed to, up to 30 different dashboard widgets can be displayed. The screen is customizable to include or hide widgets.



Call Us Toll Free: 800.234.2175

C W S D Sales Sheet