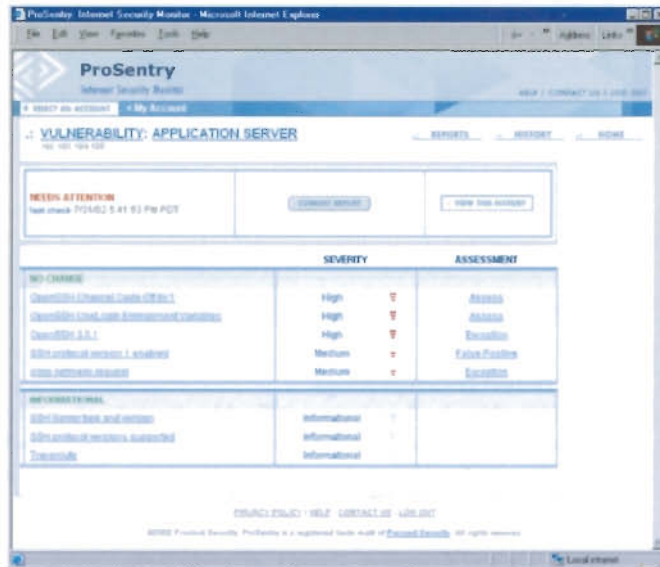


ProSentry™

INTERNET SECURITY MONITORING

Key features:

- Vulnerability Scan Monitoring
- Port Scan Monitoring
- Service Version Monitoring
- DNS Monitoring
- Page Change Monitoring
- Domain Registration Monitoring
- Event Management & Workflow
- E-Mail and Pager Alerts
- Network Reconnaissance Reports
- Vulnerability Reports
- Metrics Reports
- Trend Analysis Reports
- Inventory Reports
- Change History Reports



Get secure

ProSentry provides up-to-date vulnerability scan results automatically using the highly acclaimed open-source Nessus technology, and enhances this technology by adding assessment and collaboration features

ProSentry watches your network space using the leading open-source Nmap port scanner, alerting you to hosts and services that suddenly appear and disappear on your corporate network

All ProSentry modules, whether based on best-of-breed open-source technology or our own proprietary technology, are enhanced by ProSentry's robust change detection, event workflow, metrics and trend analysis, and historical reporting

ProSentry gives you visibility into your global Internet infrastructure, allowing you to clearly understand your risks, even for systems and networks within your organization that you do not directly manage

Consultants can offer the ProSentry service to their customers:

"The ability of our BDO Seidman Technology Alliance partners to offer a non-intrusive service like ProSentry gives them an extremely valuable offering that their customers really need. Using the ProSentry Internet Security Monitoring service, a customer can secure their Internet presence with a rapid, painless deployment. That's a win-win situation."

Dave Larson
National Business Line Leader
BDO Seidman Consulting

ProSentry™ 2.0 Internet Security Monitoring & Management

ProSentry™ 2.0 is an automated security management service that scans your Internet infrastructure for security vulnerabilities, and monitors both the integrity and availability of your Internet servers. ProSentry 2.0 performs network reconnaissance and evaluates targets as a hacker would, then continues to monitor your servers as you mitigate risks and respond to incidents. ProSentry 2.0 provides an organization with a comprehensive view of the security intelligence needed to secure and manage its systems using a non-invasive, subscription service.

Prevention is ideal, detection is a must

Your goal is to prevent hackers from gaining unauthorized access to your servers, defacing your web sites, and stealing your company's proprietary information. It's only a matter of time before a vulnerability in the software you use undermines your best efforts at prevention. ProSentry 2.0 embraces this reality and provides you with the information you need to both prevent and detect compromises.

How does it work?

ProSentry 2.0 consists of several modules that provide a baseline of security intelligence and change detection that is focused on securing your Internet perimeter and keeping it secure. One of the biggest values to you is the integration and automation of these modules, and the ability to correlate and store these comprehensive results in a single system. Using ProSentry 2.0, you can spend your time evaluating your business risk, reacting to current events, or analyzing historical trends rather than setting up and running numerous disparate tools that have no coherent integration or reporting.

Vulnerability Scan - Detect Vulnerabilities

ProSentry 2.0 vulnerability scans are based on the highly-acclaimed open-source Nessus technology. Updated constantly and widely supported by the information security community, there are currently over 1,015 tests that we run against your infrastructure. In addition, ProSentry 2.0 vulnerability management features help you better understand and manage your current security posture.

Port Scan - Detect Rogue Hosts, Services, Employees, Trojans, & Backdoors

The Port Scan Monitor detects the addition or removal of hosts from your network space, and the opening and closing of ports on each host. The Port Scan Monitor can help you detect trojans, backdoors, and employees that violate your appropriate use policies, and can help you proactively identify and secure other visible ports on your network.

Service Version - Detect Vulnerable Service Versions

The Service Version Monitor detects changes to FTP, HTTP, HTTPS, NAMED, POP3, SMTP, SSH, and Telnet on your servers. As new vulnerabilities are announced, your service version inventory will help you answer critical questions like, "What servers do I have running IIS, and what version are they running?"



Procinct
SECURITY

870 Market Street, Suite 1105
San Francisco, CA 94102
Phone 415.395.2946
Fax 415.296.8642
sales@prosentry.com
www.prosentry.com

The ProSentry 2.0 advantage

Streamlined security intelligence:

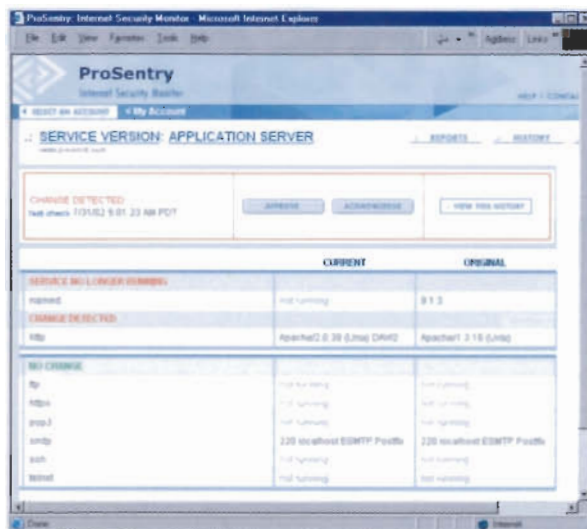
- Vulnerability scanning alone is useful, but does not monitor all the moving parts of your Internet presence
- Pairing vulnerability scanning and ongoing integrity monitoring provides both a proactive and reactive approach to your day-to-day security operations

No hassle:

- No need to download, build, and run various command line tools just to see your current security posture
- ProSentry 2.0 stays up-to-date and provides a clear picture of your Internet perimeter at all times

Stay focused:

- You concentrate on interpreting security intelligence, while ProSentry 2.0 handles the operational monitoring details
- No need to waste time correlating and integrating output from multiple tools and products, ProSentry 2.0 does it all for you and keeps you current



Stay secure

ProSentry will alert you to services that suddenly appear or disappear, hosts that show up unexpectedly on your network, new vulnerabilities that have been found, and changes to your Web sites

ProSentry maintains your historical information, allowing you to quickly and easily report on history of changes, metrics, and trend analysis

Robust workflow enables any number of people to effectively collaborate and respond to security issues

User scheduling ensures that the right people are promptly notified of integrity problems and suspicious changes

DNS - Detect DNS Hijackings

A DNS hijacking is when incorrect IP addresses get entered into the DNS database, thereby pointing traffic destined for one domain to any domain a hacker chooses. Many high profile companies have all fallen victim to DNS hijackings. The DNS Monitor will immediately notify you of any changes to DNS resolution for your corporate web and mail servers.

Page Change / Keyword - Detect Web Site Defacements

The speed at which a defacement is detected directly affects your incident response time, and your response time will often determine whether your company makes national headlines. The Page Change & Keyword monitors will look for expected content. If a hacker defaces your web site or an employee posts inappropriate content, you will be promptly alerted to the problem.

"We chose ProSentry because it gives us the baseline of security information we need to keep our Internet servers secure. As a startup gaining momentum and mind share in the market, the last thing Ritepage can afford is to undermine early adopter confidence with a security breach that we could have prevented."

Frank Galdes, CEO Ritepage, Inc.



THE CENTER FOR
INTERNET SECURITY
CHARTER MEMBER

Procinct Security Professional Services

Procinct Security provides a wide range of security consulting services:

Network Vulnerability Testing
Penetration Testing
Risk Assessment
System Hardening

Incident Response
Web Application Security Review
Independent Verification & Validation
Policies & Procedures Development

Proven success with Procinct Security

We automate paying attention™. Procinct Security Corporation is dedicated to developing cutting edge information security solutions that help clients across all industries secure their Internet infrastructure. Procinct Security, provider of the ProSentry™ Internet Security Monitoring service, is comprised of senior software architects and trustworthy security professionals who hold sensitive security clearances and CISSP and SANS GIAC security certifications. Procinct Security also provides a wide range of security consulting services.

Procinct Security is a charter member of the Center for Internet Security and an independent member of the BDO Seidman Alliance. For more information email info@procinct.com or sales@procinct.com.

© 2002 Procinct Security Corporation. Procinct, Procinct Security, the Procinct Security logo and ProSentry are trademarks or registered trademarks of Procinct Security Corporation in the United States and other countries. We Automate Paying Attention is a registered service mark of Procinct Security Corporation. All other product and company names mentioned herein are the property of their respective owners.