

SUMMARY:

The **ThreatGuard™ Vulnerability Management System** is a continuous host discovery and vulnerability detection solution. The appliance can be placed internal or external to an organization's network, and continuously scans the network for new security risks and vulnerabilities. **ThreatGuard** includes functions vital to a comprehensive security scan, such as continuous network mapping, comprehensive port scanning, operating system detection, and vulnerability scanning. When new machines appear on the network, they are automatically detected and scanned for vulnerabilities that could allow unauthorized intruders access to private information. **ThreatGuard's** team of security engineers constantly monitors government, vendor, and security resources to identify new vulnerabilities. Using our rapid deployment process, we quickly create tools to detect these vulnerabilities and remotely install them on all **ThreatGuard** appliances. **ThreatGuard** appliances automatically download system software updates from the **ThreatGuard** central database without requiring administrative intervention. **ThreatGuard** appliances can be standalone or networked together to form a **ThreatShield™** hierarchy, providing centralized management and security posture reporting. Managers can view vulnerabilities through a variety of reports, including by severity level, and are also able to prioritize and assign "fix-it" tasks to employees. **ThreatGuard** comes in versions optimized for Internet-exposed networks, internal networks, and mobile uses.

The **ThreatGuard™ Vulnerability Management System**:

A Continuous Vulnerability Detection System

Most vulnerability scanners focus on providing a point-in-time view of your network's security posture. The Anti-Virus world has proven the once-and-done approach to be naïve and dangerous. A decade ago, the IT professional could almost count on a several-month window of opportunity to fix a security issue before widespread attacks were launched. Today, this window has been as small as one day. Running a vulnerability scan once a quarter, once a month, or even once a week no longer provides adequate security awareness. Not only does the **ThreatGuard** keep a vigilant eye on your network assets, it also notifies you in real time as soon as a new vulnerability is introduced. This introduction may be caused by system upgrades, seemingly innocuous system maintenance, or malicious actions. Even when a new vulnerability is reported to the general public, the scanner will download a new test and evaluate all relevant systems automatically. **ThreatGuard™ minimizes your security awareness gap while your staff focuses on other tasks.**

A Vulnerability Management System

When the vulnerability scanner market was born, network security issues were potentially few enough to track by enumeration. But today, with over 65 new vulnerabilities emerging on a weekly basis, an organization needs a way to manage the remediation process. The **ThreatGuard** allows your administrator to automatically assign vulnerabilities to key personnel the moment they are discovered. The system sets due dates per the administrator's designations and notifies secondary and tertiary support staff or supervisors if security issues are not addressed in a timely manner. Also, it is smart enough to know whether or not a vulnerability has been fixed, overriding the operator's report when necessary and recording fixes even when the technician forgets. **The ThreatGuard provides point-and-click insight to your remediation process that would otherwise require in depth personnel interrogations to surface.**

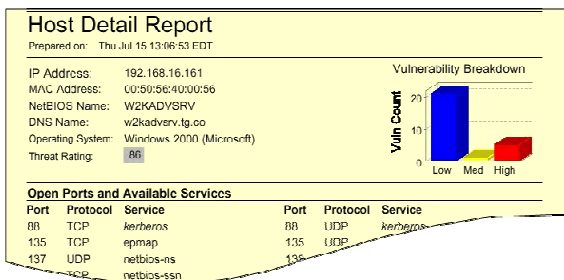
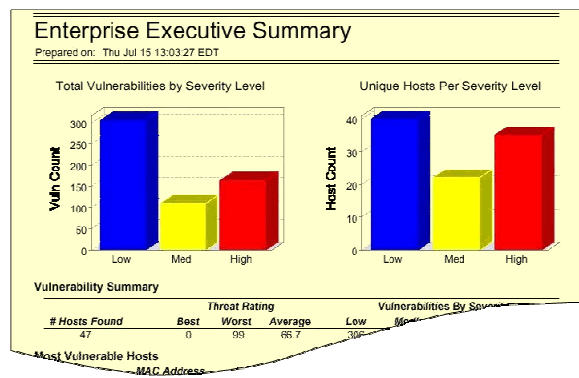
An Enterprise Security Awareness Center

Few scanner products have recognized the obvious truth that a chain is only as strong as the weakest link. Performing periodic, department-level security scans invites a false sense of security. At a very minimum, a small organization needs to consider two perspectives in concert: internal and external. As an organization grows to a multi-departmental entity, the number of security perspectives increases as well. The multi-site organization has an even greater need for multi-faceted security perspectives, and a greater challenge to achieve it.

Multiple **ThreatGuard** appliances can be tied together with a designated “Master” acting as a central controller over the others. This allows centralized security posture reporting across a large enterprise while still keeping sub-network administrators focused on the problems in their respective areas. **The ThreatGuard enterprise deployment provides instant access to security posture reports correlated and segmented across all subdivisions of the organization.**

Security Made Simple

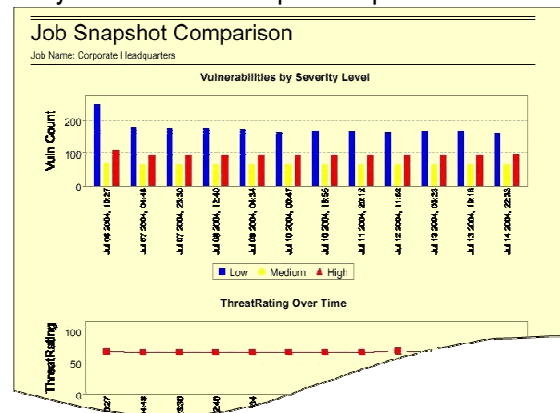
Clients and evaluators have repeatedly commented on how easy the **ThreatGuard** is to setup, integrate, and start using effectively. Major competitors often require formal training or hours of reading documentation to get started. **ThreatGuard** configuration is very simple, and the gathered data is organized in a sensible and intuitive manner. This allows a user with average networking skills to use the system out of the box.



Not only is **ThreatGuard** easy to setup and run, but it's also easy to understand. The system generates **real-time reports on demand**, from high level Executive Summaries to detailed port-level and vulnerability-level reports. In addition to at-a-glance graphics to depict security posture, the Executive Summaries provide aggregates and call-outs of the most vulnerable hosts and the most common, critical vulnerabilities.

The technicians' reports were designed to 'dumb down' security. The GUI and reports explain each security issue in detail, and provide easy-to-follow steps to mitigate or eliminate the risk. Also, a complete listing of all open ports provides insight into possible Trojan Horses and Back Doors on typically overlooked high-numbered ports. By design, **ThreatGuard becomes your security expert**, allowing your IT staff to remain sharp in other areas.

ThreatGuard will also track security posture over time. Even the most diligent organizations can see their security posture decline as increasingly more vulnerabilities threaten their assets. The Snapshot



Comparison Reports show the number of new and fixed vulnerabilities in each snapshot. **ThreatGuard provides tangible evidence to supervisors, executives, and auditors that your staff is addressing security.**

The ThreatGuard Vulnerability Management System keeps security awareness at your fingertips. Good awareness leads to good health, and being aware of details in every nook and cranny of your enterprise gives your administrator the insight needed to run a tight ship. Whether it be an auditor looking to evaluate your security practices, an executive looking to assess resources, a supervisor keeping tabs on technicians, or technicians getting the work done, **ThreatGuard** gives you the tools you need to chart, execute, and track your progress towards a secure enterprise.

Industry Leader in DoD-style Authenticated Scanning

OVAL is an international, information security community baseline standard for how to check for the presence of vulnerability and configuration issues on computer systems. The tests are standardized, machine-readable XML Vulnerability Definitions which are made freely available for the general public to download, use, reference, and implement. The OVAL project is funded by the US-CERT at the U.S. Department of Homeland Security and has been recognized by the U.S. Department of Defense as a distinct advantage in vulnerability management.

Among the first products to declare compatibility, **ThreatGuard** has integrated OVAL at an unprecedented level. The continuous detection process downloads and processes new OVAL definitions as they are made available. Fielded appliances evaluate all enterprise assets against the latest OVAL definitions, often within a day of patch release. In this manner, **ThreatGuard creates a large window of opportunity to patch and confirm systems before resultant worms attack the Internet.**

In November 2005, **ThreatGuard** earned the OVAL compatibility award and became the first product to pass MITRE's live evaluation for consuming OVAL definitions and producing OVAL results. The vulnerability detection system demonstrated its ability to apply OVAL's definition logic to various operating systems and produce results documents suitable for various patch management systems to digest. This event marked a milestone for the DHS-funded project and clearly placed **ThreatGuard** as a leader in this security space.

PARTNERS & REFERENCES:

The MITRE Corporation

Bob Martin
202 Burlington Road
Bedford, MA 01730-1420
(781) 271-3001
ramartin@mitre.org

Windber Cancer Research Center

Windber, PA
Holly Rigby, President of Professional
Services
(814) 467-3627
hrigby@conemaugh.org

Secure Orbit Labs

David Kuykendahl
<http://www.secureorbit.net/>
(210) 200-8550
David.Kuykendall@SecureOrbit.net

