

www.securecomputing.com

Secure Computing® has been solving the most difficult network and application security challenges for over 20 years, and is uniquely qualified to be the global security solutions provider to organizations of all sizes.

“RADAR is one of the few offerings in the world that trends everything. It truly is a great product.”

– Kyle Hussey, Grant County Public Utility District

Benefits

- **Real-time monitoring provides around-the-clock visibility into fraud and malicious usage of email**
- **Configurable alerts ensure real-time response to any suspicious or fraudulent email activity that may impact your reputation**
- **Comprehensive reporting tools provide a wealth of forensic information for use in stopping phishing attacks and malicious email activity**
- **TrustedSource behavior-based reputation system provides the most detailed sender IP information available**
- **Eliminates the threat of zombie PCs sending mail out of your network by identifying unusual email sending activity**

© October 2006 Secure Computing Corporation. All Rights Reserved.
 CI-Radar360-PO-October, Besis, enterprise strong, IronMail, MobilePass, PremierAccess, SafeWord, Secure Computing, SecureOS, SecureSupport, Sidewinder GZ, SmartFilter, Softoken, Strikeback, Type Enforcement, CyberGuard, and Webwasher are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. Anti-Virus Multi-Scan, Anti-Virus PreScan, Application Defenses, Compliance, Dynamic Quarantine, Edge, Encryption, GZ Enterprise Manager, Global Command Center, IronMail, IronMail Live Reporting, Message Profiler, MethodMix, On-Box, Outbreak Defender, PowerIt-Ort, Radar, RemoteAccess, Secure Encryption, SecureWire, SmartReporter, SnapGear, SpamProfiler, Threat Response, Total Stream Protection, TrustedSource, TrustedSource Portal, and ZAP are trademarks of Secure Computing Corporation. All other trademarks used herein belong to their respective owners.

Secure Computing RADAR-360

Real-time Anti-fraud Data and Resources

Secure Computing’s RADAR-360 provides enterprise risk management experts with timely, relevant, domain-specific information on fraudulent use of that domain in phishing attacks and other malicious email activities. Understanding this information is critical, as phishing attacks and other malicious activities carried out using your company name cost the company significantly in time, money, and most importantly, reputation.

- **Unparalleled real-time visibility:** With more than 7000 sensors around the globe, RADAR alerts you when phishing attacks start and when anomalous sending behavior occurs from your network.
- **Most accurate reputation scores:** Secure Computing gathers and correlates all known information about email senders and the type of email they send into the TrustedSource behavior-based sender reputation system. TrustedSource provides unmatched depth and coverage of all email sending IPs from enterprises, educational institutions and government organizations.
- **Global intelligence:** RADAR-360 correlates and aggregates multiple parameters of each email seen by Secure Computing sensors, including correct DNS resolution, returned email acceptance, spoofed IP identification, email content, embedded URLs, and other parameters.
- **Robust reporting:** The Message Summary view in RADAR-360 provides significant information about messages pertaining to a specific organization. This data includes the number of fraudulent emails using organization’s name seen by TrustedSource. A comparison of a specific organization’s fraud presence on the internet compared to other organizations is also displayed.
- **Virtual vaccine against zombies:** RADAR-360 monitors all IP addresses that are sending email from defined domains and IP address net blocks, allowing organizations to pinpoint unusual sending activity from their network that often indicates zombie machines.
- **Your second set of eyes:** RADAR-360 monitors phishing attacks and email sending patterns from your organization in real time. Flexible alerts provide instant notifications of fraudulent or suspicious activity pertaining to your organization.
- **Automatic logging and archiving:** RADAR-360 archives all activity pertaining to fraud and email monitoring for quick access through dashboard displays and drill-down screens. Trending information is supplied to allow investigators to make quick, accurate assessments of the information and take appropriate and timely action to stop fraud and suspicious sending activities.
- **Investigative assistance:** RADAR-360 supplies a wealth of forensic information designed to assist fraud investigators in identifying the source of phishing schemes that take advantage of their organization.
- **Intuitive Web-based management:** RADAR-360 is managed using a standard Internet browser, providing an organization with easy access to the intelligence gathered.

The RADAR-360 dashboard provides corporate fraud investigators with straightforward information pertaining to fraudulent activity carried out using the company's identity, including the number of phishing messages sent as well as the number of hosts imitating the company's website. Data is presented in a familiar and easy-to-navigate tabbed interface.

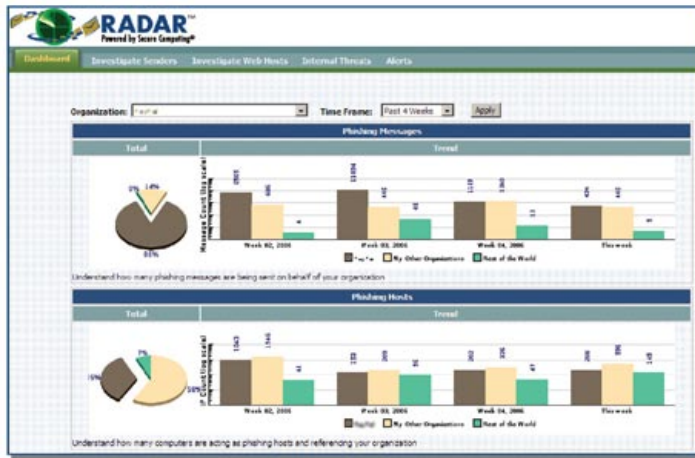


Figure 1: Secure Computing RADAR dashboard

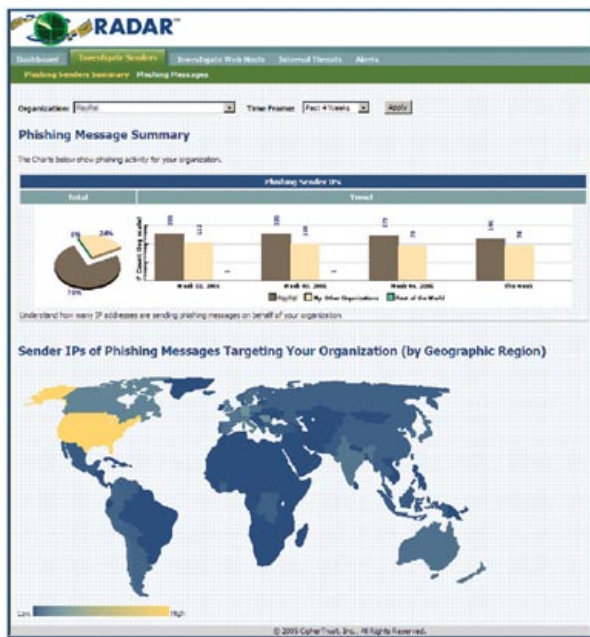


Figure 2: Secure Computing RADAR phishing message summary

The investigative areas of RADAR-360 were designed specifically for fraud investigators. The portal's tables and views are linked for ease of reference, and most views have a search capability that can access the entire database and provide sorted search data pertaining to the enterprise.

Users can easily navigate from the message summary (as shown in figure 2) and Web host or sender tables all the way down to the original messages. Using the data provided by RADAR, fraud investigators can ascertain when certain hosts are causing large problems, and can then provide that information to law enforcement to assist in shutting down the fraudulent sites.

SECURE
COMPUTING

www.securecomputing.com



For more information

Contact your local reseller, or Secure Computing at:
1-800-379-4944 (inside U.S.)
1-408-979-6100 (worldwide)
sales@securecomputing.com
www.securecomputing.com

Secure Computing Corporation

Corporate Headquarters

4810 Harwood Road
 San Jose, CA 95124 USA
 Tel: +1.800.379.4944
 Tel: +1.408.979.6100
 Fax: +1.408.979.6501

European Headquarters

No 1 The Arena
 Downshire Way
 Bracknell
 Berkshire, RG12 1PU UK
 Tel: +44.0.870.460.4766
 Fax: +44.0.870.460.4767

Asia/Pacific Headquarters

Hong Kong
 1604-5 MLC Tower
 248 Queen's Road East
 Wan Chai Hong Kong
 Tel: +852.2520.2422
 Fax: +852.2587.1333

Japan Headquarters

Shinjuku Mitsui Bldg. 2, 7F
 Nishi-Shinjuku 3-2-11
 Shinjuku-ku, Tokyo, 160-0023
 Japan
 Tel: +81.3.5339.6310
 Fax: +81.3.4496.4537

For a complete listing of all our global offices, see www.securecomputing.com/goto/globaloffices