ENIRA™ technologies

respond.
command.
control.

data sheet

ENIRA INSP: Network Response Management

ENIRA Quick Facts:

- *Instantly quarantine any node, anywhere across your network.*
- *No clients. No agents. Does not sit in-line.*
- *Only listens on SSL (tcp/443)*
- *No proprietary ports/ protocols*
- *Sensitive data is encrypted with AES 256*
- *Hardened appliance kernel*
- *Supports enterprise authentication systems*
- *Leverages your existing network technologies.*
- *Multi-vendor/technology support.*
- *Quick and easy deployment and management.*

There is no shortage of Prevention and Detection technology (IDS, IPS, SIMS, Antivirus). What is missing is technology that supports your Incident Response Plan (see separate ENIRA White Paper).

Incident Response requires a multi dimensional approach that addresses several challenges:

- Corporate Process
- Company Communication
- Technology
- Compliance
- Audit

While today's manual process could meet all of these challenges, but in reality it is not a practical approach. Your top priority in case of a compromise is driven by the need for fast response.

ENIRA has taken all requirements and put them into a technology solution, answering every single one of the above challenges. Regardless if you have one incident or many, ENIRA's response is only seconds away.

Intelligent Network Services Platform

Answering the technical challenge is the ENIRA INSP which builds and maintains a detailed understanding of your network's topology by communicating directly with your network infrastructure devices (routers, switches, firewalls, wireless access points, and VPN systems). ENIRA communicates natively (like an engineer would) using telnet, SSH, or HTTP(S).

By taking this approach, ENIRA NRM does NOT require clients or agents to be deployed anywhere in your network. Therefore ENIRA can be deployed and operated without requiring ANY changes to your existing network infrastructure and desktop environment.

Through a detailed understanding of your network topology, ENIRA's advanced, patent-pending algorithms can instantly identify the exact location of any node (wireless, wired, or VPN), anywhere across your network, and implement specific, policy based quarantine actions. These actions include disabling the node's switch port, implementing a filter on the node's traffic, or moving the node to a virtual quarantine network. Dynamic access control list (ACL) modifications to implement rules for IP ports and protocols are also available.

Enterprise Wide User Rights Management

Due to corporate processes and various job functions, responsibilities are distributed within your corporation. Several layers of support teams, separated between security operation and network management, exist and may have location-dependent rights. The ENIRA user account control takes all of this under consideration. You easily define task

groups within each module, controlling and restricting access rights in accordance to job tasks. Every member of your team can now individually be associated with one or more task groups, allowing him to use ENIRA within his job description.

This granular detail of user rights helps you to be more effective and maintain control. For example, Level 1 support might only be allowed to suggest response actions, configuration or policy changes, but may not be allowed to execute them – in this case users would have account settings that require authorization from higher levels of support teams. Some users might only be allowed to work in certain parts of the network while others have total network control (detailed user rights settings are described fully in each datasheet for the individual modules).

Disaster Recover and Threat Level support

ENIRA's powerful Disaster and Threat Level support allows you to store alternative network configurations and policies under an unlimited number of user definable labels. Alternative scenarios are only a mouse click away, when needed. A disaster recovery exercise is reduced to a few seconds versus days. Adapting to new Threats is basically instantaneous.

Details of Quarantining

ENIRA NRM provides several policy driven quarantine options. All of them can be initiated by simply providing ENIRA NRM an IP address, MAC address, or hostname. ENIRA NRM will first use its advanced topology logic to identify the node's exact location, then based on your policy implement one of following quarantine functions:

Disabling Switch Ports
ENIRA NRM can instantly identify the exact switch port any node is plugged into and disable the switch port, completely isolating the node from the network. Advanced intelligence is used to verify that the node is the only system plugged into the port and that no other nodes will be impacted by the action. If ENIRA NRM determines that there is more then one node downstream from the port, it will not disable the port and instead implement a MAC filter (examples include unmanageable hubs, unknown switches, and VOIP).

Implementing MAC Filters
ENIRA NRM can perform MAC filters (sometimes called MAC ACLs) on switch ports causing the switch to stop forwarding traffic from a specific node, while not impacting traffic from any other nodes downstream. This is also the action ENIRA NRM takes on a wireless access point (WAP), if the node it is seeking to quarantine is wireless. In this case, the filter is implemented on the WAP itself, disabling access for the specific node while not impacting other wireless nodes.

Quarantine VLAN
This function enables remote remediation by moving the node to a Quarantine VLAN. A Quarantine VLAN is a virtual network setup to allow communications to resources such as your HelpDesk, the Internet, and a patch server, but deny communication to the "general population". This is a powerful feature that enables you to quarantine nodes from infecting the network while being able to clean, patch, and update them remotely.

Remote Users
ENIRA NRM can work with VPN devices and their authentication systems (Active Directory, LDAP, etc) to quickly quarantine remote users. If ENIRA NRS determines that a node is a remote user, it can identify the exact user session and login ID, kill the active session, disable the user's login account to prevent further access, and notify you with the details. Simply clicking the Remove Quarantine button re-enables the user's account and allows normal remote operations.

.

IP Traffic Blocks
ENIRA NRS also provides you the ability to quickly dictate how IP ports and protocols are routed across your network. By simply defining a rule, ENIRA NRS determines, based on your topology, where access control lists (ACL) need to be placed to deny specific types of traffic. This function can be used to block vulnerable traffic during the patching process or granularly deny specific traffic to/from specific network nodes (Example: Deny FTP access to Websrvr01).

Quarantine Enterprise Accounts
Quarantine Enterprise goes beyond the network infrastructure and allows to disable individual user accounts. ENIRA provides you with the most robust, yet easy to use, interface to perform the quarantining activities. You can search by different categories or receive a list of all network users.

Leverage Existing Investment

ENIRA builds a bridge between Network Security and Network Operations. Several technical features (Open Integration Module, Syslog Interface, or Soap/XML) allow you to integrate into existing or upcoming security technologies. These devices become users of ENIRA and you control their reach with ENIRA's detailed user rights. Quarantining nodes and traffic is as easy as the reversal of these actions. **Deny** and **Quarantine** rules help you to either prevent accidental shutdown or implement predetermined quarantining action.

ENIRA also supports quick and easy integration with Trouble Ticket Systems, as well as, Network Management systems.

ENIRA provides complete multi-vendor support, enabling you to respond across your entire network regardless of which vendor's network devices you have deployed. Any manageable network device can be supported from old manageable repeaters to today's most advanced routers and switches.

Reporting and Compliance

ENIRA's intelligent and precise actions are completely *self-documenting,* eliminating the pain of manually capturing and consolidating incident response information. ENIRA's robust web-based reporting system makes all of the relevant details transparent – in easy to understand, customizable reports convenient for Security Managers – to ensure the organization is compliant with Sarbanes-Oxley, HIPPA, and FERC requirements.

Manual or Automation

Quarantines can be performed manually (person using the web interface) or completely automated through integration with IDS, IPS, SIMS, Network Management systems, and the like. This integration is easy and open using either Web Services integration or through the use of the ENIRA NRS Integration Plug-in which enables simple integration without any programming.

A balance of automated and manual quarantines can easily be achieved by identifying trusted vs. un-trusted (potential false positive) alarms from your detection systems. Trusted alarms can be automatically quarantined with a detailed notification sent to you, while un-trusted alarms can generate an authorization request stating "Detection system xxx has seen xyz, would you like us to quarantine it?".

Simplified Management

ENIRA NRS is packaged as an appliance, but without the normal draw backs. ENIRA NRS does NOT need to sit in-line (it can be located anywhere in your network), does not require span ports, and only one single appliance is required.

ENIRA NRS is delivered as an appliance for two simple reasons: Management and Security.

Management facts:
- Simple, web-based interface
- No consoles needed. No command line to learn.
- Completely self-contained system
- Does not require dedicated sys admin

Security facts:
- Only listens on SSL (tcp/443)
- No proprietary ports/protocols
- Sensitive data is encrypted with AES 256
- Hardened appliance kernel
- Supports enterprise authentication systems

ENIRA: Technical Specifications

About ENIRA Technologies:

Founded in 2002, **ENIRA Technologies**' mission is to eliminate the challenges that many Network Organizations face, from managing day-to- day operations to reacting to mission critical events in your network.

ENIRA Technologies was founded by network engineers who were driven to break through the barriers of lengthy manual and error prone processes. They invented and implemented "Expert Technology" to fully automate these processes and interactions within their network.

ENIRA has eliminated the manual and frustrating process that customers had to accept in the past. ENIRA's multi-vendor, multi-technology foundation focuses on improving the effectiveness and efficiency of enterprise network security and operations, giving its customers confidence in their ability to respond and stay in command and control.

Available ENIRA Literature:

- ENIRA Intelligent Network Service Platform Overview
- ENIRA NRM Quick Facts
- ENIRA NCM Quick Facts
- ENIRA NRM Datasheet
- ENIRA NCM Datasheet
- ENIRA NPM Datasheet
- Distributed ENIRA Datasheet
- White Paper
- FAQ
- Customer Case Studies

System Details

- Appliance architecture with Intel P4 3.6 GHz, 2 GB memory, 120 GB hard drive
- 2 Ethernet (10/100/1000) interfaces
- Hardened appliance kernel
- 256-bit encryption
- Network communication via Telnet and SSH
- External authentication systems supported
- Optional distributed architecture
- Accessible via HTTPS secure link
- Update and management via web interface
- Safeguard against intrusion
- Configurable L2/L3 infrastructure polling
- Central timing via NTP server

Detailed User Account Administration

- Admin Rights
  - Create/Change Users
  - Create/Change devices
  - Display L3/L2 device configuration
  - Authorize Blocks
- Reporting Rights
  - Blocking Queue
  - Current Blocks
  - Layer 2 Blocks
  - No Expiring Blocks
  - Country Reports
  - Audit Reports
  - Custom Reports
- Blocking Rights
  - By Node
  - By Subnet
  - Quarantine Type (Full/Fallback/ Basic)
  - IP Port Blocking (Any/Specific)
  - IP Protocol Blocking (Any/Specific)
  - Target Group Blocking
  - Mac Filter
  - Action Rights (Add/Remove/Both/ None)
- Action Range
  - Internal L2
  - Internal L3
  - External
  - Allowed CIDR Ranges

Supported Devices

- Routers
  - 3Com, Alcatel, Avaya, CISCO, Dell, Juniper, Enterasys, Extreme, Foundry, HP, Nortel
- Switches
  - 3Com, Alcatel, Avaya, Bay, Cabletron (24E, EMM-E6), CISCO, CISCO, Dell, Enterasys, Extreme, Foundry, HP, Nortel , ODS, SMC
- Firewalls
  - Checkpoint, CISCO, Cyberguard, Juniper/Netscreen, Sidewinder
- Wireless
  - CISCO, Enterasys
- VPN
  - CISCO, Nortel

Action Rules

- Deny Rules (User, CIDR, Mac Address, Hostname)
- Quarantine Rules (User, CIDR, Mac Address, Hostname) with Action Range (Disable Port, Filter MAC, Move VLAN, Require Authorization)

Action Activities

- Quarantine Node
- Quarantine Subnet
- Block IP Traffic
- Universal Filter
- Expiring or Non Expiring blocks (Single value,
- External/Internal Value, configurable table of values, individual user input values)
- Investigate (MAC or IP node location, Show Map, Lookup Job, Lookup trouble ticket)
- Show Authorization Queue

Reports

- Blocking Queue
- Auditing
- Country Reports
- Current Blocks
- Custom Reports

ENIRA Technologies, 11921 Freedom Drive, Two Fountain Square, Suite 550, Reston, VA 20190
www.enira.com (888) 277-7638 sales@enira.com