ENIRA technologies

respond.
command.
control.

data sheet

ENIRA Network Response System

By leveraging your network infrastructure, the ENIRA Network Response Systems™ (NRS) provides your organization the command and control to instantly quarantine any node, anywhere across your network, down to the specific point where the node is connected (switch, wireless access point, VPN, etc.) This capability enables you to move beyond complex manual processes during cybersecurity incidents.

ENIRA Quick Facts:

- *Instantly quarantine any node, anywhere across you network.*
- *No clients. No agents. Does not sit in-line.*
- *Leverages your existing network technologies.*
- *Multi-vendor/technology support.*
- *Quick and easy deployment and management.*

Quarantine Functions

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

Disabling Switch Ports

ENIRA NRS 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 NRS 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 NRS 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 NRS 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 NRS 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.

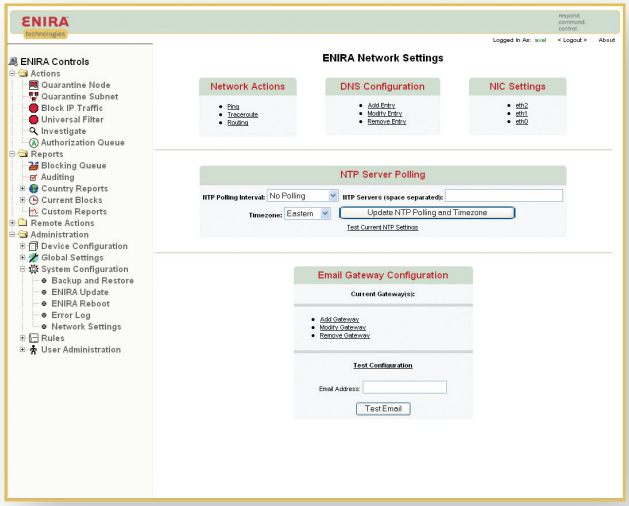
IP Traffic Blocks

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).

Leveraging Your Network

ENIRA NRS 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 NRS does NOT require clients or agents to be deployed anywhere in your network. This enables the ENIRA NRS to be deployed and operate without requiring ANY changes to your existing network infrastructure and desktop environment.
ENIRA NRS 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.



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

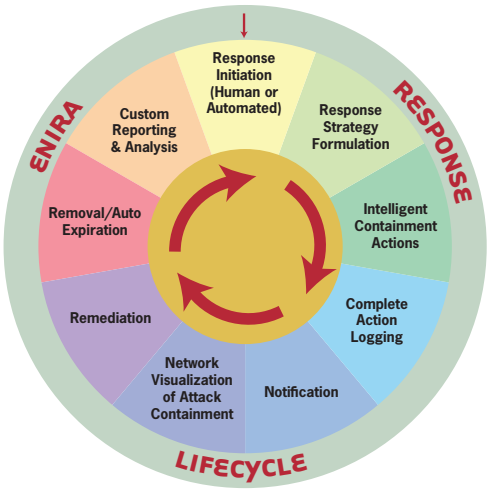
Fits Into Any Architecture

ENIRA NRS is designed to fit into any existing and future network or security architecture while not overlapping technologies that have already been invested in.
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 xxx, would you like us to quarantine it?".

Complete Response Process

ENIRA NRS provides a complete Response Life Cycle, not just a knee-jerk reaction.



It enables you to completely automate your response plan. Now the click of a single button can encompass everything from response strategy formulation, node quarantine, notification, and trouble ticket generation through reporting and analysis.

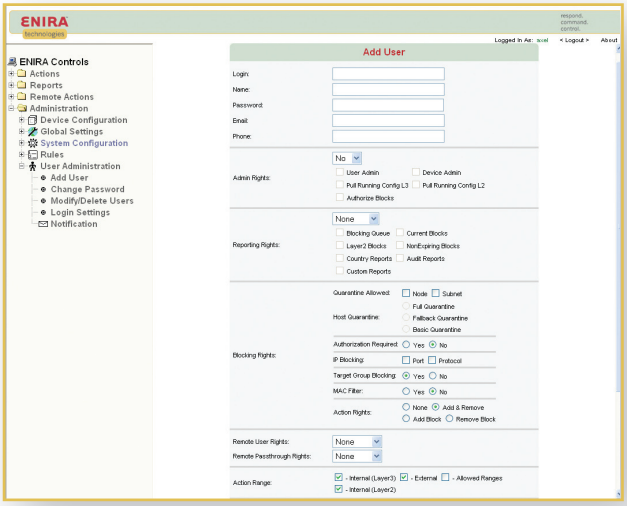
Process facts:

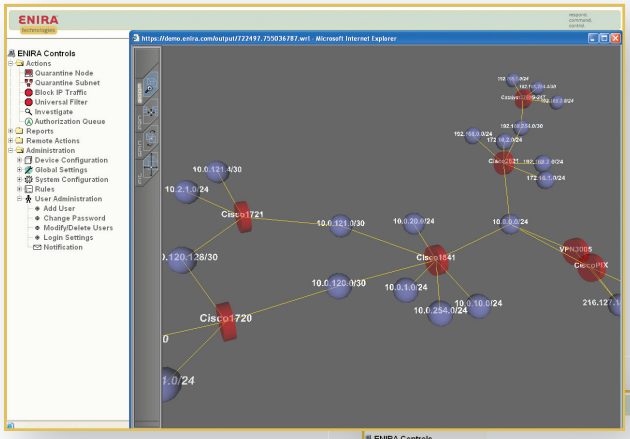
- Notification—email, syslog, or leverages third party notification systems
- Reporting—embedded, web-based, "out of the box", or can export data for enterprise reporting systems
- Trouble Ticket Generation—customizable email notifications enable easy trouble ticket generation with any modern day trouble ticket system

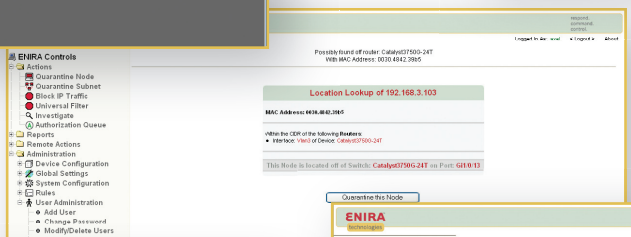
Granular User Roles

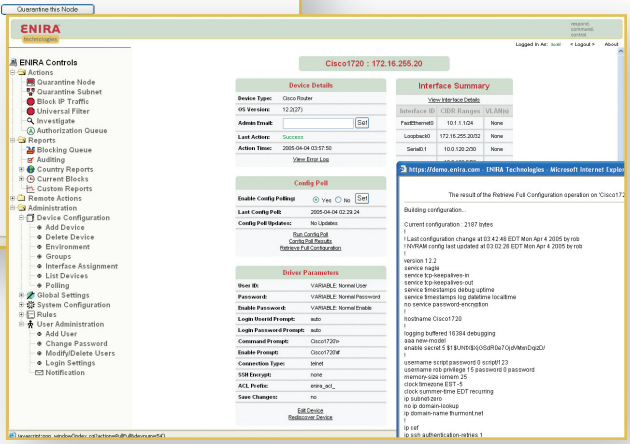
ENIRA NRS supports granular user roles enabling you to easily distribute management functions as well as control the details of Who can respond (users), Where in the network they can respond (subnets, nodes, etc), When they can respond (time), and How they can respond (which quarantine functions).

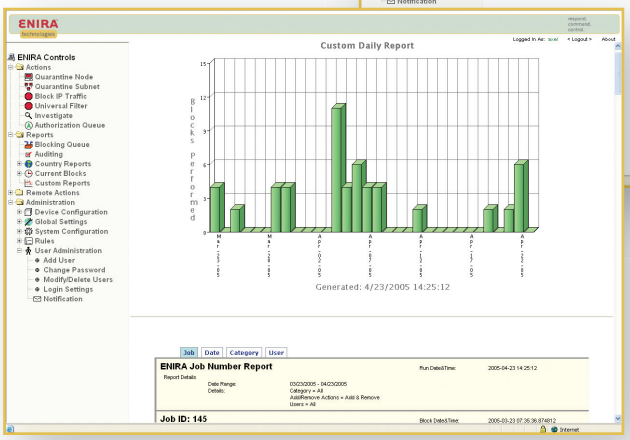
This functionality enables organizations to leverage additional staff in the response process -> increasing response time and freeing us engineers to engineer.











ENIRA Technical Specifications

About ENIRA Technologies:

Founded in 2002, ENIRA Technologies delivers sophisticated technology that empowers network operations to stay in command and control of an increasingly complex network infrastructure.

The ENIRA product line allows them to respond to the challenges posed by cyber-security and day-by-day operations. ENIRA automates tedious and time consuming tasks, while leveraging an organization's existing investments. 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 Product Overview
- ENIRA Technical Specifications
- Distributed ENIRA Datasheet
- White Paper
- FAQ
- Customer Success Story

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, 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