# WHAT IS IT?

## 1. What is ENIRA?

The ENIRA system provides an immediate response to control cyber-security breaches by automating tedious and time-consuming counter measures. ENIRA captures network configuration intelligence; and creates a topology that allows network operators to command and quarantine - any and all - infected nodes *instantly*.

By leveraging existing detection and prevention technologies, and supporting multi-vendor technologies, ENIRA gives network operators a real-time, intuitive understanding of the network's status – and the power to respond, command and control – without endangering business systems or mission-critical traffic flows.

## 2. What is ENIRA similar to?

ENIRA is unique technology, unlike anything on the market today. The ENIRA system automates tedious, error-prone, and time-intensive manual processes for network operators during a cyber attack.

## 3. What is the capacity of one ENIRA system?

ENIRA perfectly scales. Whether you have 2.500 nodes in your network or 250.000 nodes. One ENIRA appliance can handle it. We have measured the performance against a network containing 50.000 subnets and we find the correct location in 7/10 of a second.

## 4. Why and how is ENIRA an appliance?

ENIRA is a system technology that is embedded into a specialized Linux server. We do not require any installation of software when installing the system. Just configure the IP address for ENIRA and you are ready to enter the information for your network infrastructure.

## 5. What Operating System does ENIRA run on?

A Linux version with special modifications. All data inside ENIRA is 256 bit encrypted.

## 6. How is ENIRA different from an IPS?

IPS stands for Intrusion Prevention System. IPS' are devices that are a combination of a Firewall and IDS (Intrusion Detection System). They check for known signature and traffic behavior in order to prevent intrusions from the outside. However, unknown, new forms of attack will easily trick these devices and in addition many attacks happen from the inside out – already behind the firewall/IPS.

## 7. If I have Prevention and Detection Technology deployed – do I need Response Technology?

While all of these systems are essential for your overall cyber security life cycle – none of the products available today address the process of *shutting down* an infected station automatically and instantly.

Companies need therefore to mitigate the impact of attacks with quick response times. Currently you are left with the manual process, i.e. using cumbersome CLI interfaces. In addition you require a well trained engineer which uses the CLI's and their command structure to identify the location of the station and shut it down. This entire manual process wastes valuable time in which the infection spreads. ENIRA Technologies introduces the response in the *ENIRA Second*.

## 8. I have Firewalls and IDS and plan to purchase IPS/SIMS and ENIRA but I don't have enough budget.

IPSs deliver some improvement over existing Firewall/IDS infrastructure, but you still remain vulnerable to outside attacks and you still have a manual response plan. In order to successfully mitigate the cost of an attack - you need instantaneous response more than anything.

One of our customers has recently an incident impacting the network for 1 ½ months
and cost him at least $ 1.500.000. ENIRA would have cost him 1/6 of the damage.

Because Firewall/IDS/IPS systems have about 68% false positive alerts, SIMS technology was developed to consolidate information from many Detection and

Prevention devices before they send alarms. ENIRA receives alarms and automatically takes action.

### 9. How do I integrate my detection system with ENIRA?

ENIRA offers the open integration module that installs on any type of system you want to have automated activity from. This not only limited to Firewalls, IDS and IPS but can also include protocol analyzers, network management systems such as HP Openview, IBM Tivoli, and Trouble Ticket systems.

### 10. Which detection systems do you support?

ENIRA's open integration module is universal and therefore we support any detection system.

### 11. Do you integrate into my trouble ticketing system?

Activity messages can be sent to users and systems and are freely formattable. This allows you to send messages to your trouble ticket system automatically for all activities ENIRA takes. In return you could also automate responses from your trouble ticket system into ENIRA.

## HOW DOES IT WORK?

### 12. How does ENIRA Work?

Once configured with the information of your network infrastructure devices, ENIRA goes out and obtains the configuration data from all your network devices, and then builds the topology database. From that point on, ENIRA can identify the exact location of any network node within 1 second and take intelligent action.

### 13. How does ENIRA start working?

ENIRA works through either manual input via its web interface reachable from anywhere in your network; or automatically via the open integration module and your IDS and IPS systems. A third mode allows the Open Integration Module to send automatic shutdown requests to ENIRA. These requests are put into an

authorization queue for manual approval. This is specifically recommended for ½ of the event settings in today's IDS/IPS.

### 14. How Does ENIRA do a discovery of my network equipment

While you have the option to automate the installation process, with the ENIRA Open Integration Module connected to your discovery software, we have found that is good practice to just enter the IP addresses and device type of your network infrastructure devices (switches/routers/Active directory server/Wireless Access Points/time server). This process gives you the opportunity to think about some of the core policy settings you may want to configure in ENIRA as well. Once the infrastructure is configured we query all your device and automatically build the topology of your network.

### 15. What changes will I need to make to my network infrastructure to deploy ENIRA in my enterprise?

None. We work with your existing infrastructure.

### 16. Doesn't Cisco CSA solution quarantine nodes?

CISCO's CSA solution is an agent installed on Windows machines to provide individual workstation protection. This technology is only effective for known threats. In addition Cisco CSA does not enable you to take action in your network infrastructure devices, and would only work with CISCO devices. ENIRA has multi-vendor support, realizing that there are many manufacturers with excellent network infrastructure devices, which customers like to deploy.

### 17. Does ENIRA alert us to a cyber attack?

ENIRA does not alert or detect, but instead concentrates on the response and policy management. There are many vendors with detection technology and ENIRA is compatible with all of them.

### 18. Can I automate my Response in conjunction with my IPS and IDS outputs?

ENIRA comes with a custom application integration module as well as an API. The quickest and easiest way to integrate is to use the integration module, which is a command line executable that uses SSH services to communicate with ENIRA. ENIRA customers have used this technology and have integrated within minutes.

### 19. Isn't it dangerous to have my detection systems automatically initiate a response, because of false alarms?

We recommend to automate only your top categories, from which you are certain that these are true infections. Other events should be configured so they are placed into the ENIRA authorization queue.

### 20. I use a trouble ticket system, such as Remedy, OTRS, Answertrack, Momex. Do you integrate with it and how?

ENIRA allows you to send customized messages for every action taken. Sending messages to a Trouble Ticket Systems is as simple as setting up a new ENIRA user.
You can fully customize the message to accommodate your system's format in order to handle the information correctly. You can also send messages via email to any user to alert him of events in the authorization queue or of taken action.

## INSTALLATION AND MAINTENANCE

### 21. How many full time engineers will it take to administer ENIRA?

Once installed ENIRA does not require specialized personnel to operate it.

### 22. How long will it take to install ENIRA and what are the implications to my network during the process?

The typical installation does not exceed ½ day and can be done without any impact to your network traffic, since ENIRA is non-intrusive.

### 23. How many full time engineers will it take to install ENIRA?

ENIRA Technologies will come on-site for the installation and work with one of your network engineers. This is all it takes to install ENIRA.

### 24. What kind of training do you offer, and is there an additional cost?

During the installation we will show you all you need to know on how to operate ENIRA. In addition we offer classes for advanced automation techniques and assist in your efforts in event categorization. Typically installation takes half a day.

### 25. Do you provide Evaluation Units?

We are confident that after you see a demonstration of ENIRA, you will want to try it in your own environment. When you are confident that you will want to purchase a device, we provide an evaluation unit for a period of two weeks. We have many customer references that can also testify to the benefits of ENIRA.

### 26. What is your maintenance agreement and what does it include?

First year maintenance is covered in the purchase price and following will cost 18% of the initial purchase price. Maintenance covers full hardware and software maintenance. Software updates are made regularly available to cover new devices or changes in existing operation of devices.

### 27. How do I patch and/or update the ENIRA appliance?

You connect to ENIRA through your web browser. One of the menu functions allows you to update software right from your desktop and then execute a reboot of ENIRA in order to activate the new releases. We update ENIRA and the specialized Linux operating system, and all updates are included in your maintenance agreement.

### 28. How is the ENIRA system backed-up?

You can utilize the web browser interface to back-up your valuable configuration setting. ENIRA also offers redundant installations with an additional backup system.

### 29. What network equipment do you support?

ENIRA is fully multi-vendor capable and supports most vendors: 3Com, Bay, CISCO, Extreme, Foundry, HP, Juniper, NORTEL, and ODS. In addition we guarantee support for any unsupported device with your purchase.

### 30. Do you support MPLS networks?

ENIRA access is neutral to transport protocols. MPLS is a protocol that embeds network traffic, especially in your WAN to transport traffic in an MPLS cloud. . All that is required is that ENIRA has access to all network infrastructure devices.

### 31. What network infrastructure do you support?

We are independent from the network infrastructure and support all network topologies: wired, wireless, and VLAN. We identify the connection over which the offending station enters the network. In the example of VLAN we disable the user account rather then blocking just the IP address; because when reconnecting the user would otherwise receive a new IP address, and the damage could continue.

### 32. I have a decentralized organization and need a way to address independent divisions. How do I do this?

Although one single ENIRA system allows you to set up authority levels based on an hierarchical corporate structure, ENIRA Technologies found that some of our customers prefer a totally independent solution. For these customers we created the ***Distributed ENIRA system***.

### 33. How do you deal with more than 1 physical node hanging a single switch port? (Typically found if using VoIP or hubs for some locations)

Technologies such as VoIP that require a single connection to the switch or router. Therefore ENRIA allows the user to address node isolation in various ways. In the case of VoIP, MAC address filtering is the proper action, because it shuts out the traffic from the PC, while it keeps the switch port active for the VoIP connection. Some of the other possible actions include: Disable Port, Filter User/Mac Addr/IP Addr+Subnet/Hostname, Move to VLAN.

### 34. Do you support wireless access points?

ENIRA supports wireless access point like any other infrastructure device. In addition we provide the "action group" setting, bundling more than one device into a group. For wireless technology, disabling a MAC address on one access point would allow the user to automatically connect to other APs in reach. We therefore recommend configuring all APs in one building into one action group. In this case ENIRA blocks access on all APs in that action group.

### 35. How do you handle Voice Over IP?

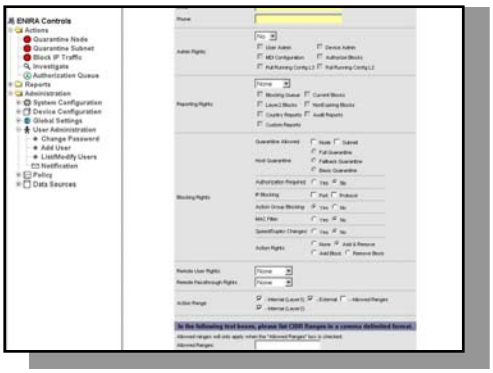
Technologies such as VoIP that require a single connection to the switch or router. Therefore ENRIA allows the user to address node isolation in various ways. In the case of VoIP, MAC address filtering is the proper action, because it shuts out the traffic from the PC, while it keeps the switch port active for the VoIP connection. Some of the other possible actions include: Disable Port, Filter User/Mac Addr/IP Addr+Subnet/Hostname, Move to VLAN

## SECURITY

### 36. Is the data I enter into ENIRA secure?

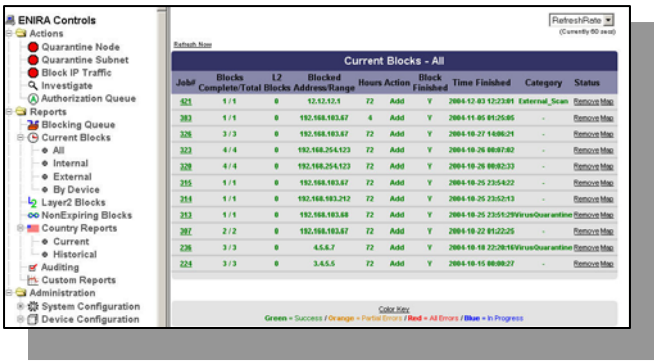
ENIRA uses 256 bit encryption technology to store all mission critical information such as user ID's and passwords.

### 37. Can you deal with different levels of user authorities?



ENIRA has a sophisticated user setup. The various layers of authority can accommodate all your corporate security needs. User rights can be given in many different categories: Administration, Reporting, Blocking, Remote Access, and Action types. The *Authorization Required* feature gives control to the network administrator, while individual users can still be alerted to a necessary shutdown.

### 38. How can you help me with reporting for HIPPA, Sarbanes-Oxley, and FERC for example require detailed reporting and integrity checking.




ENIRA is completely self-documenting. All of the actions taken are inserted into a database, to access at any time. ENRIA's extensive reporting capability includes various reports: Blocking Queue, Current Blocks, Layer 2 Blocks, Non-expiring Blocks, by Country, Auditing, and Custom.

### 39. How will ENIRA make our network more secure?

For sophisticated networks there is no single solution that provides complete protection from attacks and viruses. But when you are attacked, ENIRA can instantaneously arrest it - preventing any further damage to occur.

You will be secure in knowing that ENIRA delivers a predictable and audit-able response. Its extensive reporting systems can be used for further analysis enabling your organization to fine tune your existing strategits, and help to educate your users. You will be secure in the knowledge that you are doing absolutely everything you can to contain and control related costs.

## MISCELLANEOUS

### 40. Why is instantaneous response so important?

Responding automatically to an attack alert allows you to contain the damage, which means there is much more control for the network operator. When the infected nodes are quarantined you have contained the infection, stopping its proliferation. Analysis and clean up can begin immediately. Full reporting of what actions took place, and network topology updates are at your fingertips.

Every second you don't respond to a cyber attack the infection spreads. Dinah Greek writes on January 6th, 2004, that the Slammer (aka Sapphire) worm doubled in size every 8.5 seconds.[i] Your response today takes from minutes up to hours (in some cases even days). This means in 10 minutes the attack has spread $1.2^{21}$ times – number with 21 0s.

## 41. I did not plan in my budget for a response system, can I afford ENIRA?

The very first time ENIRA saves you from an attack that would have sent your organization into a tailspin for 48 hours, the return of investment quickly becomes obvious. Businesses differ in how they calculate the cost implications of cyber events; how much time was lost? How much personal was involved in the cleanup process? (Average $290 per node according to research from mi2g[ii]). This means in a 5000 node network your damage can be between $290 and $14,500,000[iii]. ENIRA will cost you much less than the average damage incurred by a single cyber attack.

---

[i] CSI director Chris Keating states: "*And hackers won't become complacent anytime soon. New attacks are devised every day, and we still have our work cut out for us*"[i].

It seems that hardly a week goes by when computer viruses aren't making headline news. The release of the SQL Slammer and Sobig worms last January, followed by the MSBlast.exe worm in August, graphically illustrate how the nature of these attacks is ever increasing.

They also show that, although viruses have been around for over 20 years, computer users generally are still unable to ensure that they have enough immunity to resist infection……

…. The key questions being asked today are not just 'how can I protect myself or my organization?', but 'what's the cost of being hit and recovering from it?'….

….Future threats will be a blend of viruses, Trojans and worms that will use multiple vectors to spread. So a worm may include a routine to load a Trojan onto your system, while a Trojan could be used to run a virus……

…..In September 2003 Dr Gerhard Eschelbeck, chief technology officer at computer security firm Qualys, warned in a speech to the US Congress: "Network security attacks are increasing in number and sophistication. New and evolving attacks are capable of spreading faster than any possible human response effort."

We saw this with the Slammer (aka Sapphire) worm. Propagation speed was its novel feature. In the first minute, the infected population doubled in size every 8.5 seconds.

The worm achieved its full scanning rate (over 55 million scans per second) after approximately three minutes, after which the rate of growth slowed down somewhat because significant portions of the network did not have enough bandwidth to allow it to operate unhindered. Most vulnerable PCs were infected within 10 minutes of the worm's release…….

It claims to fix the vulnerability but actually installs a Trojan allowing a virus writer to remotely control an infected PC.

Denah Greek, Personal Computer World, January 6th, 2004
http://www.computeractive.co.uk/features/1151775

[ii] **London, UK - 24 August 2004, 17:45 GMT** - There are an estimated 600 million Windows based Personal Computers (PCs) across the world of which over 200 million run Windows XP, according to the latest estimates from Microsoft. Therefore, the release of the new Service Pack Two (SP2) - designed to patch many critical security vulnerabilities in Windows XP - is a subject of direct relevance to geographic populations and corporations greater than most countries on earth and yet there is no consensus on the optimum methodology for dealing with this necessary installation. According to the latest available research from **mi2g**'s SIPS database, the economic damage from malware proliferation in 2004 including MyDoom, NetSky and SoBig is estimated to lie between $157 billion and $192 billion worldwide or expressed another way, it works out to between $261 and $320 - average $290 - of productivity losses worldwide per Windows PC. This latest estimate of losses per PC attributable to malware proliferation demonstrates the validity of the algorithm 'Economic Valuation Engine for Damage Analysis' (EVEDA), which forms the basis for the digital risk assessment research carried out by the **mi2g** Intelligence Unit.

Source:
http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/abstract.php/damage

[iii] A virus in 2000 infected 1,000 computers a Ford Motor Company. Ford received 140,000 contaminated e-mail messages in three hours before it shut down its network. E-mail service was disrupted for almost a week within the company.
(source: http://www.csis.org/tech/0211_lewis.pdf)

the Love Bug virus is estimated to have cost computer users around the world somewhere between $3 billion and $15 billion. Putting aside for the moment the question of how the estimates of the Love Bug's cost were calculated (these figures are probably over-estimates), the ability of a single university student in the Philippines to produce this level of damage using inexpensive equipment shows the potential risk from cyber crime to the global economy.
(source: http://www.csis.org/tech/0211_lewis.pdf)