ENIRA™ technologies

respond.
command.
control.

White Paper

ENIRA™ Network Response System

The missing link in your Security Solution

ENIRA Technologies

WWW.ENRIA.COM
(888) 277-7638
sales@enira.com

Table of Contents

Introduction

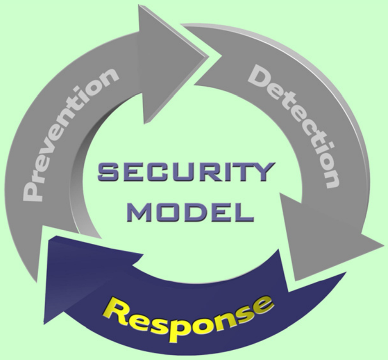
ENIRA Incident Response System provides:

- **The command and control to quickly and easily quarantine and instantly disconnect any desktop, laptop or other host, anywhere across the enterprise**
- **The ability to achieve this without requiring any agents, clients, or inline devices to be deployed across your network**
- **Specifically designed to leverage your existing and future cyber-security prevention and detection investments**
- **Automated, “self-documenting” incident response reporting**

This document describes the technology background which demands the ENIRA solution.

The Security Model

Prevention, Detection, Response is the foundation to every security model in use today.



The concept is simple:

Prevention – the methods or systems that are put in place attempting to automatically guard against the known threats and attacks.

Detection – an attempt to detect known threats or abnormalities/anomalies (anything from a visual sighting to sophisticated electronic measurement) that were able to bypass existing prevention and then quickly alert appropriate authorities.

Response – the action to be taken upon receiving an alert of a threat or unanticipated anomaly. Quickly execute a dynamic, intelligent and precise response, resulting in the containment and halting of the threat time or situation.

Heart attacks, burglaries and fires are just a few samples of threats we have to manage in our everyday lives. In each of the cases we have to utilize the same security chain. Let’s take a closer look at one of these examples:

Fire, very much like internetworking, is very beneficial if properly harnessed. If this same power, however, is uncontrolled or intentionally misused it quickly turns into life threatening disaster. In case of fire we have adapted the above well accepted security model in order to deal with the threat potential:
Prevention: fireproof materials, circuit breakers; *Detection:* smoke and fire alarms, human intelligence (sight/smell); *Response:* sprinkler systems, fire department.

Despite the advance we made from the turn of the 20th century till today in the area of prevention and detection, nobody will ever suggest to abandon the response. While this seems preposterous in the example of fire, we find that most IT organizations have at best a manual response plan for security breach in place, equivalent to a bucket line in case of a building fire. They need to recognize that there is a missing link in their cyber security strategy!

Time is the enemy, and only a rapid, intelligent and coordinated response can make the difference between a minor incident and significant damage!

What else can be taken from this analogy? The majority of the damage caused by today's cyber security attacks is based on the inability to quickly and effectively respond to these attacks. Attacks will always be successful despite the investment in prevention and detection technologies, since it is the goal of cyber criminals to find always new methods to circumvent whatever measures are put into place. Hence organizations need to strengthen their response capabilities

The strongest security configuration should provide a defense-in-depth, where technologies and procedures are deployed as overlapping layers throughout the organization, ensuring no single failure can compromise the entire organization's ability to function. A complete defense spans the entire security lifecycle of Prevention, Detection, and Response in an effective way.

Let's examine how today's available cyber security solutions fit within each of the security model components and what holes remain.

Prevention and Detection - A Quick Overview

Firewalls are the most common form of prevention technology. They provide a perimeter defense and must sit inline, at a network chokepoint, in order to effectively protect the inside from the outside. Firewalls use a rules-based security policy to determine which traffic to pass through and which traffic to discard. Firewalls are equivalent to the first check at the airport gate. A as long as you have legitimate identification, you are allowed to proceed to security.

As cyber attacks evolved and malicious activity began to be hidden within what was once considered legitimate traffic. The firewall alone has been proven to be insufficient. For example a firewall may be configured to allow web traffic on port 80 into the network, but it is incapable of telling if the traffic on port 80 is malicious or not. Similarly, you may be allowed through the gate as long as you have legitimate identification, but that does not mean you do not have a weapon in your bag.

Because of this detection technologies such as intrusion detection systems (IDS) have been developed. The goal of IDS is to perform a deeper inspection of the "allowed" traffic to see if it contains any known malicious activity. IDS is analogous to the metal detectors and video cameras that are the second line of defense in an airport. Once you made it through the entrance, now let's have a look at your luggage. IDS are signature based, meaning they have a list of known attack identifiers to compare traffic against, and must be continually updated as new forms of malicious activity evolve in order to remain effective. Detection technologies raise alarms but have no inherent capabilities to prevent attacks or stop an attack in progress. In addition to IDS, many other enterprise technologies such as Network Management Systems (NMS) and Enterprise Management Systems (EMS) can act as good sources of detection information.

Intrusion prevention systems (IPS) are relatively new security devices that combine prevention (firewall) and detection (IDS). Network traffic entering an IPS must pass both the "rules test" and the "signature of known attacks test" before being allowed through. IPS, just as firewalls, must sit inline to be an effective prevention tool.

In addition many forms of client based prevention and detection technologies exist. Among those are Anti-virus software and host-based firewalls. Like all forms of prevention and detection, these systems help guard against or display alerts on known attacks based upon configured rules and/or attack signatures.

A good combination of well configured prevention and detection technologies at an organization's perimeter and vital chokepoints provide a needed defense against common cyber attacks that have been frequently attempted and are well known.

However, the critical missing component in many organizations is the acknowledgement that no security posture or technology is invincible - prevention technologies are not capable of stopping all attacks. Detection technologies alone provide no defensive or offensive capabilities and therefore they do not provide complete security. Why are the weak points in prevention and detection?

Shortcomings of Prevention

Protecting against attacks is as old as mankind itself. So is the history of bypassing prevention measures. Germany circumvented the Maginot[1] Line which France didn't anticipate and Trojans[2] were tricked by the legendary Trojan horse an event that today describes cyber security attacks.

[1] Shortly after World War I France invested billions of dollars and years of labor into building a massive, incredibly sophisticated wall, the Maginot Line, along the French/German border in order to protect them from anticipated German aggression. With the beginning of World War II the Germans set their sights on France. The obstacle of the wall appeared impenetrable and would have taken a mammoth effort to successfully attack. So the Germans adapted their strategy and attacked Belgium, France's northern neighbor, instead. They quickly overtook Belgium and simply did an "end around" the wall, coming up behind it. This unforeseen approach caused France to fall in only 35 days, despite the massive time and resources they had devoted to their eastern border defense. The French planners did not anticipate that strategy. France's false sense of security led them to neglect proper preparation for an effective internal defense. When the French recognized in their observation posts the battles in the distant Belgium, it was already too late. There was no way to dynamically pick up the wall and move it. The defense was static and France was quickly overrun.

[2] The Greeks raged a more than 10 year long war against the Trojans. But regardless of what they tried to do, they could not bring the city of Troy to fall. The Trojan War had many casualties in particular for the Greek side. Troy's walls were considered invincible. The Greeks finally conceived the strategy to build a huge horse in which they hid their soldiers. They presented the horse as a peace present and the unsuspecting Trojans brought the horse inside their city. At night, when the Trojans had fallen asleep, the Greek soldiers hidden in the horse came out, opened the gates, and gave the signal to the main army which had been hiding. Troy was completely destroyed.

Today’s prevention technologies have the same inherent vulnerabilities as the Maginot Line or the “invincible” walls of Troy.

First, they are only effective against what is known, planned, and anticipated. They will only prevent the known attacks that they have been configured to prevent and offer no defense in unanticipated situations. They are unable to dynamically adjust their rules based on a new attack. This causes prevention technologies to be stuck in an escalation game, constantly having to be reconfigured as the enemy adapts.

Second, they are static. When there is an unanticipated event (an "end around"), the inside of the network is vulnerable, defenseless and quickly overrun. There is no way to move the wall. No way to quickly contain and quarantine an attack once it is inside the chokepoint. Static defenses will not defeat evolving attacks.

Shortcomings of Detection

Detection technologies just alarm, similar to a smoke detector or home security system. By themselves they provide no means of defeating the fire or stopping a burglar from running off with your prized possessions. You still need the fire department and police to respond.

Signature based detection technologies are always vulnerable. This opens the network “doors” to new attacks before signatures exist or devices have been updated. And even newer behavior-based detection systems base their logic still on known behavior.

Detection technologies, like IDS/IPS and event management systems, are nonetheless your eyes and ears into your network and are critical to any complete cyber-security strategy. Without them your vision is impaired and response will suffer.

The Need for Response

Back to the airport. Let’s follow an individual in. Since he has the proper identification, he is allowed through the gate. He is then being watched by the cameras and pass metal gates while passing security. This individual knows that he will be going through the metal detector. He knows that common weapons such as guns, knives, and bombs have a high probability of being detected. What does he do? He brings a new weapon. Maybe he will bring a knife made of graphite or a gun made out of yet undetectable material. Hence he will pass security. Sometimes the bad guy might just come through an unexpected back door or even worse is one of the airport employees, hence avoiding security altogether. Either way, this individual is now walking through the terminal just like any legitimate passenger. What is going to happen when he pulls out the weapon and begins inflicting damage? Detection devices, such as the video cameras, provide no means to combat the aggressor, they can only alarm. Without an efficient team of armed guards capable of quickly responding the security breach will lead to disaster.

This is no different in your enterprise when cyber attacks occurred. Many ways can be found to bypass today's cyber securities. And it really does not matter if

- a new type of attack occurs whose signature is not known yet
- there was not enough time to update rules and configurations
- the attack did not come through the perimeter or inline defenses at all
- a mobile user came to work with an infected laptop and connected to the network
- a employee brought in an infected file after working evenings at home
- a disgruntled employee causes damage to harm the company

What matters is there are many ways attacks can bypass or evade static defenses. And regardless of how it got there or what type of attack it is, once it is in...IT IS IN!

You cannot send the attack back through the firewall or IPS, update signatures, reconfigure rules, or start pushing out patches. The current attack has happened and must be dealt with quickly. These are the times where the vulnerability of relying only on prevention and detection technologies will cause major damage in your network with associated financial burdens.

Your organization must be prepared to respond quickly.

The Challenges of Responding

What does "prepared to respond" mean? You must be ready and able to quickly quarantine and contain cyber attacks anywhere on your network. You must be ready to respond at the host level anywhere on your network. An intelligent response must not only have the ability to understand the complexity of your multi-layered network consisting of routers, switches, circuits and other devices, but needs to be able to dynamically adapt to all network configuration changes. At the time of attack your information is often limited to the source or destination address. Your goal is to quickly formulate a response strategy then take the actions necessary to neutralize the attack and stop the bleeding. Keep in mind that cyber attacks are now propagating at unprecedented levels and are only getting faster, therefore any response that is not immediate can dramatically increase the scope of the damage.

For many organizations, this is when they are at their weakest. Often an unanticipated cyber attack, whether it be hacker, worm, malicious user, distributed attack, or any other form, can bring with it a feeling of helplessness, confusion, and even chaos. Organizations that actually have formal, documented response procedures, which are complex and require specific, need highly skilled engineers capable of configuring heterogeneous network devices. These engineers also require a detailed understanding of the network topology and are rarely available on a 24x7 basis. Typically these manual processes are extremely time consuming and, like any manual process, are subject to human error.

In a drastic measure many organization resort to just "pulling the plug" in an attempt to prevent being completely overrun. Of course this terminates network service to large portions of the enterprise or entire customers. This often creates a situation were the cure can be worse than the sickness, especially in today's operationally focused and politically charged environments

.

ENIRA - Cyber Security Response

ENIRA Technologies' *Enterprise Network Incident Response Appliance* (ENIRA) is an intelligent Incident Response System that drastically reduces the time required to effectively respond to cyber-security incidents from minutes, hours, or even days, to seconds.

Using **ENIRA**, a single operator can quickly and easily quarantine and instantly disconnect any desktop, laptop or other host anywhere across the enterprise without endangering the availability of business systems and mission-critical traffic flows.

ENIRA's patent pending technology achieves this without any clients, agents, or inline devices.

Think of **ENIRA** as the armed guard in the airport. He is able to quickly respond to any malicious activity, anywhere in the airport. He can respond to passengers walking about in the terminal, incidents at the metal detectors, or trouble at the gate. He does not care if the type of malicious activity being committed has been seen before or even if a weapon being used is new. He is trained to confront the threat head on and stop it before it hurts anyone else.

How It Works

Once your IT staff identifies a desktop, laptop or other host that needs to be quarantined, **ENIRA** quickly determines its precise location within your network (down to the specific switch port) and dynamically reconfigures the appropriate network infrastructure devices to completely disable the node's network access. **ENIRA** is capable of achieving this through sophisticated algorithms that combine a detailed understanding of your network's topology with the ability to centrally leverage the inherent security capabilities in your existing network devices (routers, switches, firewalls, wireless access points, VPNs etc.). **ENIRA**'s advanced technology "plugs" into your existing security architecture, enabling you to move security beyond inline devices and into the network fabric.

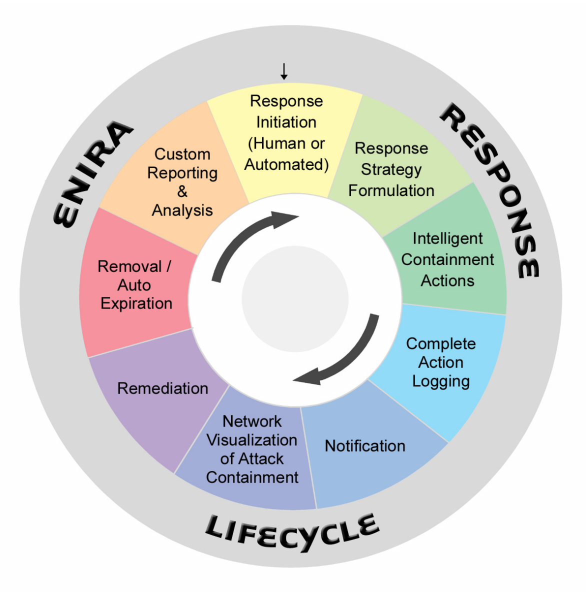
ENIRA's response can be either initiated manually, using its easy web browser GUI, or automatically, using its Open Integration Module (OIM) for your existing prevention and detection devices.

Focused specifically on incident response, and not on preventing or detecting attacks, **ENIRA** leverages your existing prevention and detection investments enhancing their capabilities while maintaining a consistent response strategy and technology.

In addition **ENIRA** provides easy control of enterprise-wide IP traffic policy. This allows you to deploy rules quickly dictating how your network routes IP ports and protocols. This is especially useful to instantaneously secure your environment against new software vulnerabilities and large scale attacks.

Complete Incident Response Lifecycle

Unlike other security solutions or complex manual processes, **ENIRA** establishes a repeatable response process and lifecycle to cyber-security breaches, bringing control and order to a situation often marked by confusion and chaos.


ENIRA
RESPONSE
LIFECYCLE
Response Initiation (Human or Automated)
Response Strategy Formulation
Intelligent Containment Actions
Complete Action Logging
Notification
Network Visualization of Attack Containment
Remediation
Removal / Auto Expiration
Custom Reporting & Analysis

This lifecycle begins with initial incident containment and steps all the way through incident reporting and analysis.

ENIRA is completely self-documenting, tracking changes in your network topology and logging details on the actions taken to implement attack quarantines.

Built-in, customizable notification schemes and authorization queues facilitate response communication and control.

Once an incident is addressed and an "All Clear" is given, the quarantine can be easily removed. The network access for the node is re-enabled by simply clicking the "Remove Quarantine" button within the GUI.

Finally, **ENIRA** provides a robust web-based incident response reporting system. All of the web-based reports are interactive, allowing you to "drill down", from a high-level graph, into the details of each incident response action. Features, like custom reporting categories and the ability to automatically access data from subordinate organizations, enable you to easily create individual or consolidated incident response reports for analysis.

Features and Benefits

A single platform provides all of **ENIRA's** functionality without requiring any reconfiguration of existing network devices, unlike many traditional security solutions which require multiple physical systems and complicated, intrusive deployment.

ENIRA is agent-less and client-less, using native communications, including telnet and SSH, to communicate with your network devices (web management interfaces are also supported). This eliminates the need for your staff to manage the challenges, complexities, and security risks associated with client based agents.

Multi-vendor and multi-technology support is a major benefit to **ENIRA** allowing you to work with most major network equipment vendors, their leading technologies, as well as the legacy infrastructure. This flexibility avoids being locked into any specific vendor.

To facilitate quick and easy deployment, training, administration, and operation, **ENIRA** is delivered as a secured appliance with 100% web-based management. There is no command line or proprietary console interface.

ENIRA leverages your existing IT staff and increases the efficiency and effectiveness by:

- Dramatically simplifying the technical skills necessary to effectively respond to cyber-security incidents
- Increasing productivity by reducing incident clean up costs and effort

Distributed Operational Support

Multi-tiered, distributed organizations have often several independent IT groups. For those environments ENIRA can be deployed hierarchically. This architecture enables distributed administration, but keep the incident communication, reporting, and response centralized.

ENIRA's flexibility empowers your organization to quickly and easily institute a commanding incident response capability, without requiring you to change operational policy or restructure distributed IT support.

Conclusion

As the cyber security battle continues to escalate, organizations must have the ability to quickly contain and quarantine malicious activity anywhere on the network and outside of what has been planned, configured, and anticipated. Without a powerful response capability, many will find themselves vulnerable and quickly overrun.

ENIRA provides the only true, comprehensive "network-enabled" response capability, completing the Prevention, Detection, Response security paradigm.

For more information, please visit us at: www.ENIRA.com

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 the 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.