RAVEN is a computer security product that makes it easy to protect your networks from attacks and intrusions. RAVEN discovers, detects/protects, reacts/alerts and presents from a single consolidated unit that is about the size of a cable TV/DVR box.

- Discovers - like a home security tech that walks through the home looking for all the entry and exit points, RAVEN finds a network's entry and exit points as well as all the assets (computers, routers, modems, switches, etc.) on the network that need to be protected so it knows what to protect.
- Detects/Protects - like the cameras in a home security system and the sensors that are triggered when a door is opened, RAVEN watches and protects your network.
- Reacts/Alerts - like an audible alarm and phone call to the police from a home security system RAVEN will react to an attack. It can alert the proper people that something "bad" is happening. It can also be set up to take action when it detects something "bad" is happening.
- Presents - like the monitors at a home security system's operations center RAVEN displays the things that are happening on your network in a web browser based display.

Not only does RAVEN do all of this but it is not visible on the network so it cannot be attacked.

Promia Inc.

101 The Embarcadero, Suite 200
San Francisco, CA 94105
Phone: 415-536-1600
Fax: 415-536-1616

www.promia.com

Network Security Background Information for the non-IT Professional

Promia Inc.

What is RAVEN?

For the geeks among us, RAVEN is an IDS (Intrusion Detection System), an IPS (Intrusion Prevention System), and a NMS (Network Mapping System). It is an entire SOC (Security Operations Center) in a single unit. We like to think of it as a SOC (pronounced "sock") in a box.

Not a geek? Well maybe this document can explain things.

How protecting your network is like protecting your home

Your **home** contains the things that are precious to you; everything from those you love to your jewelry. Home Security Systems protect them using a few things.

- Walk-through – a technician walks through the home to find all of the entry points. If your home were a computer network that technician would be a Network Mapping System (NMS).
- Sensors – sensors on doors and windows detect intrusions. You might call them an Intrusion Detection System or IDS.
- Cameras – cameras watch the doors so you can prevent those you don't know from entering. You might call them an Intrusion Prevention System or IPS.

All of these components are connected to a central location that monitors your home; the Security Operations Center (SOC).

Your network, like your home, has traffic going in and out. That traffic contains data, (i.e. payments and info about those making said payments) that intruders can steal. Imagine someone hiding in the bushes outside your front door. As you approach your home they jump out and steal your wallet. Well, the same thing can happen to a payment that is entering your network. Not only is your money stolen but so is your personal information (your identity).

Your network, like your home, needs to be protected. Plenty of products exist to help you do that. Some of them are Intrusion Detection Systems (IDS). These vary in their effectiveness sometimes protecting a single entry point (like a sensor on a single window in your home), some protecting many entry points. Some of them are Intrusion Prevention Systems (IPS). Like the cameras in a home security system they try to stop an attack before it happens. Some of them are Network Mapping Systems (NMS) that discover everything on the network that needs to be protected (like the technician that walks through your home before installing a security system). Some even combine one or two of these things but in order to have complete protection your network needs all of them and needs all of them working together. It needs a SOC (Security Operation Center) that uses information from all of them to defend and protect your network, and to alert the right people when something goes wrong.

Most IDS and IPS depend on pre-existing knowledge to identify an attack/intrusion. They don't have the ability to flag unusual behavior.

Oh, one more thing; most security products can be seen by cyber criminals (intruders) and can be attacked themselves, rendering them useless.

Why use RAVEN?

- RAVEN is an Intrusion Detection System (IDS) that will not only protect all of your network's entry/exit points from well-known attacks but will also protect your system when it sees unusual behavior on your network.
- RAVEN is an Intrusion Prevention System (IPS) that will prevent/limit damage done by attacks.
- RAVEN is a Network Mapping System (NMS) that finds all of the entry/exit points and finds all of the network assets (i.e. PCs, laptops, servers, etc.). It then uses that knowledge to help secure your network.
- RAVEN watches for unusual behavior on your network. You might think of this as a banker giving you a call when he sees a credit card charge in a foreign city when 99% of your charges are near your hometown.
- RAVEN is a "hardened" device, making it undetectable from the outside, which gives it the unique ability to avoid direct attack. If you can't see it you can't hit it.

RAVEN combines all of these functions making it a Security Operations Center (SOC) delivered as a single component. There is no need to get many products and try to get them to work together.

Like a home's security system sends alerts RAVEN can alert the right people when there is a problem on your network; be it an attack, a visit to a restricted website or even a PC crashing.

More than that, it has the ability to take action on its own. For instance, if an attack is flooding a portion of your network (thus slowing down the entire network) RAVEN can shut down that portion of the network rendering the attack useless. If a vandal were to stick a garden hose into the bedroom window the only thing your home security system could do is sound an alarm. If that home security system had RAVEN-like capabilities it could slam that window shut, putting a kink in the hose and stopping the flow of water.

Last but by no means least; RAVEN is scalable across your enterprise. RAVENs can watch individual pieces of a business' network and aggregate alerts up and through the business' top level so you are aware of widespread attacks. In the same vein, a change in your security policy is made easy because it can be pushed down to other RAVENs.

We like to think of RAVEN as a Security Operations Center, a.k.a SOC (pronounced "sock") in a box.

Now that you know some geeky terms let's end with a geek joke.

What should you do to protect your network ?..... Stick a SOC in it!