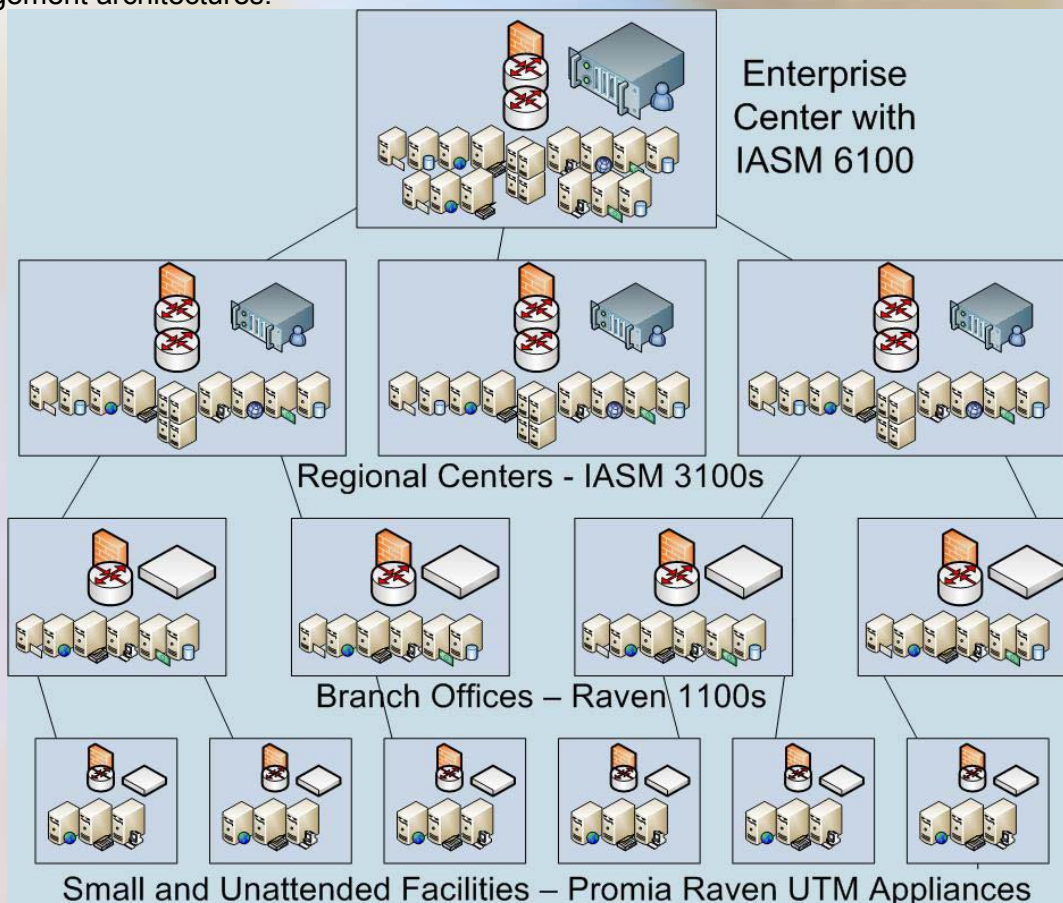


Promia Raven™ Network Appliances

PROMIA is committed to a vision of highly robust, policy-driven, information operations and security monitoring, remediation, and management in networked environments that are subject to security risks and regulatory compliance requirements. Promia delivers on this vision with its **Raven™** family of network appliance products. Raven appliances enable information systems (IS) operations personnel to: **detect, visualize, monitor, and manage** network devices, computers and enterprise applications; **manage security and operations information** from a wide range of device and software logs; and **analyze collected information to detect and respond to security and operations incidents**

As shown in the diagram below, Promia Raven and IASM (a predecessor of Raven) families of appliances interconnect to provide optimum coverage with minimal cost – they have been designed for use in stand-alone, federated, and hierarchical Information Operations and Security Management architectures.



KEY FEATURES OF Raven APPLIANCES

Raven appliances provide the capabilities described above by implementing the following feature sets: ***Asset, Anomaly, and Attack Detection***; ***Autonomic Response Behavior including Intrusion Prevention, Collection and Consolidation*** of logs from network and security devices, node OS, and applications; ***Event Analysis for Incident Detection***; ***Incident and Response Management***; and ***Network Status Visualization***.

Asset, Anomaly, & Attack Detection

All Promia Raven and IASM appliances collect raw network traffic and then filter it through a specialized tool set to provide the following features for IT operations and security personnel:

- **Passive Asset Detection:** in which addressing and protocol information in the IP traffic is used to non-invasively detect and fingerprint assets on the network and determine the topology of assets on the network.
- **Anomalous IP Traffic Detection with Blocking:** in which the Raven uses network traffic collected during a one to six hour training period to develop a profile of "normal" IP traffic for the network and then monitors subsequent network traffic to detect and generate an event for packets that deviate from the profile. The system blocks selected packets in TAP mode.
- **IP Packet Signature Matching:** in which the Raven uses the Snort™ signature matching engine to compare the content of each IP packet with known pattern rules for attacks or prohibited application behavior and generate an event when a rule is matched. Promia's Raven appliance support includes monthly updates of the operational rule set with the most recent rules that have been developed by the open-source Snort community and tested by Promia for accuracy and relevance.
- **Alert Context Capture:** (selected models only) in which the Raven records 1-60 second "snapshots" of IP traffic both before and after an IASM event for later remote forensic review by skilled incident analysis personnel.

Collection and Consolidation

One of the key functions of the Raven 1100 and 2100 models is to collect and consolidate log records from many NIDS and HIDS, as well as logs from firewalls, VPN appliances, routers and host operating systems and applications. Collection of these events is done by placing intelligent software agents at strategic locations on the network to read and forward the log records to the Ravens. All of the agents are managed from the Raven appliance.

Event Analysis for Incident Detection

One of the key distinguishing features of Raven is the advanced analytic algorithms incorporated into each Raven appliance. These algorithms consider events from multiple sensor logs to detect security and operations incidents that cannot be seen from a single sensor. The algorithms are based on unique sequencing techniques developed by Promia engineers, which use a combination of artificial intelligence and statistical analysis tools to aggregate multiple related events, thus improving analytic speed and accuracy. The algorithms are truly unique in their ability to tag each detected incident with a natural language description of the kind of incident that is indicated by the constituent events. This feature tremendously improves the ability of operations personnel to validate and respond to detected incidents.

Incident and Response Management

The Raven provides a standardized web interface for managing the incident lifecycle, including: triage, assignment, validation, remediation, and closure. The Raven can be configured for either or both manual and automated response to detected incidents. In support of manual response, Raven can be configured to display enterprise policy for remediation of the kind of incident detected. The Raven automatically blocks selected packets based on intelligent filters.

Network Status Visualization

The Raven appliance uses the model of network assets and topology generated by the **Passive Asset Detection** feature as the basis for the powerful, 3-dimensional consolidated visualization of all assets and incidents on the monitored network that is presented by the Raven Asset Viewer. This visualization allows operators to quickly see the operational and security status of the network and provides them with context for effective verification and appropriate remediation of detected incidents. The Asset Viewer in the Raven also provides a detail drill-down feature, which allows an operator to see all of the detected operational and security incidents for a business-level asset (such as a server or application), expand any one of those incidents to show the set of event records that comprise the incident, further expand any of those events to show the detailed event information, and finally, in the Raven 1100 and 2100 units, use the **FishbowlSM** feature of the Raven Web interface to review the network packets that were being transmitted when the event was detected.

THE Raven VALUE PROPOSITION

Operationally Proven In US Navy Global Network Operating Centers

The Raven emerged from a Small Business Innovative Research contract with the US Navy to collaboratively develop a security incident management tool for its Global Network Operating Centers (GNOCs). The GNOCs have the daunting challenge of managing a network environment that spans the globe and is under constant attack from determined, technically sophisticated, and well-funded adversaries. In this environment, the Raven has evolved and matured into a proven enterprise-class product that has become a key tool in the U.S. Navy's Computer Network Defense strategy and architecture.

Network and Security Operations Management Convergence

Guided by US Navy GNOC operations personnel, the Raven capabilities have steadily evolved to include many basic network asset management features. The Raven derives its effectiveness as a management tool from two complementary factors: first, incident detection becomes far more accurate when the analytic process factors in the operational importance of protected assets and, second, the observable causes and effects of operational security faults and malicious attacks are often close to identical. The result is that the Raven provides a common picture of both the operational and security status of the networks it monitors – thus providing real value to both Network and Security operations personnel.

Enhanced Network Transparency for Regulatory Compliance

The United States market for products like the Raven appliance has evolved and prospered due – in large part – to the many emerging laws, regulations, policies, and standards that require both government and commercial enterprises to exercise more control and permit greater transparency of their operations. Promia has developed a series of white papers describing the role that Raven plays with respect to implementing the controls needed to comply with FISMA, OMB A123, Sarbanes-Oxley, Gramm-Leach-Bliley, and HIPAA. Additionally, Promia has developed an enterprise regulatory compliance analysis process, which allows organizations that are subject to multiple laws, regulations, policies, and standards – some of which contain contradictory mandates – to identify and consolidate the technical effects of all applicable mandates into a single regulatory compliance strategy and architecture.

For more information, please contact:

PROMIA, Inc	415-536-1600 (Phone)
160 Spear Street, Suite 320	415-536-1616 (Fax)
San Francisco, CA 94105	sales@promia.com