

Protect Against Threats in Today's Digital World

With the incidence of malicious activity by worms and hackers constantly on the rise, the challenge of balancing authorized access with essential protection of business resources is continually becoming more difficult. Sana Security and Service Integrity provide the most powerful, integrated solution for the protection of private and proprietary customer information. Primary Response leverages Sana Security's unique adaptive profiling technology (SanAPT) to prevent and notify about activity outside of the norm. Service Integrity's SIFT[™] product monitors and analyzes application layer information in real time. The rich security event information from Primary Response, combined with the detailed transaction information from SIFT, provide a holistic view and unprecedented awareness of business infrastructure. Applicable to a wide range of customers' infrastructure and security scenarios, this joint solution comprised of Primary Response and SIFT products is of particular value to organizations in financial services, healthcare and government sectors.

Consider:

- By 2006, all major off-the-shelf enterprise applications that provide Web services interfaces will suffer from the regular discovery of significant security vulnerabilities and from numerous automated attacks." (Gartner, November 2003)
- In its first 3 minutes of life, the Slammer worm was scanning 55 million targets per second. By the 10 minute mark, 90% of vulnerable machines on the planet were infected. (CIO, November 2003)
- Enterprises already spend roughly \$2bn/year to investigate, prioritize, test and deploy patches. (Aberdeen Group)
- While fewer than 15% of all attacks occur within the first month of a vulnerability announcement today, that number is expected to reach roughly 30% by 2006. (John Pescatore, Gartner)

Improve Application Security and Awareness to Reduce Costs of Regulatory Compliance

Primary Response represents a breakthrough approach in intrusion prevention. Unlike traditional signature- or rules-based products, Primary Response not only protects your standard and custom applications from known and malicious code and events, but also blocks previously unknown ("zero-day") activity. This unique approach to security through inclusion of authorized operation rather than simple exclusion of a defined set of harmful events, secures your critical business infrastructure from both its historic vulnerabilities as well as new ones that seem to emerge every week. Its robust management and alerting capability, when combined with the innovative SIFT software from Service Integrity (designed to analyze, capture, alert and report on underlying web or XML based interactions between applications and throughout networks), enables customers to complement industry leading intrusion prevention with real time, actionable information about such prospective breaches for unparalleled awareness. And, Primary Response provides a concise record of activity, intended target and business impact (or lack thereof) related to attempted security breaches for forensic and regulatory compliance purposes.

Ensure Efficient, Yet Secure Business Operation

Failure to adequately protect your network infrastructure, critical business applications and services, and proprietary (and private) business information from both existing and previously known attacks can have huge detrimental impacts on your business operations, costs and customer relationships.

Leverage this innovative, integrated solution from Sana Security and Service Integrity to attain:

- The highest level of security and availability
 - Protection from both previously known and unknown (zero-day) attacks
 - Pro-active alerting with complete visibility into relevant activity
- Secure business operations
 - Preservation of irreplaceable business information
 - Continuity of service/uptime/productivity
- The lowest cost of deployment and management
 - Self-discovery, configuration and update
 - Real-time visibility into activity before, during and after attacks
 - Seamless integration into existing monitoring and management systems
- Clear, concise records of attempted breaches
 - Actionable information and log of XML-based interactions related to abnormal activity
 - A record of the integrity of important business/privacy information

Avoid Crippling Security Threats Today and Tomorrow

Large enterprise organizations continue to benefit from powerful, new information management and business applications, tools and systems. However, these technological advances also increase the vulnerability to unauthorized access. In today's digital world the simple detection and prevention of established worm and hacker activity is insufficient! Only Sana Security's adaptive profiling technology and Service Integrity's real time web services visibility offer you the complete protection required at a cost you can afford.

Stop security breaches before they occur leveraging real time visibility into auditable records of the underlying application interactions, and reduce costs of daily business operation and mandatory regulatory compliance. What you don't know *can* hurt you. Protect your business today! **For more information about Primary Response, contact Sana Security at 866-900-SANA.**

Primary Response

FEATURE	FUNCTION	BENEFIT
<ul style="list-style-type: none"> SanAPT technology core 	<ul style="list-style-type: none"> Learn, monitor and ensure proper operational states Prevent unauthorized activity by code or parties 	<ul style="list-style-type: none"> Reduce cost of security deployment and management Ensure business continuity and productivity. Protect critical information
<ul style="list-style-type: none"> Bootless Agents 	<ul style="list-style-type: none"> Allows for boot-less introduction and update 	<ul style="list-style-type: none"> Zero downtime
<ul style="list-style-type: none"> Self-Contained Agents 	<ul style="list-style-type: none"> Run with minimal (<5%) CPU utilization 	<ul style="list-style-type: none"> Reduce infrastructure cost and performance impact
<ul style="list-style-type: none"> Open-standard APIs 	<ul style="list-style-type: none"> Standards based integration and deployment with existing delivery and monitoring systems 	<ul style="list-style-type: none"> Reduce cost of deployment. Increase value of legacy systems Ensure ease of use

SIFT XML Visibility Software 2.0

FEATURE	FUNCTION	BENEFIT
<ul style="list-style-type: none"> SIFT Stream Sensor 	<ul style="list-style-type: none"> Monitor transactions, measure performance and report faults through multi-tier web services 	<ul style="list-style-type: none"> Improve visibility into operations and ensure business continuity and productivity
<ul style="list-style-type: none"> Distributed Logging Capability 	<ul style="list-style-type: none"> Capture and maintain logs of web and XML-based interactions 	<ul style="list-style-type: none"> Reduce cost of regulatory compliance and penalties
<ul style="list-style-type: none"> Web Service Autodiscovery 	<ul style="list-style-type: none"> Auto-discover web services 	<ul style="list-style-type: none"> Reduce cost of deployment
<ul style="list-style-type: none"> Dashboard Wizards 	<ul style="list-style-type: none"> Create intuitive graphical displays of real-time information 	<ul style="list-style-type: none"> Reduce costs of security management Faster problem identification/resolution
<ul style="list-style-type: none"> Open-standard APIs 	<ul style="list-style-type: none"> Standards based integration and deployment with existing delivery and monitoring systems 	<ul style="list-style-type: none"> Reduce cost of deployment Increase value of legacy systems Ensure ease of use