

Corporate Overview



SS8 is an established global provider of highly sophisticated communication interception and forensics solutions in the multi-billion dollar cyber security market. SS8's solutions allow law enforcement and intelligence agencies to conduct lawful interception and cyber monitoring of both circuit and packet-mode communications, extract related metadata, accurately reconstruct all targeted voice and data communications — telephone calls, emails, chat sessions, web surfing, and more — and provide comprehensive analysis of communication patterns. SS8 solutions enhance and contribute to personal safety and national security, all in accordance with local laws and standards.

COMPANY BACKGROUND

SS8 is a security software company that leverages its extensive knowledge of network operations, signaling, call flows and ever-changing internet protocols to accurately identify and extract targeted communication content and associated metadata from all wireless, wireline, broadband or cable networks. By combining these advanced interception techniques with extensive back-end forensics that provide comprehensive visualization, reconstruction and analytics of the intercepted data, SS8 has a true “end-to-end” interception and forensic solution for both network operators and law enforcement agencies.

Headquartered in the heart of Silicon Valley, SS8 has a global reach with over 250 deployments in more than 25 countries in the world's largest service provider wire-line, wireless, cable, VoIP and broadband IP data networks, supporting more than 500

million subscribers. SS8 has emerged as the world's leading provider of communication interception and forensics solutions that assist law enforcement and intelligence agencies around the world to effectively and efficiently monitor and analyze electronic correspondence in today's cyber world, leading to the apprehension of terrorists and criminals in the real world.

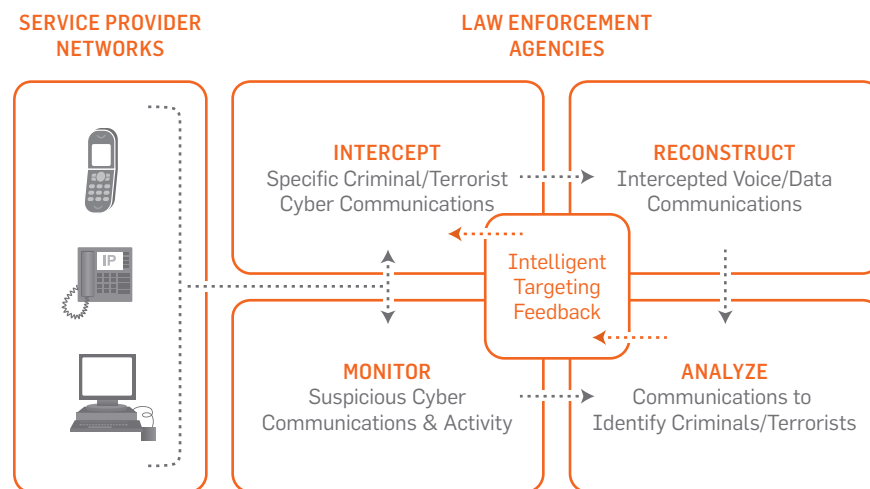
INTERCEPTION & CYBER SECURITY OVERVIEW

In today's cyber world, lawful interception and monitoring are critical to law enforcement or intelligence agency's ability to detect, prevent and prosecute terrorist and criminal activity. In most countries, support for interception and cyber security monitoring within the network has become a condition of the carriers' licenses and is an operational requirement as important as the security of the network itself. Effective solutions that address the needs of the law

enforcement and intelligence agencies globally are predicated upon the ability to achieve the following:

- » **Interception** – the successful real-time interception of a specific communication stream of a particular individual or group of individuals (targets that have been identified);
- » **Cyber Monitoring** – the proactive monitoring of specific behaviour within cyber communication streams which match law enforcement and intelligence agencies' specified characteristics;

- » **Visualization and Reconstruction** – the accurate reconstruction of intercepted voice and data communications and Internet activity including Web 2.0 applications such as webmail and chat;
- » **Analysis** – the generation and forensic analysis of metadata that provides a high level summary of all historical communication and Internet activity. Very sophisticated analysis functions, in turn, provide the law enforcement or intelligence agencies with intelligent targeting capabilities to identify new targets to provision for interception.



While the roll-out of IP-based communications has enabled many new services for customers and vastly reduced costs for carriers, it has created tremendous challenges for Law enforcement Agencies (LEA). In the old world of telecommunications, the path of a call was easy to follow and it was easy for investigators to select a point somewhere along the line to tap the call. However, all information transmitted over the Internet, including emails, web pages and voice calls, is segmented into small packets of data and sent across the IP network. The path one packet takes across an IP network may be different from the path of the next packet, and packets may arrive

at their destination out of order, or not arrive at all. Interception and monitoring solutions must be able to capture packets from both sender and recipient that form a communication stream, regardless of their route, reassemble them in the correct sequence, and format them for further analysis.

The emergence of Voice-over-Internet-Protocol (VoIP) telephony and other forms of electronic communication has been problematic for both the LEAs and the service providers trying to comply with national security laws mandating real-time interception and monitoring of voice calls. Therefore, there is

significant demand for new products that can keep pace with rapidly changing Internet protocols and applications to address the interception and cyber security needs of government regulators, national and local LEAs, intelligence agencies and communications service providers.

SS8 PRODUCT AND SOLUTION OVERVIEW

SS8's solution portfolio includes not only the network-based interception technologies required in service providers' networks but also the forensic tools employed by intelligence and law enforcement agencies to accurately reconstruct and analyze intercepted traffic. SS8's products include an intelligent mediation device for standards based intercept and delivery, scalable passive probes for traffic inspection and interception, and cutting edge software applications to record, monitor and analyze intercepted traffic.

Mediation & Control

Xcipio® is the Network Interception product that bridges communications networks and law enforcement monitoring centers. It provisions the intercepts, converts "raw" network traffic and signalling into a standard format, maps traffic to the appropriate intercept order, generates metadata and delivers it all in real-time to law enforcement.

Xcipio supports over 80 different network interfaces, allowing it to connect to a wide range of network equipment – wireline, wireless voice, wireless data, satellite, VoIP, WiFi, WiMAX, IMS, IP – all from a single software base. This kind of connectivity requires extensive knowledge of protocols, call flows and network operations in order to properly and accurately intercept communications networks. SS8's experience and expertise with these interfaces allows for a free flow of real-time information from the intercept access points in the network, through Xcipio and delivery to law enforcement.

Passive Probes

As service providers rapidly move towards all IP networks, they rely on a host of devices – SBCs, routers, switches, feature servers, gateways – to provide service to their subscribers. In some cases these devices include an active intercept capability, however in many cases this capability doesn't exist or isn't powerful enough to meet the needs of law enforcement today. For these situations the AXS family of probes is perfectly suited to perform passive intercept. Based upon purpose-built deep packet inspection hardware, AXS probes perform full line rate passive communication interception for today's 10 Gigabit Ethernet IP links and will accommodate the 40 Gigabit per second requirements of tomorrow's networks.

As a passive device the probe is independent of the network and doesn't impact its performance. And unlike network taps that only replicate electrical currents or beams of light, the AXS probe actually performs intense computations to examine and assess each packet. By inspecting both the header and the payload of the packets, the AXS probe can examine the contents, perform string matches, take action on the contents and correlate additional intercepts. All in an effort to make sure law enforcement gets the information they need.

Visualize, Reconstruct & Analyze

With the public moving to heavier and heavier use of services like email, on-line chat, ecommerce, VoIP communications and web browsing, law enforcement needs the capabilities of web reconstruction tools to analyze and reconstruct on-line Internet sessions. SS8's reconstruction and forensic applications are key components of SS8's end-to-end interception solution, enabling law enforcement to investigate today's complex Internet communication activities.

To date, the analysis of packets and IP sessions has required very technical end-users who need to understand the inter-workings of protocols, network equipment and web applications. They use time consuming packet analyzers that expose the framework of the packets and the content they carry, but don't recreate the user's on-line experience. While the packet headers and payloads are part of the investigative process, law enforcement is much more interested in the actual activities of the target (websites visited, contents of emails and email attachments, chat discussions, communication metadata, etc.) that SS8 can provide.

SUMMARY

SS8 stands uniquely positioned to provide communication interception and monitoring in any network environment. Our strength comes from our long-time relationships with telecommunications carriers and equipment manufacturers, law enforcement, our ability to assess any network to discover the best place to perform interception and monitoring, and being able to identify, analyze and reconstruct specific transactions amongst billions of daily communication interactions. We are meeting these challenges through continued innovation, expansion and investment in our product portfolio.



Some of the features listed may be under development. Please contact SS8 for feature availability schedule. This document does not create any express warranty by SS8 Networks or about its products or services. SS8 Network's sole warranty is contained in the written product warranty for each product. The end-user documentation shipped with SS8's products constitutes the sole specifications referred to in the product warranty. The customer is solely responsible for verifying the suitability of SS8's products for use in its network. Specifications are subject to change without notice.

Copyright © 2008 SS8 Networks, Inc. SS8, the SS8 logo, Xcipio, The Architects of Intercept and ServiceController are trademarks of SS8 Networks, Inc. All other trademarks mentioned in this document are the property of their respective owners.