TECHNOLOGY PARTNER BRIEF

Symantec Security Analytics + Ixia CloudLens

Seamless security intelligence and network forensics for modern hybrid environments

Symantec™

ixia
A Keysight Business

Partner Product: Ixia CloudLens

Symantec Product: Security Analytics

Extend complete, real-time visibility to the cloud

Security experts can't stop what they can't see—and that includes threats targeting applications in the cloud. They also can't wait for threats to take hold before they act.

Cyber security best practices require that you not only detect and respond to threats more quickly, but also eliminate vulnerabilities before an attacker finds and exploits them. This requires that you put threat intelligence, forensics, and analytics to work for you.

Symantec™ and Ixia™ have teamed to deliver the complete, ongoing visibility and insight you need to hone cyber security processes and shrink your company's attack surface. The joint solution makes your hybrid network and security infrastructures more intelligent, integrated, and automated—saving you time and effort and reducing your organization's cyber risk no matter the size of its network.

How it works

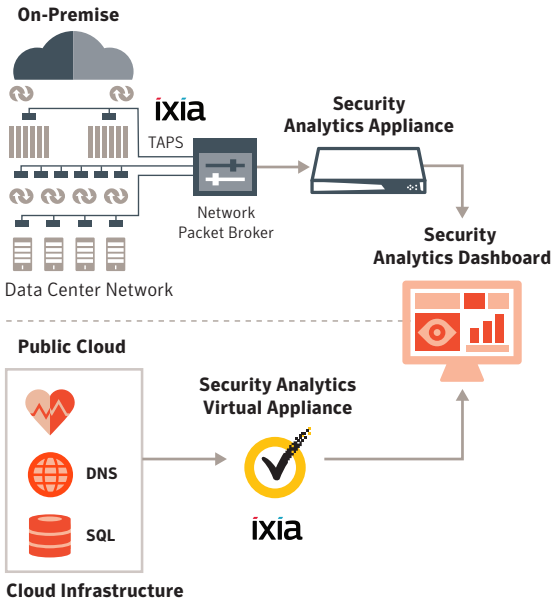
Symantec Security Analytics exposes the full source and scope of all threats and attacks no matter where they originate—across your own network or in cloud workloads—to effectively arm incident response (IR) teams and threat hunters against even the most sophisticated threats. Use the insights it generates to conduct network forensics faster and more thoroughly than was possible before.

Ixia's hybrid-network visibility solutions efficiently feed packet-level data to Security Analytics in real time, speeding troubleshooting and eliminating blind spots, even in public clouds. Ixia's Vision series of intelligent network packet brokers (NPBs), CloudLens™ products and services, and broad suite of network test access points (TAPs) capture and filter precisely the right data from your network and private or public clouds, and deliver it to Security Analytics.

Symantec Security Analytics improves forensics for faster response

Sophisticated threats demand a sophisticated, intelligent defense. Symantec Security Analytics gives you complete visibility and forensics capabilities—right out of the box—to thoroughly analyze prior attacks and react to security issues in real time. Once Ixia delivers the packets, Symantec turnkey, preconfigured appliances harness Security Analytics software to capture, index, and classify all network traffic (every

Seamless operation across hybrid (on-premises and cloud) networks.



In physical networks, Ixia's Vision NPBs aggregate, process, and feed traffic from multiple access points to Security Analytics appliances. In virtual environments, including cloud, Ixia's CloudLens visibility agents send traffic to Symantec's virtual appliances. In both cases, Security Analytics then analyzes the traffic and presents the results via its dashboard.

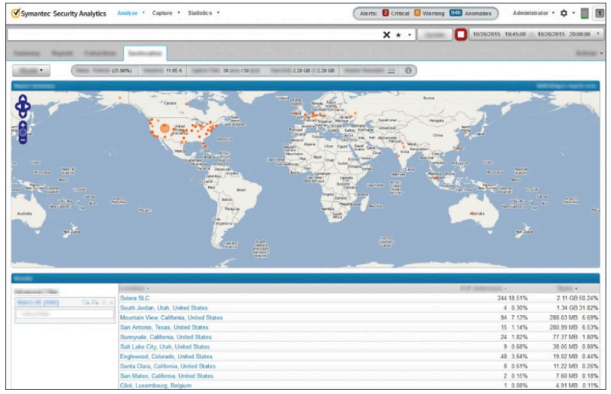
packet header and payload) and enrich it with the massive threat intelligence only Symantec provides. The appliances store data in a file system optimized to instantly retrieve, rapidly analyze, and completely reconstruct threat scenarios as you respond to incidents.

Gain complete hybrid network visibility by placing Security Analytics physical appliances anywhere in the network—at the perimeter, in the backbone or core, or at a remote link; place virtual versions on premises or in public and private clouds. Full, packet-level detail provides more insight than service provider logs, equipping Security Analytics to deliver clear, actionable intelligence you use in ongoing threat hunting and to swiftly respond to and resolve incidents. Options include:

- High-speed Security Analytics appliances—including storage and central management—with multiple interfaces and storage options (up to 1.5 PB on a single sensor)
- Virtual Security Analytics appliances with the same feature set as on-premises appliances
- Cloud security analytics for full visibility into, and better response to incidents in, your cloud workloads

To enable fast threat identification, Security Analytics uses:

- **Full network packet recording and classification**
- **Application classification through powerful deep packet inspection (DPI)**—2,800+ applications and thousands of descriptive, metadata attributes (content types, file names, etc.)
- **Real-time threat intelligence**—Via integration with Symantec Intelligence Services, the Symantec Global Intelligence Network—the world's largest civilian threat database—the Symantec Managed Adversary and Threat Intelligence (MATI) database, and numerous third-party threat reputation services
- **Anomaly detection**—Through advanced statistical analysis that identifies a baseline for your organization and then sends alerts for anything abnormal
- **Emerging, zero-day threat detection**—Uses automatic brokering of unknown files to Symantec Content Analysis or third-party sandboxes



See where all your traffic and threats are coming from

To enable fast incident response, Security Analytics uses:

- **Security events context**—More easily and quickly contain and remediate breaches.
- **Layer 2-7 analytics**—Engage in complete session reconstruction, data visualization, root cause exploration, timeline analysis, file and object reconstruction, IP geolocation, trend analysis, and anomaly detection.
- **Tight integration with a range of security technologies**—Work with security information and event management (SIEM) systems, next-generation firewalls (NGFWs), intrusion prevention systems (IPSs), malware sandboxes, and endpoint detection

Joint solution highlights

- Promotes rapid threat detection, forensics, and incident response
- Provides complete, scalable visibility across hybrid networks
- Ensures access to all data required from physical and virtual networks and public clouds
- Offers flexible implementation, easy operation, and high availability

About Ixia

Ixia, a Keysight Business, develops testing, visibility, and security solutions to strengthen applications across physical and virtual networks.

and response (EDR) solutions including Symantec Endpoint Detection and Response.

- **Context-aware security**—Pivot directly from any alert or log and obtain full-payload details and file reconstruction.

Ixia delivers the right data to the right tool at the right time

Ixia improves cyber security, operational efficiency, and control by giving you complete visibility into physical and virtual networks. This ensures each monitoring solution reliably receives exactly the right data it needs for analysis—efficiently and in real time—which improves network and security operations, speeds threat detection and response, and optimizes network and data center management.

Intelligent network visibility features include:

- **A broad range of physical and virtual TAPs**—Capture data anywhere in the network or cloud.
- **Intelligent NPBs**—Streamline, groom, and quickly deliver the right data to each inline or out-of-band monitoring tool.
- **Bypass switches**—Ensure 'fail open' capabilities for high availability.

TAPs, NPBs, bypass switches, and cloud visibility combine to deliver:

- **Access to all needed traffic**—Across physical networks, and private and public clouds
- **Reduced resource and bandwidth usage**—Traffic aggregated from multiple SPANs/TAPs in the network or cloud
- **Better coverage**—Data filtering and sharing from each TAP/SPAN to multiple analytics tools (eliminates TAP/SPAN shortages)
- **Improved tool utilization**—No duplicate and unwanted data, reducing the processing burden; load-balancing to distribute the workload
- **Easy setup**—Highly intuitive and intelligent interface (automatically resolves configuration issues)
- **High availability**—Automatic 'fail open' capabilities during planned and unplanned outages

Take the next step

Contact your Symantec representative to find out how Symantec Security Analytics and Ixia CloudLens provide advanced forensics and incident response for your hybrid environments.

About Symantec: Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

19D226351_SB_TIPP_IXIA_EN