ProtectWise™ + Ixia: Disrupting Network Security

THE CHALLENGE

Moving enterprise workloads to the cloud is beneficial, because it allows increased agility, flexibility, and scale. However, migrations can create stumbling blocks for security teams, because they lose access to packet-level data. The visibility that security and monitoring tools depend on no longer exists. This issue is worsened when multiple cloud platforms come into play. With the Ixia and ProtectWise joint solutions, busy information technology (IT) professionals do not have to tradeoff between the benefits of the cloud and the security and accuracy of their security and monitoring tools. With this joint solution, CloudLens provides access to packet data across multiple clouds and sends it to the ProtectWise Grid for complete visibility and detection of enterprise threats.

THE PROTECTWISE AND IXIA JOINT SOLUTION

ProtectWise and Ixia, a Keysight Business, are shifting network security to the cloud for complete visibility and threat detection across any cloud environment for faster incident response with two unique platforms:

- Running on demand and entirely from the cloud, the ProtectWise Grid is a new utility model for enterprise security that delivers pervasive visibility, automated threat detection, and unlimited forensic exploration.

Key Benefits

- Access to data across multiple cloud providers, such as AWS, Azure, Google Cloud, and more.
- Easy collection and visualization of NetFlow, metadata, truncated flows, and full-fidelity PCAP by protocol and application
- Long-term retention for retrospective analysis and correlated event creation
- Continuous, automated threat detection and analysis in real time and retrospectively
- Community-scaled threat intelligence and analysis
- Complete visibility to secure workloads in enterprise, cloud, or hybrid deployments
- Single data access layer across providers and operating systems (Windows or Linux)
- Rapid access to full PCAP for comprehensive forensic investigation and reduction of attacker dwell time
- Auto-scaling in the cloud—scaled visibility with instances
- The first service provider agnostic Visibility-as-a-Service (VaaS) solution for public, private and hybrid cloud, Ixia’s CloudLens can access and filter network traffic to send to The ProtectWise Grid.

Together, these solutions give security teams a single place to get end-to-end visibility across enterprise, cloud, and hybrid environments.

**RECORD EVERYTHING**

The ProtectWise Grid creates a lasting high-fidelity memory of enterprise activity on any network segment. It captures, optimizes, and stores full-fidelity traffic into a single haystack in the cloud and retains it for as long as needed to give you the ability to know whether threats have ever impacted your organization.

The CloudLens platform ensures that The ProtectWise Grid receives all relevant packet data, across all cloud providers and platforms, running with any operating system (OS). With this data, The ProtectWise Grid delivers pervasive visibility and advanced multi-stage attack detection in real-time and retrospectively.

Additionally, The ProtectWise Grid enriches security data with the output of analytics models trained on billions of attributes and a range of indicators, and provides search at unparalleled speeds. As a result, security teams can intuitively make sense of massive volumes of historical data to hunt for and investigate threats through all stages of the Cyber Kill Chain.
SEE EVERYTHING

The ProtectWise Grid uses a finely tuned hierarchy of expert systems to analyze network traffic and provide threat detection that stand-alone appliances cannot. Cloud economies of scale enable The ProtectWise Grid to apply a range of techniques in parallel on massive amounts of live data to detect known and unknown threats in real time. These techniques include machine learning, intrusion detection, retrospective analysis, customer-specific event modeling, and heuristics. In the process of automatic retrospective analysis, The ProtectWise Grid continuously evaluates historical data against the latest threat intelligence to detect prior exploits of newly discovered vulnerabilities and reduce attack dwell time. This means you can measure the full impact of attacks going back to weeks, months, or even years of past data.

The ProtectWise Grid correlates intelligence from proprietary research, flow-based traffic algorithms, and multiple third-party intelligence feeds. Collective correlation of security events across customers creates a feedback loop that eliminates noise in the security environment. It is a shared brain that constantly learns and adapts to reduce alarm fatigue caused by false positives.

The Ixia CloudLens platform provides The ProtectWise Grid with a single source of network traffic across all modern environments. This integration enables you to scale your business operations securely without compromising on visibility, retrospection, or threat detection. CloudLens offers unprecedented visibility across all of your public, private, and hybrid cloud environments. The platform provides a cloud-based framework that scales to meet the elastic demands of public cloud customers in a multi-tenant, self-serve model. With CloudLens, deploying traffic monitoring solutions in the public cloud occurs in a matter of minutes, not hours or days.

Cloud resources are constantly changing. CloudLens scales your cloud network visibility dynamically without adding any automation or infrastructure management burdens. Its powerful embedded automation capability helps analysis tools adapt to changes in demand or failures automatically without needing operator-in-the-loop actions. Virtualizing analysis tools inside the cloud provides significant bandwidth savings if you do not want to tunnel your virtual data back to a centralized physical analysis tool.

The ProtectWise Grid also integrates with a variety of security products, including firewalls, gateways, endpoints, and security information and event management (SIEM) to add context for streamlined incident response.
EXPERIENCE IMMERSIVE SECURITY

The ProtectWise Grid enables analysts to cut through noise via a stunning graphical user interface. It distills massive data sets into an intuitive experience, enabling analysts to efficiently interact with petabytes of data and make precise, more informed security decisions. This one-of-a-kind presentation layer elevates the incident response and threat hunting skills of analysts of any experience level. Get an at-a-glance view of your entire network, see events by kill chain stage across past and current timelines, and more. Easily pivot into a deeper forensic workbench that includes deep packet inspection (DPI), replaying policies for applications and protocols, and packet capture (PCAP) download for more advanced threat hunting.