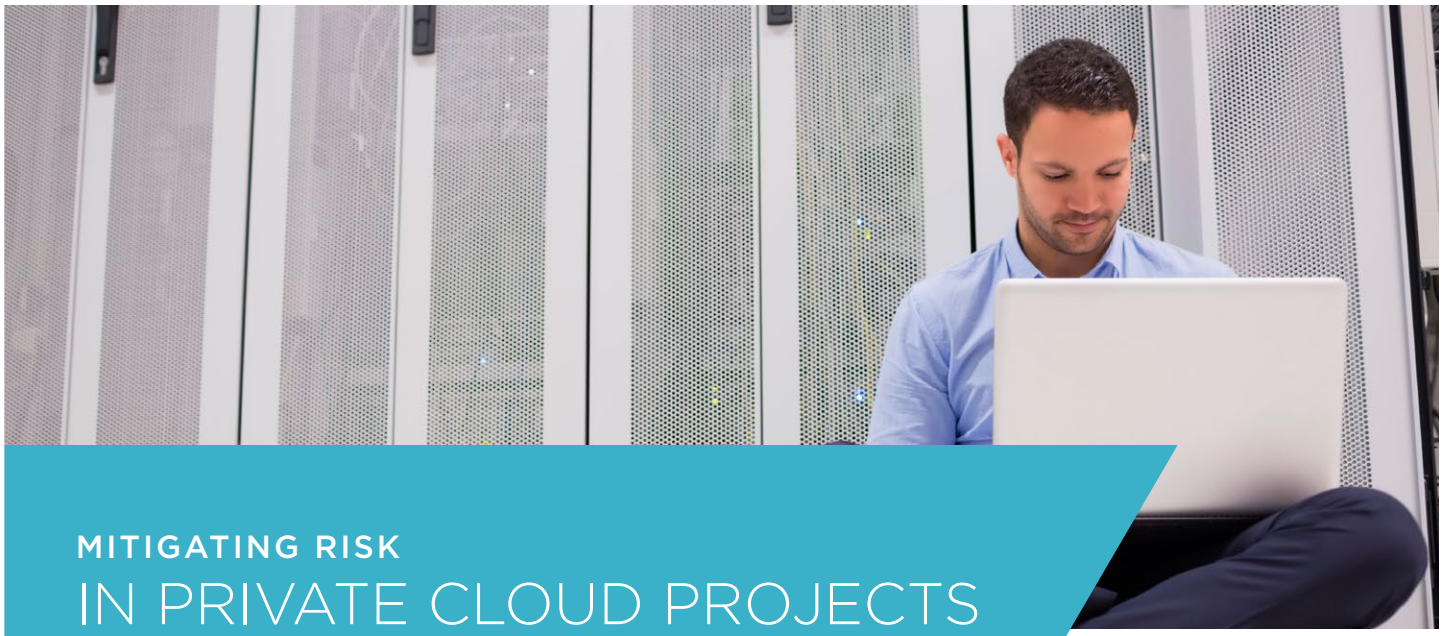
QUICK GUIDE



MITIGATING RISK
IN PRIVATE CLOUD PROJECTS

Ixia has extensive experience helping organizations of all sizes test and validate their private cloud implementations. The key to mitigating risk is a continuous testing and remediation process including the following steps

First Step	Develop the next iteration of your private cloud infrastructure and identify what real usage of the cloud will look like—how many users, what types of applications, etc.
Second Step	• Emulate traffic: "the good, the bad, and the ugly" • Artificially generate good traffic you expect from your users. • Generate bad traffic, such as that caused by malware and security attacks. • Generate "ugly" traffic—unwanted traffic originating from proxy servers, content caching, and apps not permitted for use in your organization. • Monitor how your infrastructure and applications respond.
Third Step	**Remediate:** Identify problems, such as performance issues and security vulnerabilities, and make the necessary changes on your staging environment. Run the tests again to make sure all is okay.

The key to testing on-demand is the second step—emulation. If you can realistically emulate traffic on the cloud, you can perform accurate tests at any stage of your development process.

915-8099-01 Rev A

Fourth Step	Deploy: Push your latest version to production and re-run the tests to make sure you have a solid baseline with none of the previously-discovered issues.
Fifth Step	Shakeup: Periodically re-run the same tests and see if everything still holds up. If problems are discovered, have development resources in place to prepare a quick patch so you don't have to wait for the next release.

To implement a continuous testing and remediation process, you must have the ability to perform realistic tests of your cloud, even when there is little or no production traffic. For example, when testing on a staging environment, or on a real production environment on a weekend, you must be able to emulate realistic network traffic to really see how systems behave. In addition, you must be able to test anomalous types of traffic like security attacks and malfunctioning network devices.

The key to testing on-demand is the second step—emulation. If you can realistically emulate traffic on the cloud, you can perform accurate tests at any stage of your development process.

MITIGATING PRIVATE CLOUD RISKS WITH TRAFFIC EMULATION AND ACTIVE MONITORING

The following summarizes how you can use **Ixia solutions** to mitigate some of the main risks to your private cloud implementation.

IXIA SOLUTION FOR SECURITY BREACHES

BreakingPoint® can simulate the entire "kill chain," representing the movement of threats through your private cloud infrastructure. This helps you assess the efficacy and performance on your security infrastructure, teams, and policies. Ensure your security measures scale and respond appropriately as you dynamically create VMs to address application requirements and changing user workloads.

Cyber Range is a training solution in which Ixia experts help you conduct a full-scale "military exercise" with blue team and red team to see how your team and security systems will react in case of a real security attack.

Ixia Threat Intelligence Gateway - ThreatARMOR™ acts as a gateway that blocks known bad IP address traffic, blocks bots inside your network from communicating out, and eliminates network traffic from countries you do not trust. By eliminating known bad and unwanted traffic, it reduces the amount of data which needs to be inspected by in-line security tools by up to 35%, and reduces the volume of security alerts by up to 80%.

PERFORMANCE PROBLEM SOLUTIONS

IxNetwork® helps you actively test the scale and capacity of infrastructure elements, such as switches and routers, by emulating different types of traffic. This makes it easier to right-size your investment early in a private cloud project. If you are implementing software-designed networking (SDN) or network functions virtualization (NFV), IxNetwork can also test virtualized or software-controlled network elements.

IxLoad® measures key performance and Quality of Experience (QoE) indicators for applications and multimedia services, such as Voice over IP (VoIP) and Over the Top Video (OTT). It provides scalable, stateful application emulations, which provide the data you need to make quick decisions about technologies you implement in your private cloud. IxLoad makes it easy to compare competing products and technologies, using data-driven PoCs, and identify QoE degradation before they are experience by users of your cloud infrastructure.

BreakingPoint provides simulation of real-world applications and security threats for the purpose of performance and security testing. Its elastic deployment model allows you to simulate enterprise-scale traffic and realistic threats to verify the resilience of your security setup.

IxChariot® lets you create a testing "endpoint" within any part of your private cloud infrastructure—hypervisor, machine instances, user devices including mobile phones and tablets, and even servers in different data centers. You can then actively emulate traffic and get an on-demand network performance assessment between any or all of the endpoints.

SOLUTIONS FOR LACK OF VISIBILITY

Ixia provides the capabilities—and intelligence—to improve the effectiveness of your security appliances and the efficiency of your infrastructure with the Ixia IxVision architecture and the Ixia Security Fabric. Ixia's IxVision makes applications and networks stronger by delivering end-to-end visibility that removes network blind spots across your private cloud infrastructure, as well as boosting the power of existing security tools.

Companies use Ixia's IxVision visibility architecture to:

- Implement proper data access capabilities across physical, virtual, and cloud networks to capture better monitoring data for faster mean time to repair and resolution
- Improve insights they get from their out-of-band monitoring tools
- Proactively reduce performance problems, monitor SLA's, and improve customer experiences

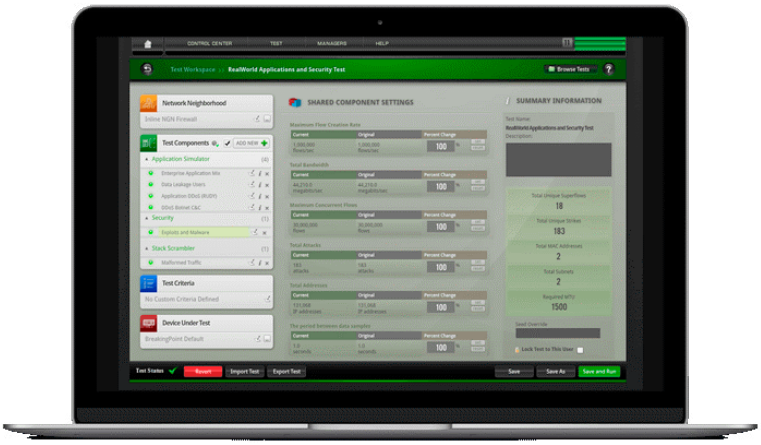
- IxVision bolsters enterprise private cloud performance by providing complete data access, resiliency and intelligent data processing with Ixia taps and network packet brokers (NPBs). This ensures data routing, filtering, and load balancing to all out-of-band tools. When NPBs are used, you create a smart duo that can see and inspect network packets and route them to the most appropriate appliance. NPBs help you zero in on what is important and strip away unnecessary detail. Ixia's application and threat intelligence processor (ATIP) identifies applications and geolocation to help you make intelligent decisions about how to best manage your traffic pass/fail with alerts to existing network management system (NMS) or remediation systems.

DATA LOSS

BreakingPoint can help you secure your cloud against data exfiltration. You can emulate traffic that includes sensitive data, such as social security numbers or confidential documents, and see if it's possible for such traffic to exit your network. This will test if your data leakage prevention policies are actually working.

BUILDING BLOCKS OF IXIA'S PRIVATE CLOUD SOLUTION

BREAKINGPOINT



BreakingPoint can help you secure your cloud against data exfiltration.

- Emulates more than 300 real-world application protocols
- Allows for customization and manipulation of any protocol, including raw data
- Generates a mix of protocols at high speed with realistic protocol weight
- Supports more than 36,000 attacks and malware
- Delivers all types of traffic simultaneously from a single port, including legitimate traffic, Distributed Denial of Service (DDoS), and malware
- Bi-monthly updates ensure you're up-to-date on the latest applications and threats

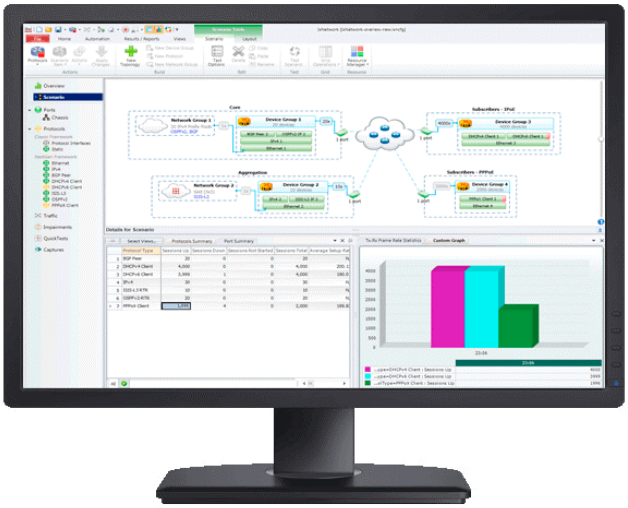
Combined with PerfectStorm hardware, BreakingPoint can:

- Perform massive scale, high-fidelity emulations of security attacks (e.g., large scale DDoS)
- Massive scale emulations of good user traffic (e.g., millions of web users in a traffic spike)
- Emulate encrypted connections with built-in, hardware-based acceleration for Internet protocol security (IPsec) and Secure Sockets Layer (SSL)

BreakingPoint Virtual Edition (VE):

- Able to run seamlessly as part of your deployed network functions virtualization (NFV) architecture
- Rich application program interface (API) access enabling automated testing in the continuous integration and continuous delivery (CI/CD) pipeline
- Run realistic user testing with every deployment to a testing or production environment

IXNETWORK AND IXLOAD

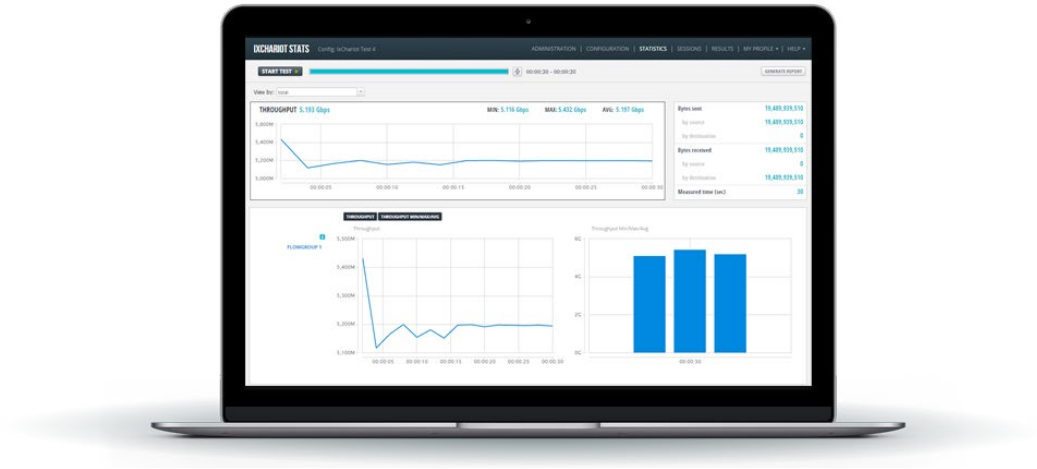


Real-time insights into QoE—the only solution on the market that can model dynamic user behavior

- IxNetwork performs realistic performance testing by generating terabytes of data and analyzing up to 4 million traffic flows simultaneously
- IxLoad can emulate web, video, voice, storage, virtual private network (VPN), and wireless traffic
- End-to-end testing of converged application delivery infrastructure and services
- Real-time insights into QoE—the only solution on the market that can model dynamic user behavior
- Available as a virtual software-based unit that can be deployed within your cloud infrastructure, or hardware-based to enable testing physical network ports and larger traffic scale

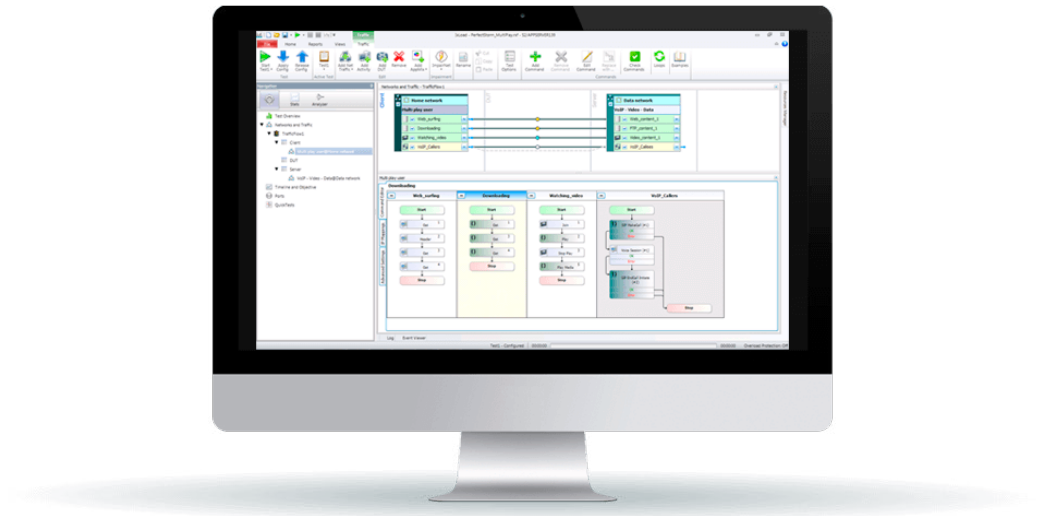
- Test coverage from 1G to 400G Ethernet, comprehensive protocol coverage for routing/switching, MPLS, broadband, industrial Ethernet (IE), data center networking, and software-defined networking (SDN)
- Delivers end-to-end test system automation

IXCHARIOT



- A powerful assessment tool that uses software agents to emulate application traffic between any two points in your cloud or other integrated systems
- Instantly assesses network performance, including wireless performance and geo-location
- Performance Endpoints run on mobile, PC, Mac, or in any hypervisor
- Application emulation and key performance metrics, including throughput, packet loss, jitter, delay, MOS, and application latency
- Trusted tool for both private virtual and public cloud infrastructures

VIRTUAL TAPS AND PACKET BROKERS



- Bridges the physical and virtual, so that you can monitor the virtualized network with your existing set of tools.
- Capable of capturing and then sending inter-VM traffic of interest to the tools that are already monitoring your physical network
- Enables monitoring for security and compliance in virtualized environments
- Applies existing physical monitoring tools, processes, and procedures to the virtual network
- Aggregates virtualized traffic, filter and grooms to remove redundant information, load-balances and passes traffic on to external tools for closer inspection

SEE FOR YOURSELF HOW IXIA HELPS MITIGATE PRIVATE CLOUD RISK. SCHEDULE A DEMO.

WORLDWIDE HEADQUARTERS

26601 W. Agoura Road
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800

(FAX) 1.818.871.1805

www.ixiacom.com

EUROPEAN HEADQUARTERS

Ixia Technologies Europe LTD
Clarion House, Norreys Drive
Maidenhead SL64FL
United Kingdom

Sales +44.1628.408750
(Fax) +44.1628.639916

ASIA PACIFIC HEADQUARTERS

101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
(Fax) +65.6332.0127