WHAT YOU CAN DO TO
Strengthen Cloud Security

INTRODUCTION
The agility and cost savings of cloud technologies have helped our digital economy grow and thrive. Cloud providers take care of security for the physical data centers and server hardware that cloud services run on, but cloud users are still responsible for protecting their own virtual machines and applications. Security is a shared responsibility that requires constant attention and investment by both providers and users. So, what can enterprises do to strengthen security in the cloud?

THE CLOUD ATTACK SURFACE
Once an enterprise begins using public cloud infrastructure, the potential attack surface expands to include attacks on the cloud provider, as well as the provider’s other clients. Most providers employ strong security measures, but they still face the same threats as traditional networks—the only difference is that, as a customer, you do not have as much control over what is done to safeguard against these threats. The scope and monetary value of a successful attack on shared infrastructure can be extremely attractive to hackers and cyber terrorists.
The most serious attacks include:

- **Data breaches**: If your cloud provider suffers a data breach, you may suffer exposure of sensitive customer information that could lead to serious financial or legal consequences, as well as damage to your brand.

- **Denial of service**: These attacks take advantage of vulnerabilities in Web servers, databases, or other resources to disrupt a cloud service, sometimes as a distraction while another attack is taking place.

- **Insecure interfaces**: The connectors of digital services are the most exposed part of any system and are frequently targeted. If the mechanisms used to manage systems, move data, and conduct admin tasks are compromised, an attacker can get access to almost anything.

- **System vulnerabilities**: In multitenant computing, vulnerabilities in one environment can lead to an attack on an adjacent tenant with shared resources. The source is often poorly implemented or unpatched software.

**YOU NEED YOUR OWN SECURITY MONITORING SOLUTIONS**

Complex multi-cloud environments have many potential vulnerabilities that attackers can exploit. The data breaches we see in the press remind us that building an impenetrable environment is not realistic, and we cannot rely solely on cloud providers to handle our defense. Security in the cloud is a shared responsibility between the cloud provider and the user—and enterprises need to take ownership by deploying data access and security solutions, as well as testing those solutions to make sure they provide adequate protection.

In some organizations, the pressure to achieve the cost advantages and speed associated with cloud deployments or having a “cloud first” mandate can divert attention away from the basics of security enforcement. For example, data breaches reported in 2017 at Dow Jones and Verizon were attributed to faulty implementation of Amazon Web Service (AWS) security options. Persistent, multi-layered security is, therefore, the best way to defend our enterprises against security breaches, data loss, and business disruption.

---

SECURITY DEPENDS ON FULL VISIBILITY OF DATA

Most organizations invest considerable time and money implementing sophisticated and advanced security solutions to examine data packets and identify threat signatures or suspicious behavior. Unfortunately, they do not always ensure these critical security solutions have all the data they need to perform effectively. Traffic in the cloud is not as easily observed as traffic moving between physical devices in the data center. To be effective, your security systems must have full transparency to every data packet that flows in your organization, including metadata about that packet. This type of data is not readily available from cloud providers, and organizations need alternative methods to fully expose data in the cloud. This is the role of a cloud visibility platform.

DEPLOY EVERY CLOUD WITH VISIBILITY

The most straight-forward way to get complete transparency to cloud data is to include visibility automatically as a component of each cloud instance or virtual machine deployed. A cloud visibility platform gets access to data in public clouds by embedding an agent or container-based traffic sensor inside each cloud instance the user deploys. The sensor makes copies of all the data passing through the cloud instance. In private clouds, a virtual network tap inside the hypervisor performs a similar function. In both cases, visibility scales automatically every time a new cloud instance or virtual machine is deployed.

The mirrored traffic can be filtered and sent to a cloud visibility platform that aggregates packets from multiple sources, processes as necessary to remove duplicates and unnecessary packet data, pinpoints traffic of interest, and delivers it to security solutions located in the cloud or on-premises. A centralized, Web-based interface is used to manage the visibility platform across the entire enterprise (see Figure 1). The Ixia CloudLens visibility platform can aggregate data from multiple cloud providers to simplify visibility management. Filtering policies are configured using simple drag-and-drop technology; no programming or training is needed to get the solution up and running.
ENSURE VISIBILITY IS SCALABLE AND RESILIENT

**Deploy visibility that is as flexible as your clouds**

Once deployed, your cloud visibility platform becomes a key component of your security system. It must scale along with your clouds, so there are no blind spots that are unexamined by your security solutions. Ixia CloudLens is a cloud-native and container-based solution that is completely distributed, so it scales without limit, just like your clouds. Integration and pre-validation with popular cloud security solutions means that data begins flowing to your tools automatically, with no need for manual intervention or the risk of configuration mistakes.

Your visibility platform must also be resilient, so there are no disruptions in monitoring that give intruders an opportunity to act. This means there can be no single point of failure in the components that collect, filter, and distribute data to your security solutions. A visibility platform that relies on a single, monolithic processing engine—common in data center solutions retrofitted for the cloud—is dependent on that component to provide data access and is limited by the capacity of that engine. With a centralized processing engine, resiliency requires having an expensive backup system available to take over in case of an outage. In contrast, a cloud-native visibility platform is naturally resilient, since processing is spread among all the cloud and virtual machine instances. If any component stops working and sending data, another is automatically spun up to replace it, while all other images are unaffected.

**OPERATING EFFICIENCY IMPROVES SECURITY MONITORING**

In both public and private clouds, a visibility platform makes monitoring more efficient and cost-effective by sorting and filtering the large volume of raw traffic, stripping away unnecessary data, and pinpointing the information that is relevant to each of your security solutions. Intelligent filtering decreases overall workload, reduces the potential for congestion, and can delay the need to increase security tool capacity.

**APPLICATION LAYER FILTERING**

While filtering packets based on ports, Internet Protocol (IP) addresses, or protocols is common, there is additional value in being able to filter and load-balance data on the basis of Layer 7 characteristics, such as application type, access device, operating system, geography, or other customized parameters (see Figure 2). The more granular the data provided, the more the security algorithms have to work with. Ixia CloudLens is the only visibility platform currently providing this level of data access.
SINGLE HYBRID VIEW

Hybrid cloud environments, where data may move between public and on-premises infrastructure, can be more complex to monitor. A cloud visibility platform gathers data from both environments, filters it, and delivers it to security solutions, whether they are located in the cloud, are software-based and running on-premises, or are highly specialized hardware appliances in the data center. The cloud-based interface of Ixia CloudLens, for example, provides a single pane of glass for managing filters across both environments and any public cloud.

APPLICATION IDENTIFICATION

ALL-CLOUD WITHOUT BACKHAUL

Cloud computing is cost effective until you want to take data out of the cloud and transport it back to the data center. Providers generally charge a steep price for what they call data exfiltration. To save money, enterprises may choose to use cloud-based security monitoring solutions. It can be less expensive and faster to deliver filtered data to a solution hosted by the same cloud provider.

FUTURE FLEXIBILITY

A visibility platform filters traffic from multiple sources using consistent rules and provides the flexibility to support a wide variety of security monitoring solutions—including open source tools and tools that are not even created yet.

REDUCE RISKS WITH PROACTIVE SECURITY TESTING

Companies focused on risk reduction use testing to validate their security solutions are working as desired and not diminishing network and application availability. With testing, you can simulate network traffic across protocols and applications, scale traffic volume with bursts of activity, and watch what happens on your most trusted security devices. Test results help you understand how your security functions under attack, what level of service is provided during an attack, and long it might take to recover. Some companies run these tests routinely when evaluating any new security solution.
SECURITY TEST PLATFORMS.
An integrated test platform gives users more granular control over test scenarios to more accurately reflect real-world network conditions. Advanced testing features will increase the insight you get from testing.

- **Hardware-based load modules** allow multi-terabit emulation of complex traffic, including SSL-encrypted traffic and high-volume bursts of cloud activity to observe how congestion affects latency, throughput, and concurrent processing.

- **Flexible, user-controlled simulations** let you specify a customized mix of traffic with hundreds of real-world application protocols from a single port to validate the stability, accuracy, and quality of your cloud environments.

- **Integrated threat intelligence** injects thousands of actual attacks, malware, and botnet activity into the testing mix. Some platforms provide specific DDoS attack simulations to prepare for one of the biggest and most common threats to any organization.

- **Integrated traffic recording** lets you include copies of production network traffic in your simulations to further increase the relevancy of testing results.

- **Pay-as-you-go option** matches the needs of today’s networks by eliminating the need for capital investments in testing infrastructure.

**SUMMARY**
Moving to public cloud eliminates the burden of operating information technology (IT) infrastructure, but organizations are still responsible for the security, availability, and performance of their services, no matter whose equipment they run on. Therefore, cloud adopters must make sure their security solutions have all the data and metadata they require to defend against security breaches, data loss, and business disruption. Automatically deploying each new cloud with total visibility to the data inside is the best way to ensure no blind spots exist. A cloud visibility platform also makes security monitoring more cost efficient by filtering the large volume of raw traffic to pinpoint the relevant data. Security risk can be further reduced by pro-actively validating your security architecture using cloud-scale traffic simulation with a realistic mix of protocols, applications, malware, and attacks.