



Lack of Visibility Drives Public Cloud Security Risk

REPORT

Spending on cloud computing is growing faster than ever before. The worldwide public cloud services market revenue is projected to grow 18.5 percent in 2017 to total \$260.2 billion, up from \$219.6 billion in 2016, according to Gartner, Inc.¹. This rapid growth of cloud adoption has driven increased interest in securing data, applications, and workloads that now reside in a cloud-based environment. For companies that are looking to migrate to the cloud, it has become clear that the first thing they need to think about is security and data visibility to ensure their cloud services are managed in a secure way.

Ixia recently commissioned Dimensional Research to conduct a survey to measure security and visibility into applications and data in public or private cloud environments. The survey found that more than 90 percent of IT professionals responsible for their company's public and private cloud environments are concerned about data and applications security in the cloud.

The results in the private cloud improve slightly with 82 percent of IT professionals concerned with security and data privacy in the private cloud. Data privacy and compliance, security attacks, loss of control over location of data, and achieving full data visibility were slated as the top security concerns for IT professionals.

1. Gartner, Inc. Press Release, "Gartner Forecasts Worldwide Public Cloud Services Revenue to Reach \$260 Billion in 2017," October 12, 2017



With nearly uniform concern around security and data privacy in the public and private cloud, the results make it clear that the need for visibility in the cloud is not just a trend, it's a must-have for organizations of all sizes.

How concerned is your company about maintaining data and application security in your PUBLIC cloud environments?

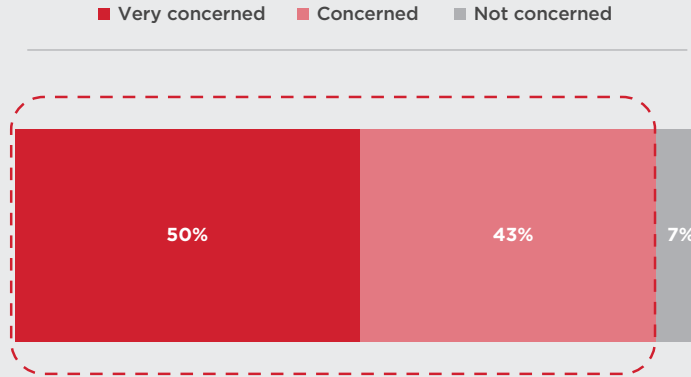


Figure 1.
93% concerned about data and application security in public clouds

NEARLY ALL COMPANIES ARE CONCERNED ABOUT SECURITY IN THE CLOUD

The security concerns these companies are facing are well founded. Nearly 9 out of 10 respondents indicated their companies have at some point seen a direct business impact from a lack of visibility into public cloud traffic. Companies experience delays in troubleshooting application and network performance issues, as well as delays in resolving security alerts stemming from a lack of visibility. These problems lead to long term issues like a missed security threat or attack - making a lack of visibility the heart of the cybersecurity problem.

Which of the following issues has your company experienced from lack of visibility into PUBLIC or PRIVATE cloud data traffic?

Select top three

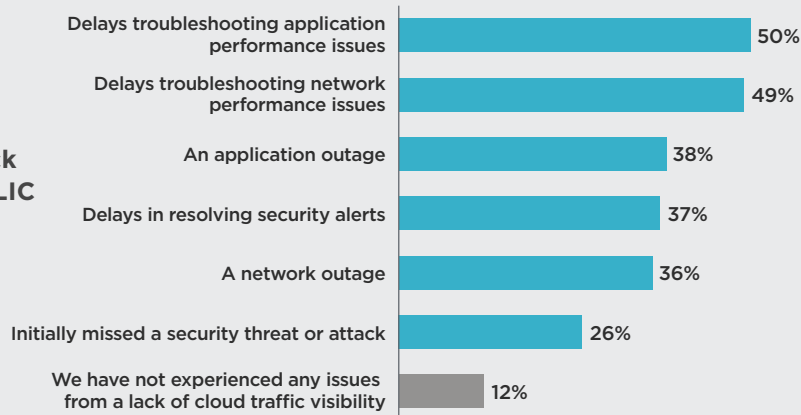


Figure 2.
88% experienced issues from a lack of visibility into public cloud data traffic

These concerns are rooted in the fear of becoming the next security breach headline. Unfortunately, few IT administrators have an accurate picture of what's going on inside the network, and lack the automated visibility and analytics tools that can quickly identify and act on threats. Network visibility tools help these professionals discover network vulnerabilities and user behaviors that were never before realized, and in turn help to bolster security policies.

The security breaches that result from lack of visibility into clouds can cause customers to avoid or mistrust cloud-based services and applications. Total cloud visibility and constant monitoring can restore customer confidence and even become a differentiator for companies that go the extra mile to protect customer data and transactions.

What are your company's top priorities related to your PUBLIC cloud environments over the next 12 months?

Choose up to 3

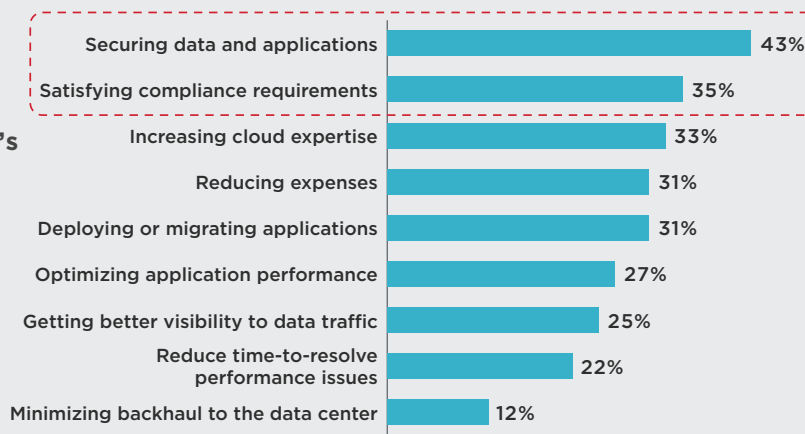


Figure 3. Security and compliance top public cloud priorities

FINDING THE RIGHT BALANCE FOR YOUR CLOUD ENVIRONMENT

Cloud computing is not a simple IT initiative – the move to a cloud environment brings with it a loss of control over the underlying infrastructure that introduces risk to the information being stored there. Reflecting this reality, the top priorities of public cloud users are security focused.

While securing data and applications may take precedent with 43 percent of respondents stating this as a top priority, satisfying compliance requirements is not far behind, with 36 percent of respondents stating this as a top priority in the cloud. Compliance is a large area of focus for companies in highly-regulated industries such as financial services and healthcare, partially in wake of the long-awaited General Data Protection Regulation (GDPR) coming into force on May 25, 2018.

Organizations must take control of their data to align with this focus on security and compliance, as there is no other way to be more accountable to your customers than through full visibility.

METHODOLOGY

Ixia, a Keysight Technologies business, commissioned Dimensional Research to conduct this survey in the field. A total of 353 IT professionals in companies larger than 1000 employees with responsibilities for cloud deployment about security and visibility into applications and data in public or private cloud environments were invited to participate in the survey which was administered electronically. Participants were offered a token compensation for their participation.



IXIA WORLDWIDE

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

IXIA EUROPE

Clarion House, Norreys Drive
Maidenhead SL64FL
United Kingdom
Sales +44.1628.408750
(Fax) +44.1628.639916

IXIA ASIA PACIFIC

101 Thomson Road,
#29-04/05 United Square,
Singapore 307591
Sales +65.6332.0125
(Fax) +65.6332.0127