The Business Case for Sophos Cloud Optix:

Public Cloud Visibility and Threat Response

The Potential Cost of Errors in the Public Cloud

Protection from the latest generation of public cloud cyberattacks and regulatory compliance penalties requires a new level of visibility and security automation. The thousands of data storage service breaches publicized in the news have raised awareness of vulnerabilities caused through misconfigured "public" access, but cloud security breach tactics go far beyond this.

MISCONFIGURED DATA STORAGE SERVICES

According to the 2019 Verizon Data Breach Investigations Report[1], insider-initiated incidents now account for 34% of data breaches. Accidental data exposure through misconfigured storage services continues to plague organizations, with reports of airlines exposing the data on millions of passengers, and of leaked data from fortune 100 customers, including internal business documents, system passwords, sensitive employee information.

OVER-PRIVILEGED IAM ROLES

Data storage services with "private" mode enabled are still not safe. Recent high-profile attacks are said to have exposed 140,000 Social Security numbers and 80,000 bank account numbers, exploiting over-privileged IAM roles and instance permissions through a flaw in the WAF. These attacks retrieve IAM credentials via an SSRF vulnerability to access data and files in "private" mode.

ELASTICSEARCH EXPOSURES

Elasticsearch services make it easy to store, search and analyze large volume of data, and that makes it a prime target for cybercriminals. But with their "public" mode, Elasticsearch domains leave data exposed to unsigned requests made to these resources (ES clusters). Examples of unprotected Elasticsearch clusters include the personally identifiable information of more than 20 million Ecuadorian citizens, and over 20 million tax records belonging to Russian citizens.

THE KEYS TO YOUR KINGDOM

Virtual hard drive snapshots and database services can be the keys to your kingdom. While MongoDB and any database running on a virtual network has potential to have open ports to the public internet, recent attacks have seen popular services such as Amazon Relational Database Service (RDS) and Amazon Elastic Block Store snapshots (EBS) compromised through a "public" mode. Recent reports have highlighted the scale of the problem with approximately 1,250[2] EBS snapshots of virtual hard drives found to be "public" and unencrypted for the world to see across Amazon cloud regions.

HIJACKED CLOUD RESOURCES

Hijacking cloud resources to mine for cryptocurrency is a fast-growing threat for enterprises. Whether exploiting containers without password protection, as in the as in the case of a high-profile car manufacturer, or illegally provisioning instances using stolen credentials, these attacks conceal their activities from conventional firewalls by hiding the IP addresses of their mining programs behind a content delivery network, and throttling mining software to avoid high-usage-detection systems, leaving organizations with a large invoice for cloud usage.

The Need for Public Visibility and Threat Response

As organizations look to expand in the cloud, take advantage of top growing services in serverless, containers, and Kubernetes, or adopt methodologies such as CI/CD and DevOps, they should be aware of the techniques used by cybercriminals to targeted hidden gaps in security responsibilities, misconfigurations, user access roles, and permissions.

The secret to effective cybersecurity across dispersed environments in Amazon Web Services, Microsoft Azure, and Google Cloud Platform is to improve your overall security posture, ensuring your architecture is secure and configured correctly, and that you have the necessary visibility into your architecture, and importantly, into who is accessing it.

Public Cloud Security Must Evolve

To ensure protection, organizations should evaluate security solutions able to wrap security, compliance, and configuration monitoring controls around all cloud assets, as well as the CI/CD pipeline, to protect against the range of attacks at work.

Sophos Cloud Optix security and compliance services enables organizations to accurately visualize and secure cloud infrastructure continuously and confidently. This enables teams with a single view of security posture across Kubernetes clusters, Amazon Web Services, Microsoft Azure, Google Cloud Platform, and Infrastructure-as-Code environments to:

- Automatically detect valuable cloud assets across multi-cloud estates
- Provide a full inventory and topology visualization of cloud infrastructure
- Combine the power of AI and automation to identify hidden configuration vulnerabilities and enable traceability of unusual user access, API calls, and changes in configuration
- Apply root cause analysis, risk-based prioritization, and remediation support to security and compliance alerts
- Integrate with the CI/CD pipeline by automatically scanning infrastructure-as-code templates merged to source control management, with pipeline deployment based on Cloud Optix assessment results
- Enable security, development, operations, and compliance teams with the tools to automate security and compliance checks, improve collaboration and shrink response times
- Continuously map compliance and security best practice standards to cloud infrastructure, with audit-ready reports available on demand

Selecting the Right Approach

To provide you with a clear picture of the benefits and considerations when positioning or implementing a cloud visibility and threat response service such as Cloud Optix, Sophos interviewed a range of CISOs, cloud infrastructure specialists, and DevOps professionals and found they were evaluating two main approaches.

- Development of in-house solutions utilizing cloud provider APIs
- Investment in security solutions from dedicated providers

CONSISTENT REQUIREMENTS

The challenges and requirements shared in these interviews where consent across both approaches. The table below highlights how Sophos Cloud Optix addresses these focus areas.

Organizational Focus	Public Cloud Security Requirements	Cloud Optix Benefits
Security Operations	Avoid data loss and leakage	Automatically prevent, detect, and remediate accidental or malicious changes in network configuration that could lead to a breach
	Improve visibility into cloud assets in elastic multi-cloud environments	Allow teams to save hours by generating network topology diagrams and asset inventories on demand
	Save valuable time spent identifying, assessing, and remediating security risks	Aggregate and prioritize security and compliance alerts across multiple providers and provide contextual remediation steps
	Stop unauthorized access through misuse of employee credentials	Be alerted to unusual behavior in users' activity, API calls, and network traffic
	Enable teams to aggregate alerts through a SEIM, but also reduce unnecessary SEIM data ingestion costs if appropriate	Provide alerts to the right team fast to reduce incident response times via SEIM integration or direct access to the console
	Integrate with current security tools, and be flexible enough to onboard new technology platforms	Access features programmatically via API, or utilize integrations with common tools including Jira, ServiceNow, Slack, and Splunk

Organizational Focus	Public Cloud Security Requirements	Cloud Optix Benefits
Automate CI/CD Pipeline Security	Enable continuous delivery without risk of replicating security vulnerabilities in the development pipeline	Automatically scan Infrastructure-as-Code templates merged to source control management, with pipeline deployment based on security assessment results
	Reduce time taken to identify if deployments were made following an authorized deployment method	Enable teams to quickly review changes and determine which were outside the authorized processes, and take measures to remediated

Organizational Focus	Public Cloud Security Requirements	Cloud Optix Benefits
Regulatory Compliance	Stop diverting resources from business generating projects to address compliance requirements	Integrate compliance into daily processes through integrated alert management with collabortaion and ticketing tools
	Avoid the time taken to map security best practices and compliance standards to dynamic infrastructure environments	Automatically analyze configuration settings against compliance and security best practice standards, with the option to customize policies to meet organizational requirements
	Reduce the cost associated with regular audits	Automate continuous monitoring of standards and streamline audit processes by defining cloud assets subject to compliance reviews and mapping control IDs from existing overarching compliance tools

The Build or Buy Dilemma

The rapid growth of cloud usage has resulted in fractured distribution of data, with the average organization now utilizing at least two public clouds platforms[3]. This multi-platform approach compounds the visibility challenge for security teams who must switch from platform to platform for a complete picture of cloud assets.

As you begin to build your own requirements and evaluate solutions, plan for what it means to build and maintain your own solutions to ensure continued compliance and security in your own dynamic public cloud environments. Investing internal time and resources may sound attractive at the outset, but the reality is that this will involve connecting multiple point products and consoles, and is likely to lack the comprehensive visibility required to address the highest-priority challenges for organizations:

- What hardware, software, and skills are needed to develop a custom product?
- Can the organization afford to wait to build a solution?
- As cloud providers introduce new services, and as regulatory standards change, how will the organization resource the maintenance of a custom product?
- In the event of a security breach or misconfigured resource, how will the organization discover it, and how will teams respond?
- How will unusual user access, API calls, and changes in configurations be tracked and traced?
- How will security be automated at all layers of the CI/CD pipeline?
- How much time will it takes to map industry and regulatory standards requirements to infrastructure and maintain those policies?
- Will it be possible to monitor multiple cloud provider accounts, environments, and regions from a single console, and what are the implications for DevOps and SOC teams?

Savings and Benefits With Sophos Cloud Optix

Sophos Cloud Optix is born in the cloud security, providing measurable benefits that enable your security, operations, development, and compliance teams with the security and collaboration tools to own and automate security and compliance response. This allows organizations to reduce the risk of security breaches, and compliance penalties, and redirect saved time and energy to strategic projects.

ROI Benefit Analysis

The following section explores the ROI of Cloud Optix over a three-year period based on three public cloud environments sizes (small, medium, and large):

- Small environment: 100 cloud assets | One regulatory or industry compliance standards
- Medium environment: 500 cloud assets | Two regulatory or industry compliance standards
- Large environment: 1,000 cloud assets | Three regulatory or industry compliance standards

Note that these ROI estimates do not include Cloud Optix subscription costs, which should be subtracted from these models.

Calculation Assumptions

When calculating the return on investment for Cloud Optix, Sophos have applied the following assumptions based on analysis of the live Cloud Optix service and industry analysis. The results presented in this document are an estimate, not a guarantee, and actual savings may vary. Note that alert volume may appear less inflated than native cloud provider monitoring tools and other industry vendors. This is due to two factors:

- Cloud Optix ability to perform root cause analysis and risk-based prioritization of alerts to reduce alert volume, without compromising security
- Removal of "low" priority alerts from our calculations

21

Average alerts per 100 cloud assets per week

180

Time to investigate and resolve each cloud alert manually (in minutes)

$98k

Compliance team FTE salary

25%

Percentage of time spent managing compliance policies, procedures, and reporting

20

Time to investigate and resolve each cloud alert with Cloud Optix (in minutes)

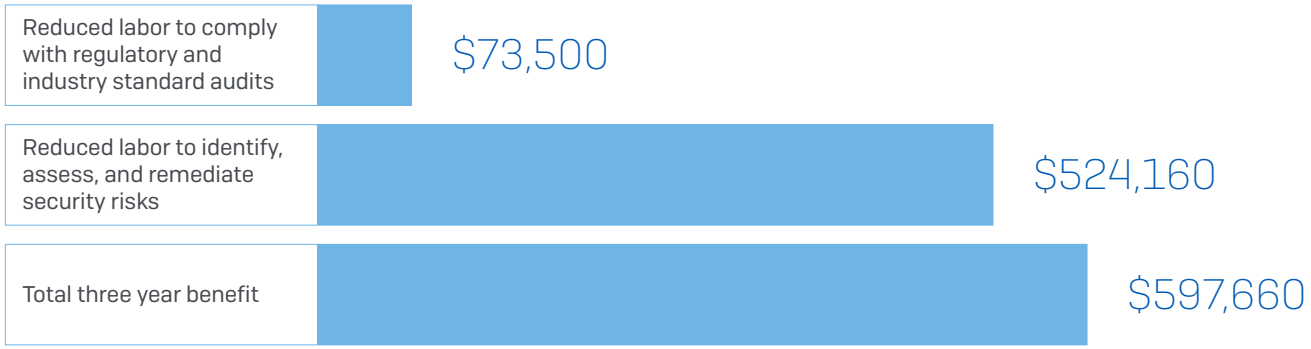
$143k

Information Security FTE salary

Small Cloud Environment ROI Benefits

100 CLOUD ASSETS | ONE REGULATORY OR INDUSTRY COMPLIANCE STANDARDS

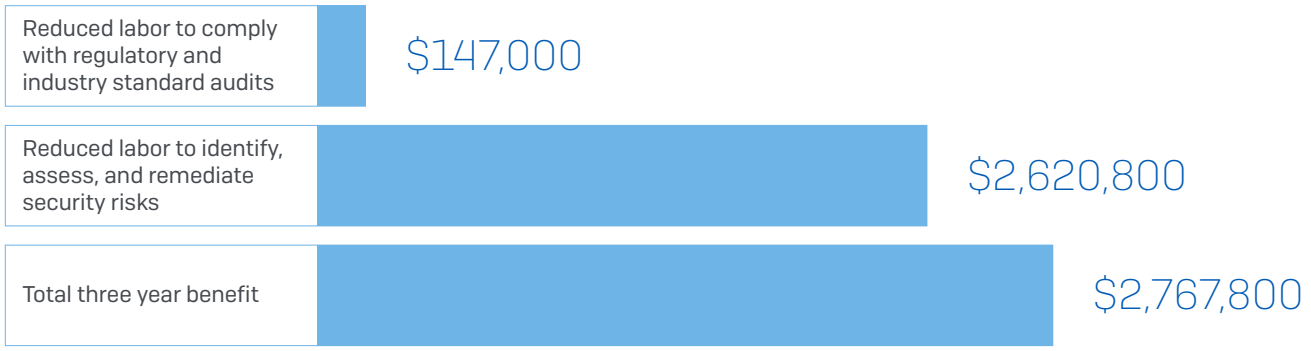
The savings created by Sophos Cloud Optix for an organization operating a small public cloud environment are shown below.



Medium Cloud Environment ROI Benefits

500 CLOUD ASSETS | TWO REGULATORY OR INDUSTRY COMPLIANCE STANDARDS

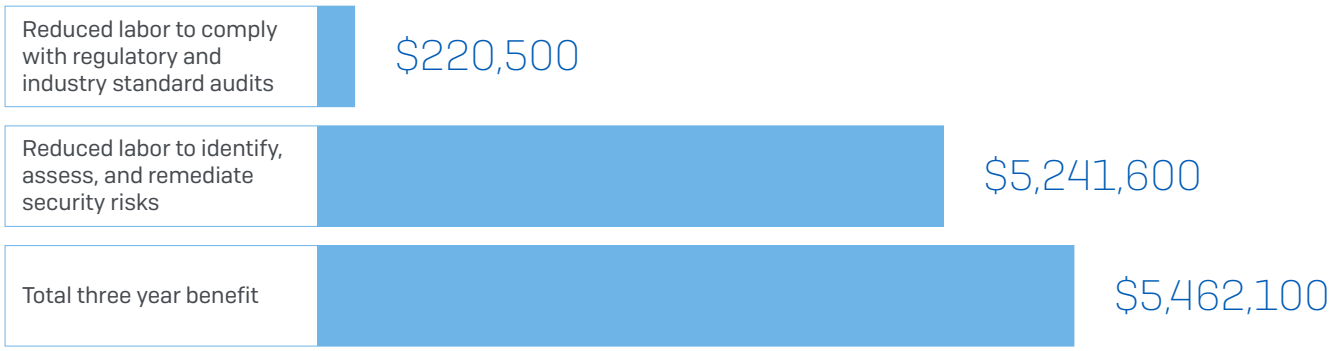
The savings created by Sophos Cloud Optix for an organization operating a medium-sized public cloud environment are shown below.



Large Cloud Environment ROI Benefits

1,000 CLOUD ASSETS | THREE REGULATORY OR INDUSTRY COMPLIANCE STANDARDS

The savings created by Sophos Cloud Optix for an organization operating a large-sized public cloud environment are shown below.



Additional ROI Considerations

DATA BREACH RISK REDUCTION

The Ponemon Institute's 2018 Cost of a Data Breach Study: Global Overview revealed the estimated average cost of a security breach at $3.86 million with a 27.9% likelihood of a recurring breach in the following two years[4].

By automatically detecting misconfigurations and security vulnerabilities, and continually monitoring architecture changes to stay ahead of attacks, Cloud Optix has the potential to significantly reduce the likelihood of breaches in the first year and beyond when maintained by your security team.

REDUCED SCRIPTING OF AUTOMATED CI/CD PIPELINE TESTING

Half a day can easily be consumed by development teams coding automated pipeline testing scripts for each cloud account. While the structure and asset types included in an individual organization's cloud accounts vary to widely for an accurate ROI estimate, considerable time savings can be gained with Cloud Optix. To estimate ROI for an organization, work with development and operations teams to identify:

- The number of cloud accounts requiring regular or continuous security testing across development, QA, and production environments
- Time spent developing automated test scripts that could be replaced by Cloud Optix IaC scanning capabilities
- Time taken to identify and maintain policy checklists automatically applied and updated by Cloud Optix

Conclusion

Moving from traditional to cloud-based workloads offers huge opportunities for organizations of all sizes, yet securing the public cloud is imperative if you are to protect your infrastructure and organizations from cyberattacks.

Sophos Cloud Optix is the ideal solution for organizations using or moving to the public cloud. Combining the power of AI and automation, it provides organizations with the continuous analysis and visibility needed to detect, respond, and prevent security and compliance risks that could leave them exposed.

With Sophos Cloud Optix, your organization can save substantial time, money, and resources while ensuring continuous compliance, a strong security posture, and most critically of all: reducing your likelihood of a security breach.

REFERENCES

1. 2019 Verizon Data Breach Investigations Report.
2. Security Boulevard, Amazon EBS snapshots exposed publicly leaking sensitive data in hundreds of thousands, security analyst reveals at DefCon 27, by Fatema Patrawala.
3. RightScale 2019 State of the Cloud Report from Flexera.
4. Ponemon Institute, 2018 Cost of a Data Breach Study.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2019-11-01 (TN)