CISO's playbook to cloud security

Key strategies to secure your enterprise cloud infrastructure from cyber threats

LACEWORK

Securing enterprise assets in a multicloud era

Transform cloud security challenges into business opportunities

To secure enterprise assets in the cloud, CISOs have to address several new challenges unseen in traditional IT and on-premises data centers:

Long threat-dwell periods

In highly dynamic and complex cloud architectures adversaries can evade detection for months, average dwell times ranging up to 101 days. This is a considerably long period to perform reconnaissance to locate critical assets which quite commonly result in data theft and exfiltration.

Shared security responsibility

Enterprise and cloud provider's security responsibility boundaries often lack clarity. Even when the cloud provider delivers certain security functionalities as-a-service, the enterprise is responsible to detect any breaches. In practice, enterprises are responsible to protect user accounts, service configuration, security monitoring and compliance of their cloud infrastructure.

Multicloud – the new normal

Research indicates about 85% of enterprises having some form of cloud-based operations leverage multiple private and public cloud resources. On average, the number of cloud applications enterprises use exceed 90.

Inadequacy of traditional security

Traditional perimeter defenses may serve isolated datacenters well but not the dynamic and shared cloud environment. Conventional security tools using manually defined policies, rules, and signatures fail to keep up with the speed at which the cloud's runtime configurations change.

Velocity overweighs security:

In spite of recognizing the criticality of cloud security at a governance level, in actual practice, the ease and velocity of deploying cloud workloads often take precedence over the security implications of doing so. Implementing a security strategy designed specifically to address these unique challenges in the cloud is the key to effectively monetize cloud efficiencies without losing sleep over security.

High-net-worth incidents

Cloud exploits with lengthy dwell-time are costly and compromise sensitive data, reputation, and an organization's bottom line. Ponemon Institute's 2018 "Cost of a Data Breach Study"1 found the total cost of a data breach exceeds $3.8 million (global average), a 6.4 percent increase from the previous year's average.

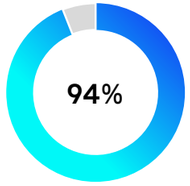
LACEWORK

> “94% of the participating IT leaders from large and mid-sized companies recognized early security engagement as an enabler to reduce the risk of cybercrime and data loss.”

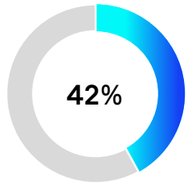
What are the top benefits of early engagement by the security team in a cloud project?

Involving the security team earlier in a project, you can ensure that a project meets compliance goals. Early engagement allows the security team to integrate security throughout an offering and often prevents costly delays. The ultimate result of engaging security early in a project is that you can provide safe and secure applications and services that don’t put your organization or your customers at risk.

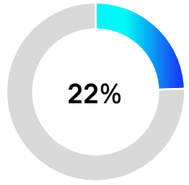
In Hurwitz and Associates’ 2018 cloud security survey, 94% of the participating IT leaders from large and mid-sized companies recognized early security engagement as an enabler to reduce the risk of cybercrime and data loss. Accelerated project delivery and diminishing project costs were the other significant benefits cited in the survey.



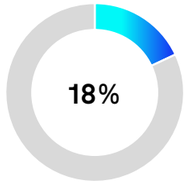
Reduced risk of cybercrime and data loss



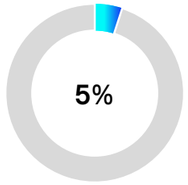
Faster project delivery



More predictable schedule



Lower project costs



No significant benefits

Cloud security maturity model

Cloud security has far-reaching implications in organizational success. A cloud security maturity model enables business leaders to benchmark and to assess their organization's security evolution across all cloud operations along these three stages:

Step 1: adopt

This is an early adoption stage where the cloud footprint is limited to a few dozens of workloads, containers and a few user accounts. The primary security objectives are security governance and compliance. The security tools used are usually open-source or native to the public cloud offering.

Cloud footprint:

- Dozens of workloads & containers
- Few cloud accounts

Objectives:

- Compliance assurance
- Security governance

Other security solutions:

- Open source tools
- Cloud provider tools
- Configure monitoring tools

Step 2: expand

As the cloud operations expand to hundreds of cloud workloads, containers, and many user accounts, security activity needs to evolve to include security monitoring, automated threat detection, vulnerability management, etc. using third-party security tools to protect the cloud infrastructure, workloads and containers.

Cloud footprint:

- Hundreds of workloads & containers
- Many cloud accounts & providers

Objectives: (+Stages 1 objectives)

- Central visibility
- Automated threat detection
- Vulnerability management

Other security solutions:

- Cloud infrastructure
- Assessment tools

Step 3: scale

As the cloud usage scales to thousands of workloads, containers, and several cloud accounts in a multicloud environment, the security model needs to add external threat intelligence, automated remediation, incident response management, etc. using unified cloud security solutions to protect the cloud infrastructure, workloads, and containers.

Cloud footprint:

- Multiple cloud providers
- Thousands of workloads & containers
- Dozens of cloud accounts

Objectives: (+Stage 2 objectives)

- External threat intelligence
- Auto-remediation
- Incident investigation

Other security solutions:

- Unified cloud security solutions cloud infrastructure, workload, containers

The new generation of security for the cloud

In the cloud, infrastructure resources for network, storage, and compute are delivered as virtual services. Virtualized, dynamic architectures underpin the benefits of cloud velocity and runtime flexibility... but add multiple layers of security complexity. A future-proof solution must be capable of delivering security for these unique cloud dynamics:

Fluid workloads

Cloud workloads function in highly fluid architectures involving complex sets of applications, microservices, and serverless instances. The deployed instances come and go on-demand causing the security environment also to be in constant flux.

Containers and microservices

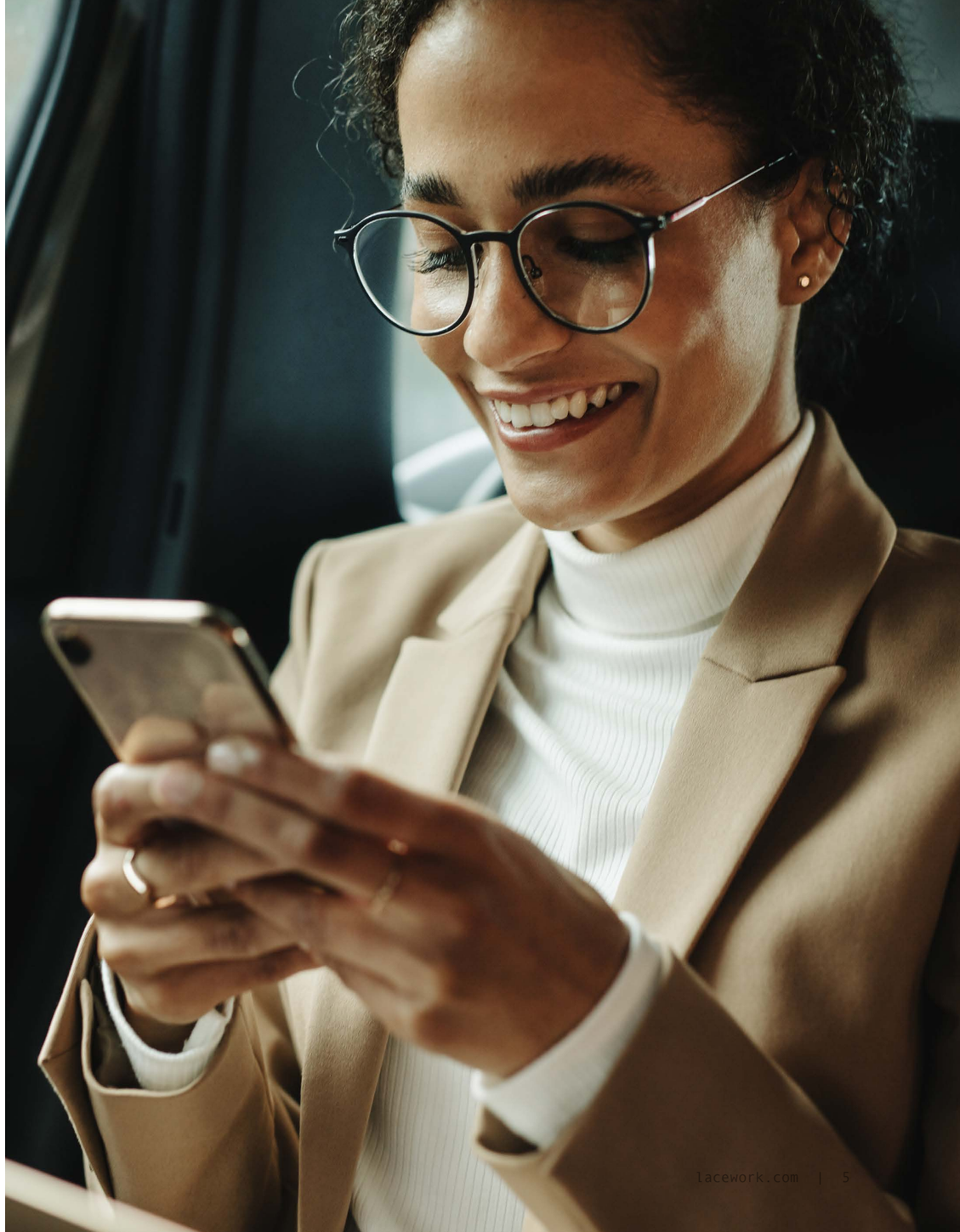
Containers and microservices deliver resiliency and elastic scale. However, due to less isolation, containerized environments are more vulnerable to various attack vectors. Instead of one application, there's now the need to access control and authenticate every single microservice, container, and cluster.

DevOps process

In the cloud, DevOps team run cloud workloads in multiple short iterations several times during the week. The new code constantly expands the attack surface.

Ephemeral resources

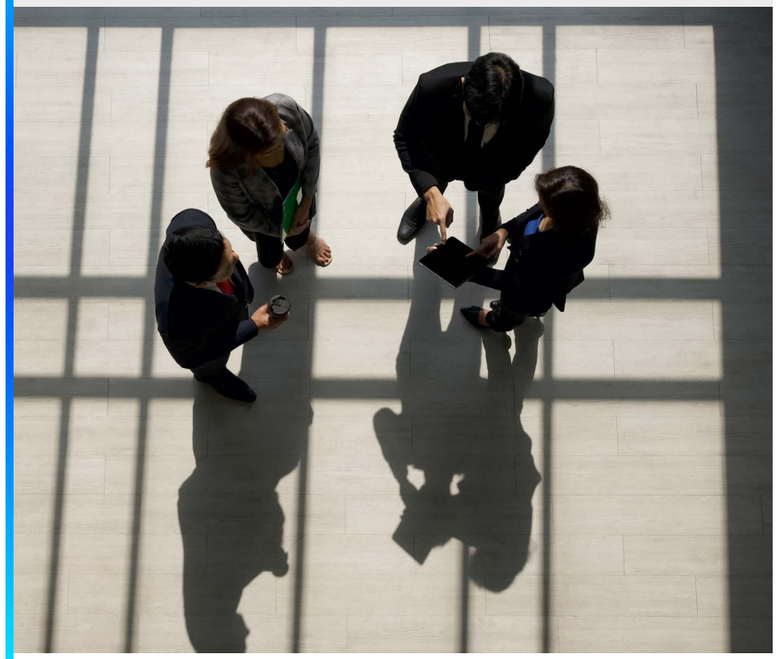
Cloud workloads are constantly destroyed and recreated. It is common to recycle cloud platform assets like servers, IP addresses, firewalls, drives, overlay networks, etc. to optimize utilization. Perimeter and IP address-based security controls are useless when resources are ephemeral. Forensic investigations are also impossible when logs disappear after the workloads are spun down.



Cloud security needs a new approach

6 cloud security strategies to harden your enterprise cloud infrastructure

Secured cloud operations result in significant business benefits. However, fluid cloud architectures, where traditional security controls fall short, pose a formidable challenge to implement security. The following 6 strategies provide a game plan to secure a continuously changing cloud environment through continuous, real-time approaches to security.



1. Maximize visibility into your cloud

When everything is encrypted on the wire, you need deep, process-level visibility to continuously evaluate your cloud activity.

Most security-relevant events never leave the cloud's virtual machines and containers which limits your ability to gain insight. Security evaluation requires visibility into traffic between containers and microservices.

Adopt a security platform capable of monitoring at the application and process levels. Events logged at the process level persist even when the workload is spun down, which is a key capability to support forensic analysis when workloads are ephemeral.

2. Automate security

Cloud security automation is an increasingly critical strategy to meet your business goals.

In containerized environments where hundreds of cloud workloads execute simultaneously, you need to automate the entire security workflow from install, configuration and event management, to file monitoring, notifications, and threat analysis. Automation is critical to scale your security operations in the cloud without being capped by the size of your security team.

3. Track activity with container-aware tools

Without the container-context, threats can escape your anomaly detection process.

As cloud applications are increasingly run in containerized environments, security teams need insights into inter-container traffic within the cloud, not just from and to the cloud. This underscores the need for a container-aware security solution that traditional rule-based tools fail to deliver.

Having the container-context integrated into security monitoring and logging allows your security teams to track activity and identify anomalies at the microservices and container orchestration layers.

4. Correlate data to identify anomalies

Cloud security solutions should be able to ingest relevant data and understand what the environment looks like under normal conditions to accurately flag runtime anomalies.

Instead of relying on rules-based security, leverage security automation based on behavioral analysis and machine learning. You need security products that can actively learn the behavior of the enterprise cloud environment and use that knowledge to create baselines to defend it. Fully automated behavioral analytics solutions produce high efficacy alerts, scale seamlessly, and minimize alert fatigue.

5. Adopt the culture of collaborative security

In the cloud, security needs a shift from isolation to collaboration.

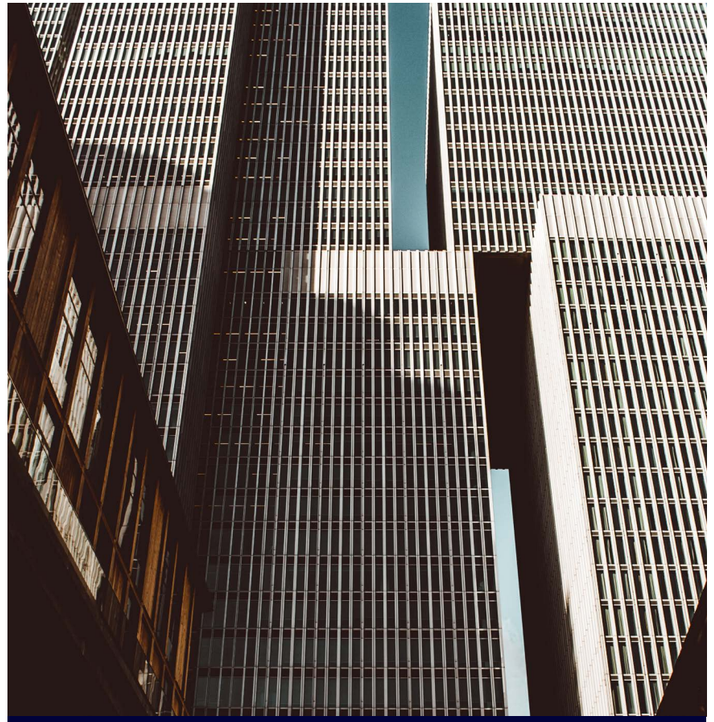
Promote a culture where security disciplines go beyond the silos of the centralized security team. Security for the cloud needs to get distributed and get integrated with DevOps processes. There are multiple ways to accomplish this. The centralized security organization can provide distributed security engineering within each development team in addition to offering governance, guidelines, and tooling. Processes to support developers when they seek security guidance improves productivity. For example, a security expert can be part of the daily scrum calls to address concerns. Ticketing systems and collaboration tools can be instituted to provide answers on business risk questions.

6. Adopt a comprehensive security platform

A comprehensive cloud security platform ensures nothing is left unprotected that point solutions fail to guarantee.

Your cloud security solution needs to comprehensively secure the enterprise cloud infrastructure, workloads, containers, and Kubernetes – from build-time to run-time. You also need to identify security platforms designed specifically for dynamic and elastic multicloud environments. A comprehensive security platform offers:

1. Vulnerability management to reduce software risks
2. Compliance to minimize risks due to misconfigurations
3. Account security to protect the critical entry point in most cloud incidents
4. Workload security for host-level protection of all applications
5. Container security for container-aware runtime threat-detection
6. Kubernetes security to secure the container orchestration layer



> “Fully automated behavioral analytics solutions produce high efficacy alerts, scale seamlessly, and minimize alert fatigue.”

A complete cloud security and compliance platform for comprehensive protection

Multicloud security platforms are helping companies to adopt and securely scale their environments in the cloud. The security landscape is replete with many point solutions?

But, why increase the cost and complexity with a patchwork of solutions? The new generation of cloud security is powered by unified SaaS platforms where you can leverage an ever-increasing set of security functionality over-time. These are built by utilizing a common framework of principles, interfaces, and data-stores.

A comprehensive security platform easily integrates with the security capabilities from your cloud service provider such as Amazon Web Service's governance, compliance, risk auditing, and other security services.

The rewards of securing enterprise cloud infrastructure

The positive outcomes benefit the entire enterprise

The cloud has emerged as the operational backbone of modern enterprises. The benefits of securing your cloud infrastructure lead to enterprise-wide positive business outcomes:

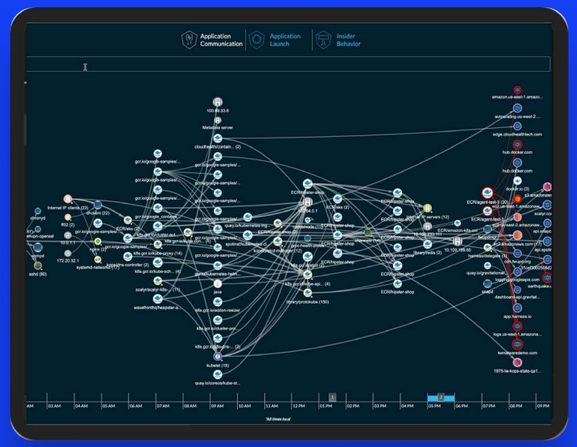
Accelerate feature velocity – DevOps teams can leverage integrated security disciplines to reduce unexpected risks, which accelerates their development cycles.

Reduce the cost of compliance – Automated and continuous audit checks ensure compliance and reduce the risk of regulatory penalties.

Reduce remediation cycles – Security integration from build-time to run-time improves the quality of products and services you deliver. It lowers CVEs and security escapes, and the associated cost of remediation.It also bolsters customer confidence in your products.

Reduce the risk of a security incident – Security awareness and concerted actions by teams to prevent security issues reduce the risk of a breach and improve the overall security posture of the organization.

Lower security budget – Matured cloud security helps to streamline resources, tools, and security processes that positively improve the bottom line.



Ready to chat?

Request a demo

Lacework delivers security and compliance for the cloud generation. The Polygraph® Data Platform is cloud-native and offered as-a-Service, delivering build-time to run-time threat detection, behavioral anomaly detection, and cloud compliance across multi-cloud environments, workloads, containers, and Kubernetes. Trusted by enterprise customers worldwide, Lacework significantly drives down costs and risk, while removing the burden of unnecessary toil, rule writing, and inaccurate alerts. Lacework is based in San Jose, California, and backed by Sutter Hill Ventures, Liberty Global Ventures, Spike Ventures, the Webb Investment Network (WIN), and AME Cloud Ventures.

Get started at www.lacework.com

LACEWORK®