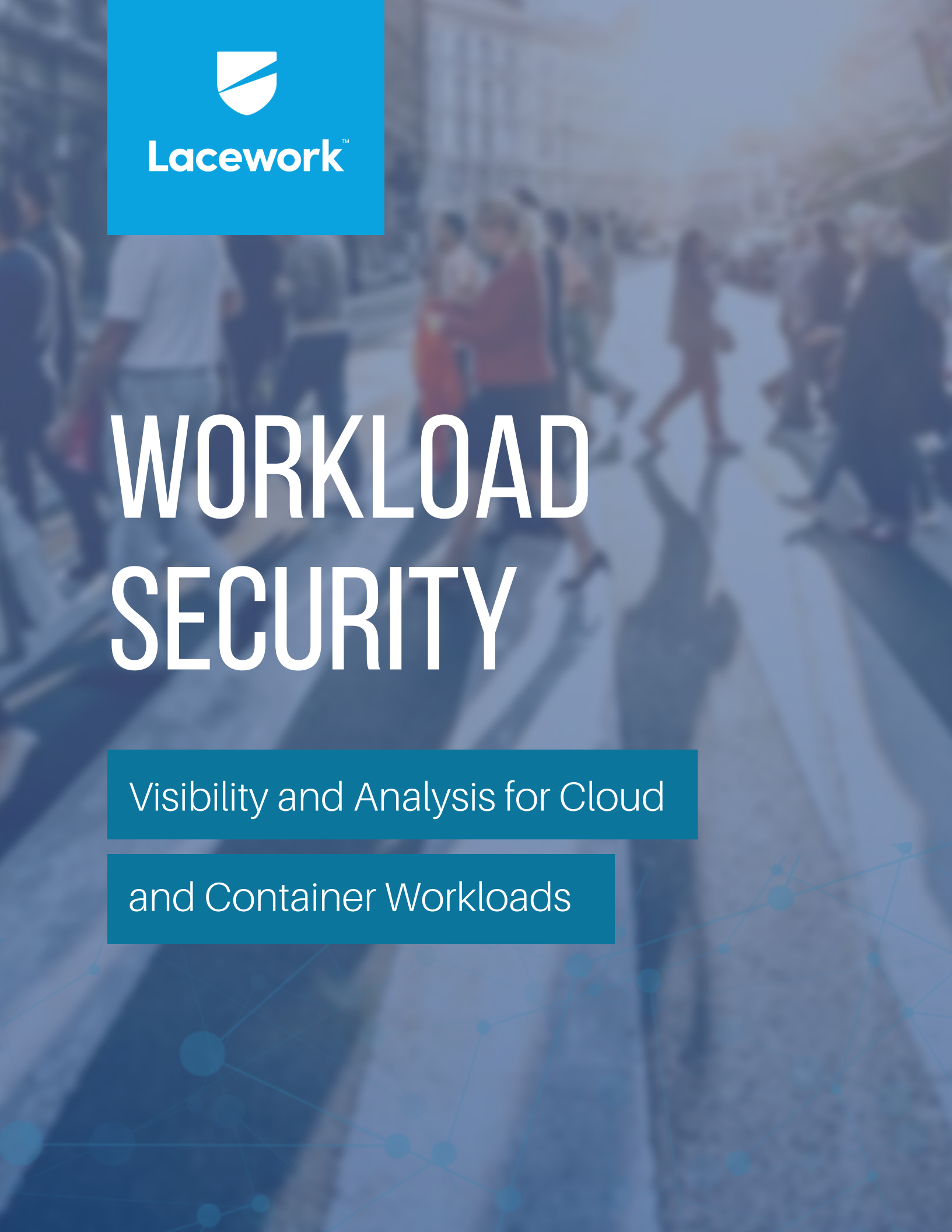


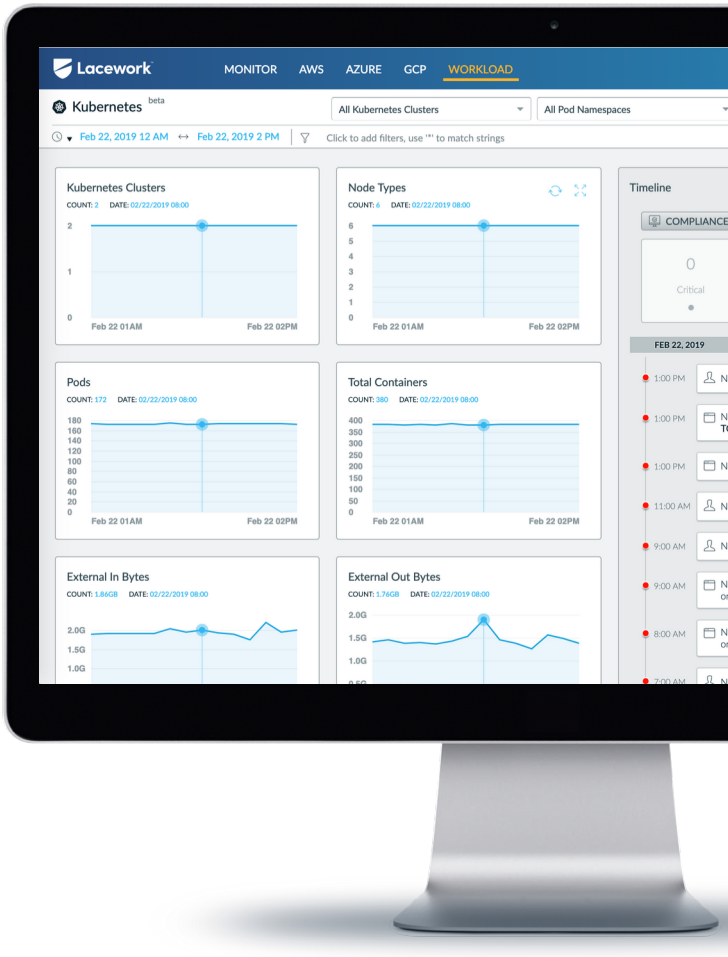
WORKLOAD SECURITY

Visibility and Analysis for Cloud and Container Workloads

LACEWORK WORKLOAD SECURITY

Visibility and Analysis for Cloud and Container Workloads

The public cloud enables enterprises to automatically scale workloads, deploy faster, and build freely. This infrastructure allows organizations to rapidly deliver on business objectives. Unfortunately the old security solutions are unable to adapt to this new paradigm. At Lacework, we developed our security solutions from the ground up, specifically for the rapidly changing cloud. Our platform provides a comprehensive solution that encompasses cloud configurations, account activities, workload/runtime analysis, and automated anomaly and threat detection.



Lacework's workload security provides visibility to all processes and applications within an organization's cloud and container environments. The breadth and depth of visibility helps detect vulnerabilities, and then uses Lacework's machine learning analysis to identify anomalous behavior that poses threats.

Traditional security solutions rely on network logs and the firewall rules to identify potential risks, but those approaches required a manual effort, and could not keep pace with the speed of modern cloud deployment methodologies.

Lacework was built specifically to deliver contextual data about cloud events; every update, configuration change, access point, and a million other activities that might represent potential threats.

We track all machine/process communications , the users associated with those processes, and the amount of data that was transferred between processes during a given time. This deep level of detail allows teams to save time on their investigations because all the relevant information are on one platform.

The Lacework agent shows exactly which processes received and launched connections, the associated users, and the amount of data that was transferred between processes.

AUTOMATED WORKLOAD INTRUSION DETECTION

Lacework's workload protection is fully automated, no rule writing required. Using sophisticated machine learning, Lacework learns what constitutes normal behavior versus those that indicate potentially malicious activity. Examples of such anomalous activities are when a user launches a new unknown application, when an application connects to a suspicious endpoint, or when privileges are unexpectedly escalated. When Lacework identifies a potential threat, a contextual alert is generated with relevant data to allow users to investigate and triage the issue.

In a rapidly changing deployment environment, traditional security rules are stale as soon as they are deployed and new attacks are missed because they require someone to write the appropriate rule. Lacework's automated approach provides the following benefits:

1.) No Missed Events: Lacework will always alert you on new activity, so that you are given a chance to investigate any behavior within your environment that could potentially be malicious.

2.) Low Alert Noise: Lacework will only alert you on what is new or anomalous, preventing alert fatigue within your organization.

3.) Simple Operations & Maintenance: Automated workload detection means no writing and maintaining error prone rules. With Lacework you will not need to constantly maintain rules, allowing you to focus on securing your environment.

CLOUD SECURITY, AT SCALE, AT THE SPEED OF BUSINESS

The modern cloud infrastructure allows organizations to deploy, scale, and configure their infrastructure faster than ever. The ability to automate and operate at DevOps speed poses a challenge to traditional security approaches. Lacework's approach is to automate the detection of threats and anomalies and provide human understandable investigative insights. Lacework supports public clouds AWS, GCP, Azure and supports computer hosts and containers.

SECURITY VISIBILITY

Get deep observability into your cloud accounts, workloads, and microservices to give you tighter security control.

THREAT DETECTION

Identify common threats that specifically target your cloud servers, containers, and IaaS accounts so you can action on them before your company is at risk.

ANOMALY DETECTION

Detect and resolve anomalous changes in behavior across your workloads, containers, and IaaS accounts that represent a security risk or an IOC.

HOST COMPLIANCE

Achieve compliance for SOC 2, PCI DSS, HIPAA, and other compliance measures that require host intrusion detection (HIDS).

CONFIGURATION COMPLIANCE

Spot IaaS account configurations that violate compliance & security best practices the could put your company at risk.