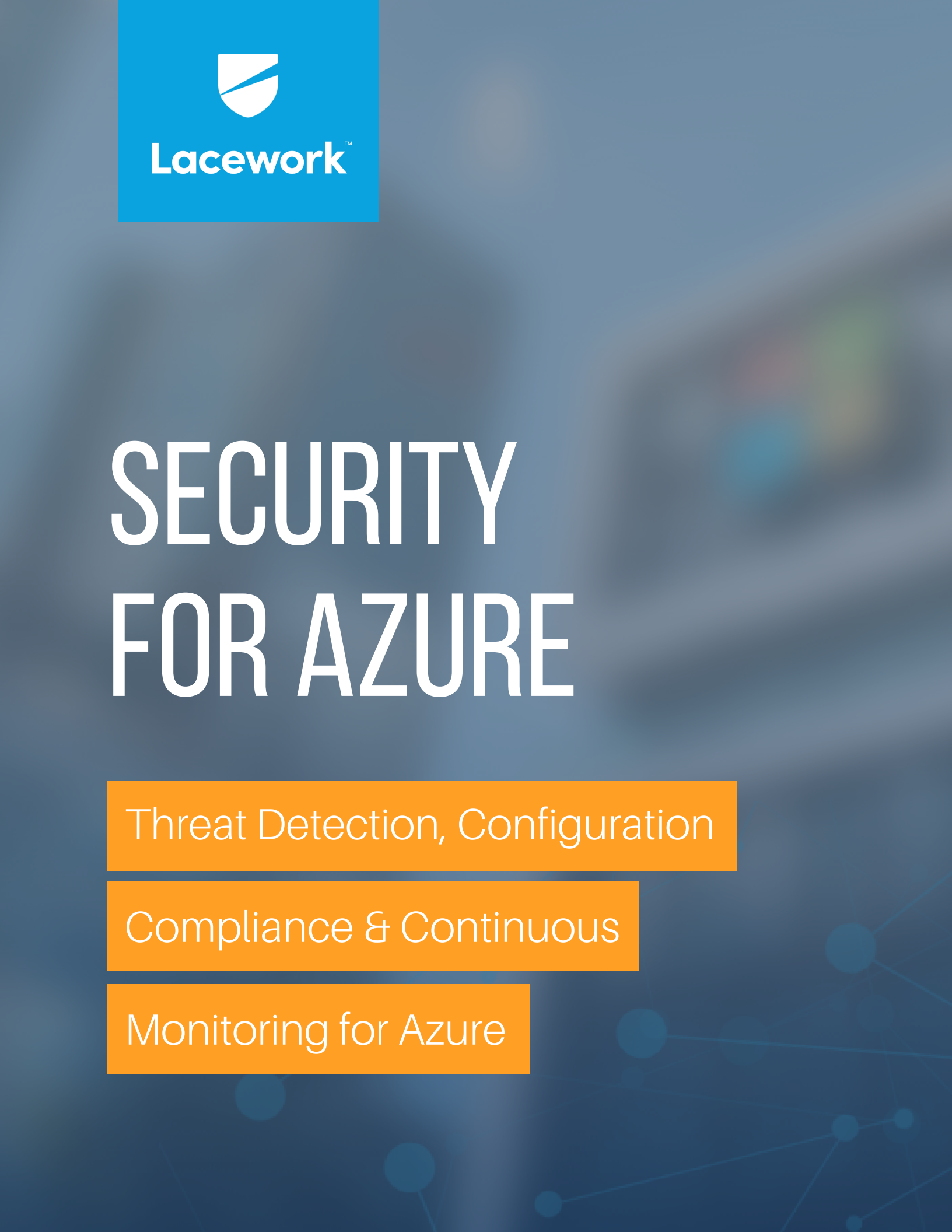
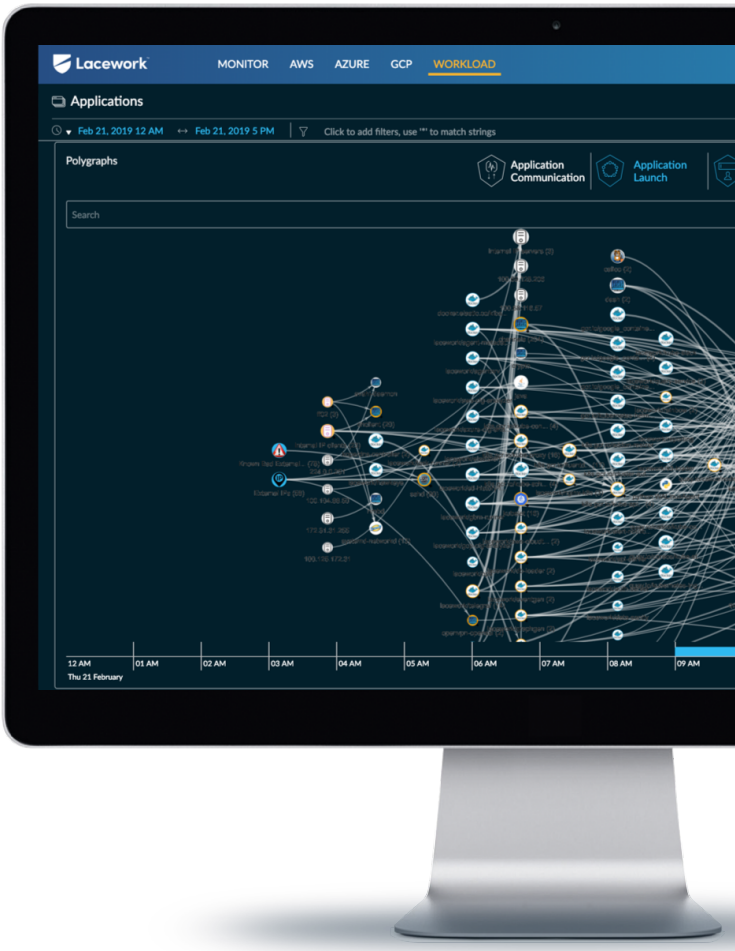

Lacework™
SECURITY
FOR AZURE
Threat Detection, Configuration
Compliance & Continuous
Monitoring for Azure

Lacework

SECURITY FOR AZURE

THREAT DETECTION, CONFIGURATION COMPLIANCE & CONTINUOUS MONITORING FOR AZURE

Lacework provides comprehensive, continuous end-to-end security and configuration support for workloads and accounts running in Microsoft Azure. As more organizations move their critical infrastructure to the cloud, and choose to adopt a multicloud approach, there is an increasing need for a solution like Lacework that can identify, analyze, and report on misconfigurations, vulnerabilities, and behavioral anomalies in user and account behavior.



Lacework checks for a series of additional controls specific to Azure resources, and helps you validate that data is not inadvertently exposed to unauthorized users. Lacework protects every layer of your Azure deployment - accounts, workloads, and PaaS services such as Azure SQL - and it is done on a continuous basis, sending notifications on any change that might trigger a security weakness.

You can now effectively and efficiently protect assets deployed on Azure, from the initial configuration to everyday operations.

THREAT PROTECTION

For all Azure events and configurations, Lacework monitors activities and behaviors of cloud entities beyond network traffic to detect anomalies indicative of a misconfiguration, a human error, malicious activity or a threat. Lacework enables security and development teams to identify escalation of privileges, lateral movement, misuse of Azure resources early on so that breaches can be stopped early.

Risks and threats are visible within the Lacework dashboard, a e ranked by risk severity, and can be delivered through the most common modern methods such as a Slack channel or a Jira ticket.

CLEAR AND SIMPLE

Fast and easy installation (no agent). Interactive information on individual violations with explicit instructions on how to remediate each issue. Customizable reports and alerts.

CONTINUOUS AUDITING

Daily re-audits with notifications when changes impact security. Continuous usage monitoring with alerts for anomalous behaviors and activity - all without manual rule or policy development.

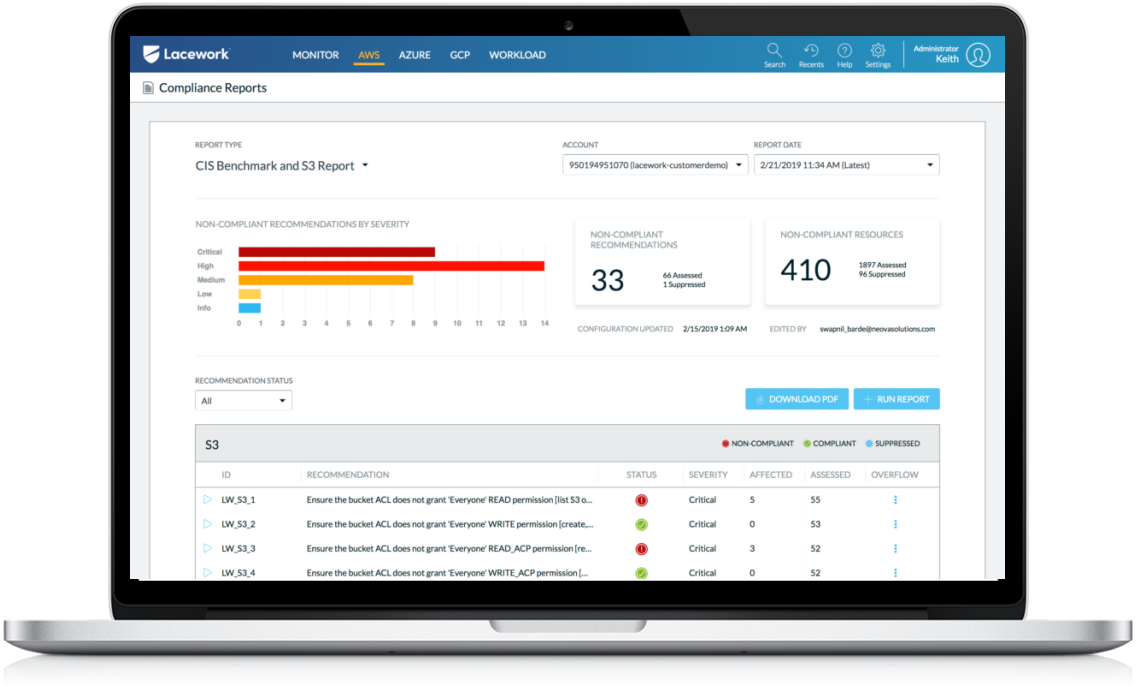
INTEGRATED WITH AZURE SERVICES

Integration across Azure services ensures the most complete visibility into Azure configuration. Get exceptional visualizations, search by service, and other investigative tools focused on account security.

CONFIGURATION COMPLIANCE

Lacework automatically validates your configuration against the controls established as best practices for Azure. Our interactive report delivers insights into passed or failed controls with recommendations on how to fix out-of-compliance configuration components. A similar report is available for additional security controls specific to Azure resources.

Lacework ensures continuous compliance by auditing your configuration daily and alerting you of any change that represents a degradation in compliance.



CONTINUOUS MONITORING OF AZURE ENVIRONMENTS

As Azure environments continuously adapt to new users, services, and resources, the corresponding security landscape changes in a dynamic way. Lacework is a single, comprehensive solution that captures, analyzes, and reports on all cloud activity so you are able to get an accurate assessment of your Azure and multicloud workloads and accounts.

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.