SOLUTION BRIEF

Simplifying security for Microsoft Azure

Achieve continuous compliance, manage vulnerabilities, and automate threat detection with Lacework

OVERVIEW

Securing your cloud environments

Adopting cloud architectures can be transformative, allowing for greater flexibility, efficiency, speed, and innovation. But with these benefits come a new set of challenges. Cloud environments are complex and dynamic by nature, which means that legacy security approaches can't offer adequate protection from configuration errors, vulnerabilities, and threats.

When it comes to your Microsoft Azure environments, it's important to protect your business by securing your cloud accounts and workloads. Lacework partners with you to address these concerns by offering an automated, end-to-end security solution on the global, secure, and trusted infrastructure of Azure. We monitor for threats to workloads and accounts across Azure, multicloud, and containerized environments. With Lacework, you can keep your organization secure.

CHALLENGES

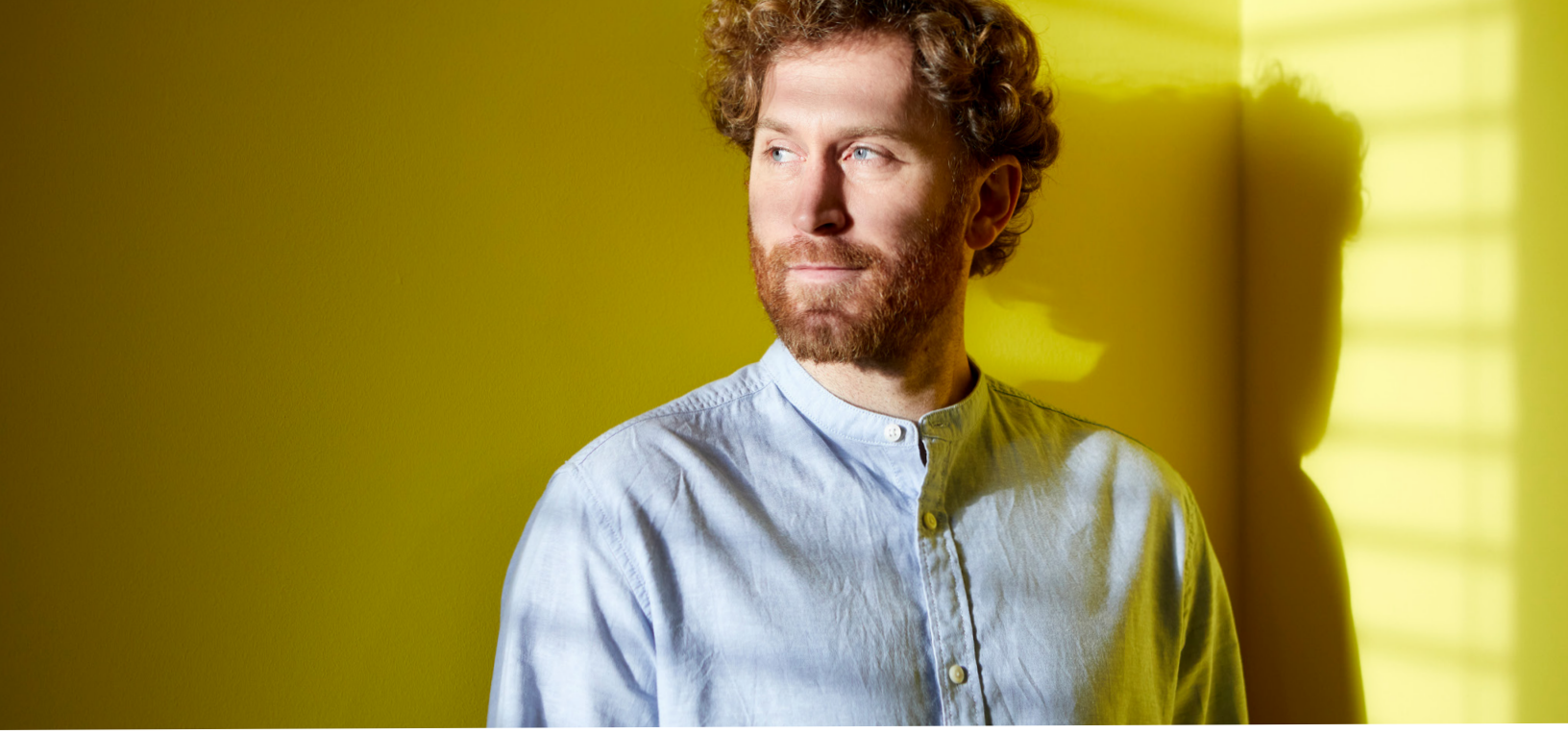
Minimizing risks in Azure

There are many reasons to prioritize the security of your Azure environment. Cyberattacks can be harmful for your business and your data, costing money and compromising customer trust. No matter the size of your security team, manual monitoring can be slow, eating up your valuable time. And whether you are in a regulated space or your customers require it, the continuous need to prove compliance can be time-consuming – not to mention expensive. Luckily, Lacework is here to help with all of this, and more. We automatically find true threats, which reduces your false positives and alerts to help you stop danger in its tracks.

Microsoft Azure

Key Lacework use cases

- Automated threat detection that eliminates the need to write and maintain rules
- Build time and runtime vulnerability management across hosts and containers, plus risk scores to help with prioritization
- Configuration assessments and checks for compliance standards like SOC2, ISO 27001, HIPAA, PCI, NIST, and CIS Benchmarks



OUR APPROACH

A data-driven solution

Lacework reduces risks with a data-first approach. We begin by collecting the most important information: gathering data through our combined agentless and agent-based approach. Our agentless approach collects the data to provide a clear picture of Azure-base across projects and services, while our agent collects data on Azure Virtual Machines. Through Azure Audit Logs, we continuously observe your cloud resources, monitoring the behavior of users, apps, processes, and networks to identify indicators of compromise.

Once the initial data is collected, Lacework moves on to detection so we can find the greatest risks to your business, including misconfigurations and vulnerabilities. For runtime threats, Lacework surfaces indicators of compromise based on unusual activity through our patented Polygraph® anomaly detection engine. We can find vulnerabilities throughout your build time and runtime processes, identify cloud misconfigurations in cloud assets like Azure Blob Storage, and discover issues that concern cloud best practices as well as compliance requirements.

Finally, we tell you what we discovered, so you can decide how best to proceed. Lacework surfaces only the most critical risks, eliminating alert fatigue, and provides context-rich visualizations and notifications so you can take quick action. We also offer comprehensive reporting to help you prove compliance. And by integrating with ticketing, messaging, SIEM, and more, we allow you to solve issues more efficiently.

> "I find that Lacework is so granular in detecting anomalies within either cloud [AWS and Azure], that it allows me to make all of my other operations better because it's so fine-tuned."
>
> BRIAN LACHANCE, FORMER CHIEF INFORMATION SECURITY OFFICER, CAZENA

USE CASES

Advanced protection for Azure environments

Lacework provides a modern security solution for the modern cloud. Not only do we help you ensure continuous compliance and protect your data from unauthorized exposure, but we do it all in a way that requires minimal maintenance. We offer more protection with less hassle.

Configuration assessment

Understand your configurations with Lacework, which lets you monitor your assets across your Azure environments. Simplify your configuration assessment process by leveraging just one platform to easily track configuration changes, find vulnerabilities, and detect threats.

Cloud and industry compliance audits

In addition to helping with configuration assessment, Lacework allows you to check your environment against industry standards. We audit your configuration daily and alert you of any concerning changes, ensuring continuous compliance in your Azure environments. Lacework can help you meet compliance standards including SOC2, ISO 27001, HIPAA, PCI, and NIST. Not only do we generate reports in formats like PDF and CSV, giving you context-rich recommendations to help with all your audits, but we also integrate with tools like Jira and Slack to accelerate your remediation efforts.

Lacework also offers Center for Internet Security (CIS) Benchmarks for Azure, which enables you to assess your security posture according to industry best practices, as well as measure security improvements over time. During container image development and container deployments, we scan across CIS Benchmarks for secure configurations for cloud accounts and workloads.

Why Lacework?

- Assess vulnerabilities at both build and runtime with continuous monitoring
- Detect abnormal activity during runtime, even before a vulnerability is identified, without requiring rules
- Speed investigations with Polygraph visualizations to better understand what happened before, during, and after a specific event

Customer outcomes

- Reduced costs and consolidated technology from several security vendors
- Gained deep visibility across cloud environments
- Improved productivity by investigating alerts 4x faster than before
- Grew business value while preparing for compliance audits
- Reduced risk by building security into the development process

Threat detection

Reduce alert noise and surface only the most critical events with Polygraph anomaly detection support for Azure. Lacework gives you actionable alerts so you can stay on top of behavior changes in your environment, offering automatically built and updated baseline models of a data center's behavior. We'll alert you to all kinds of anomalous behavior, such as a process communicating with an external IP address for the first time ever.

Vulnerability management

With our end-to-end vulnerability management, Lacework helps you identify vulnerabilities sooner, making it easier for you to proactively manage risks across your hosts and containers. We continually assess container images and hosts for new vulnerabilities, as well as changes to existing ones. Plus, once we've identified which vulnerabilities pose the greatest risk to your Azure environment, we provide you with a risk score so you can decide what to prioritize.

> "Lacework identifies all activity happening across all cloud workloads and accounts. Lacework alerts on security events and non-conformations daily. This allows the security team to identify issues and close them almost immediately.
>
> AVINASH RAJU, SENIOR SECURITY ENGINEER, DATAVISORMANAGER, NYLAS

Do you use other cloud service providers? Lacework supports Amazon Web Services (AWS), Google Cloud, and IBM/Red Hat.

AT A GLANCE

What Lacework supports

	Environment			Lacework support
Azure Services	· Azure Kubernetes Services (AKS)	· Google Anthos		Yes
Technologies/OS	· ARM64 · Docker · Docker Swarm · Kubernetes · Kubernetes Helm · Kustomize	· CentOS · Container Linux by CoreOS · CoreOS · Debian · Fedora · Kali	· Oracle Linux · Red Hat Enterprise Linux · Scientific · SUSE · Ubuntu	Yes
Container Registries	· Amazon Elastic Container Registry (ECR)	· Docker Hub · Docker V2 Registry · Github Container Registry	· Google Artifact Registry (GAR)	Yes
Container Runtimes	· containerd	· Docker		Yes
CI/CD Tooling – Automation and Pipelining	· Ansible · BuildKite · Chef	· CircleCI · Github · Harness	· Jenkins · Spinnaker · Terraform	Yes
Integrations – SIEM/ Alerting/Ticketing/ Performance	· ArcSight (Microfocus) · AWS CloudWatch · Cisco Webex Teams · Datadog · Elastic/ELK Stack · Google Pub/Sub	· IBM QRadar · JIRA · Microsoft Teams · New Relic · OpsGenie · PagerDuty	· ServiceNow · Slack · Splunk · Sumo Logic · VictorOps · Webhook	Yes

Ready to chat?

Request a demo