Polygraph® Data Platform: Proactively securing cloud environments at scale

LACEWORK®

Executive summary

The cloud has created massive opportunity for businesses of all sizes to innovate faster at scale. Yet the speed of innovation spurred by cloud services results in an explosion of configuration mistakes and software vulnerabilities that expose businesses to significant risk. In fact, according to the 2020 Bitglass Cloud Security Report, 93% of companies are concerned about cloud security[1], yet the existing tools in the market are not ready to secure modern cloud environments.

To stay secure at cloud speed and scale while eliminating friction between product, development, and security teams, everyone needs to understand exactly what's going on in their cloud environment. Lack of visibility leads to a lack of prioritization and inefficient utilization of limited resources. Developers receive a long list of issues that need to be fixed and redeployed, delaying time to market. This creates a reactive cycle focused on repair, not innovation and customer success.

Organizations need a better way to assess, prioritize, and manage vulnerabilities across their fluid cloud environment. You can reduce costly mistakes by creating a culture that integrates security into every aspect of application design and development, from build to runtime. By interlacing security practices earlier in the software delivery process, everyone wins. Product teams get to focus on designing products that are needed in the market. Developers can engineer with confidence knowing vulnerabilities and misconfigurations will be addressed as early as possible, before code is pushed to production. Security teams can reduce alert noise and focus on real threats facing workloads and cloud accounts that pose risk. By making security accessible to all teams, security moves from a blocker to an enabler of your digital business transformation.

This paper explains the current security and compliance challenges facing organizations today and how the Lacework Platform can provide a single tool for consistent visibility, context, and security for DevOps, IT, and security across your cloud environment.

1. *https://www.cpomagazine.com/cyber-security/most-businesses-concerned-about-cloud-security-but-few-adopt-data-loss-prevention-measures/*

By interlacing security practices earlier in the software delivery process, everyone wins.

Current cloud security challenges

Threats are not slowing down. According to Cybersecurity Ventures, worldwide cybercrime costs are projected to reach $10.5 trillion by 2025.[2] Unfortunately, data breaches are climbing and attackers have their sights set on the cloud.

Existing legacy tools can't keep pace with the speed of cloud innovation. Infrastructure security tools were built for an on-premises and hybrid environment. The dynamic nature of cloud and containerized environments creates blind spots. With multiple tools to manage and operate, staff can't keep up with the manual tooling demands. Organizations with a cloud-first and hybrid strategy need centralized control and a simple automated way to secure the myriad of services, workloads, configurations, APIs, and infrastructure underpinning their business.

In addition, legacy security solutions don't foster shared responsibility and ownership between product, development, and security teams. This lack of visibility can lead to conflict. It's hard to get a unified view of your environment when you have multiple cloud configurations and rapid release cycles without continuous monitoring. Adding to the challenge is the need to keep pace with industry, government, and institutional standards. Operating multiple cloud platforms can increase the attack surface and make it harder to secure your environment and identify misconfigurations and vulnerabilities.

In order to prevent data and cloud resources from being compromised, organizations need a way to automate detection and ensure that development, security, and compliance teams are made aware of issues as soon as they arise. The enormous scale and evolving nature of the cloud creates a massive amount of data that is difficult to interpret. A new approach is needed that ingests, processes, and analyzes an organization's unique data to identify threats or vulnerabilities to better surface the right alert at the right time with the right context. Proactive monitoring and security is the best way to secure cloud environments at scale while maintaining a single source of truth for security.

Cloud computing trends

For IT departments, Infrastructure as a Service (IaaS) is one of the biggest line items on their budget. According to Gartner, spend increased by 41% in 2020.[3] Additionally, as organizations spend more, they are investing in a multicloud strategy. By 2022, Gartner expects 75% of enterprise customers to adopt a deliberate multicloud strategy.[4] Further, Infrastructure as code (IaC) is quickly becoming the primary mechanism to manage cloud infrastructure at scale. According to Gartner, by 2023, 60% of organizations will use infrastructure automation tools as part of their DevOps toolchains, improving application deployment efficiency by 25%.

2. *https://cybersecurityventures.com/cybersecurity-market-report/*
3. *https://www.computerweekly.com/news/252503145/Gartner-IaaS-growth-boosted-during-pandemic*
4. *https://www.gartner.com/en/doc/375973-comparing-multicloud-management-and-governance-approaches*

Introducing Lacework

Lacework is a data-driven security platform that delivers end-to-end visibility into what's happening across your cloud environment from build time through runtime—including detecting vulnerabilities, misconfigurations, unusual activity, and potential attacks.

Lacework learns everything about your cloud environment and narrows it down to what matters most to you. We take millions of incoming data points, correlate them into behaviors, detect all potential security events, and then help you focus on the critical security risks that you need to take action on.

Lacework also helps customers "shift left," making it easier to interlace security practices earlier in the software delivery process, before code goes live. This creates harmony across teams so your product managers can focus on design, your developers can innovate quickly, and your security team can be confident they are detecting difficult-to-identify attacks against servers and infrastructure, securing misconfigurations and demonstrating compliance with industry regulations. Better visibility into all major public and private clouds, on-prem, and workloads enables our customers to detect the events that matter the most, and provides the context to investigate and speed remediation efforts.

The Polygraph® Data Platform

Lacework is purpose-built as a platform with a single detection engine, user interface, and API framework. With Lacework, your team only needs to learn one system for all of your cloud and workload protections leading to tool consolidation, greater organizational efficiencies, and cost savings.

How it works

Lacework captures, analyzes, and baselines your cloud activity to spot anomalies in your applications, container activity, and user behavior, alerting you only when something deviates from your norm. By taking a data-driven approach to security, the more data you put in, the smarter the Lacework platform gets. This automated intelligence drives better efficacy and a higher return on your investment. With a single UI to learn, one set of APIs, one agent, and one common language, Lacework seamlessly fits into your existing cloud environment to protect workloads and cloud accounts.

Lacework simplifies deployments for even the largest and most unique cloud environments. Lacework Terraform modules accelerate deployment and integration with alert channels to optimize response and remediation workflows. In addition, customers can use the Lacework CLI to integrate with inline scanner for container image and registry scanning. With Lacework, you can securely build, run, and grow your use of the cloud, and transform security from a blocker into an enabler that drives your business forward.

Driving business outcomes that matter

Support revenue, innovate faster

Unlocked $10M in new business — HYPER GIANT

Improve productivity

Sped up investigation time from 3 hours to 15 minutes — snowflake

Reduce risk

Reduced annual risk by $1.1M; cut security bill in half — lendingtree

Reduce costs

Reduced security spend by 50% in 6 months — sift science

Key use cases

Lacework customers primarily leverage our platform to solve the following key use cases.

1) Maintain cloud posture and compliance

Lacework provides the visibility and context you need to know what is happening in your multicloud environment at any time. We eliminate the guesswork so you can quickly identify all of your assets, find misconfigurations, and be aware of compliance violations to reduce risk and exposure.

2) Uncover and manage vulnerabilities

Unlike traditional vulnerability management tools that were not built to secure modern cloud environments, Lacework helps you assess risk, prioritize action, and maintain a secure cloud environment to protect against vulnerabilities. Lacework achieves this by scanning containers, container registries, and hosts for OS and third-party packages earlier in the development process and can be integrated into your CI/CD pipelines. Lacework tracks containers and hosts into runtime to discover any abnormal activity that could exploit potentially unknown vulnerabilities. Security teams are empowered to spot vulnerabilities and provide remediation guidance to developers in an easy to understand dashboard, prioritized by risk.

Lacework helps you assess risk, prioritize action, and maintain a secure cloud environment to protect against vulnerabilities.

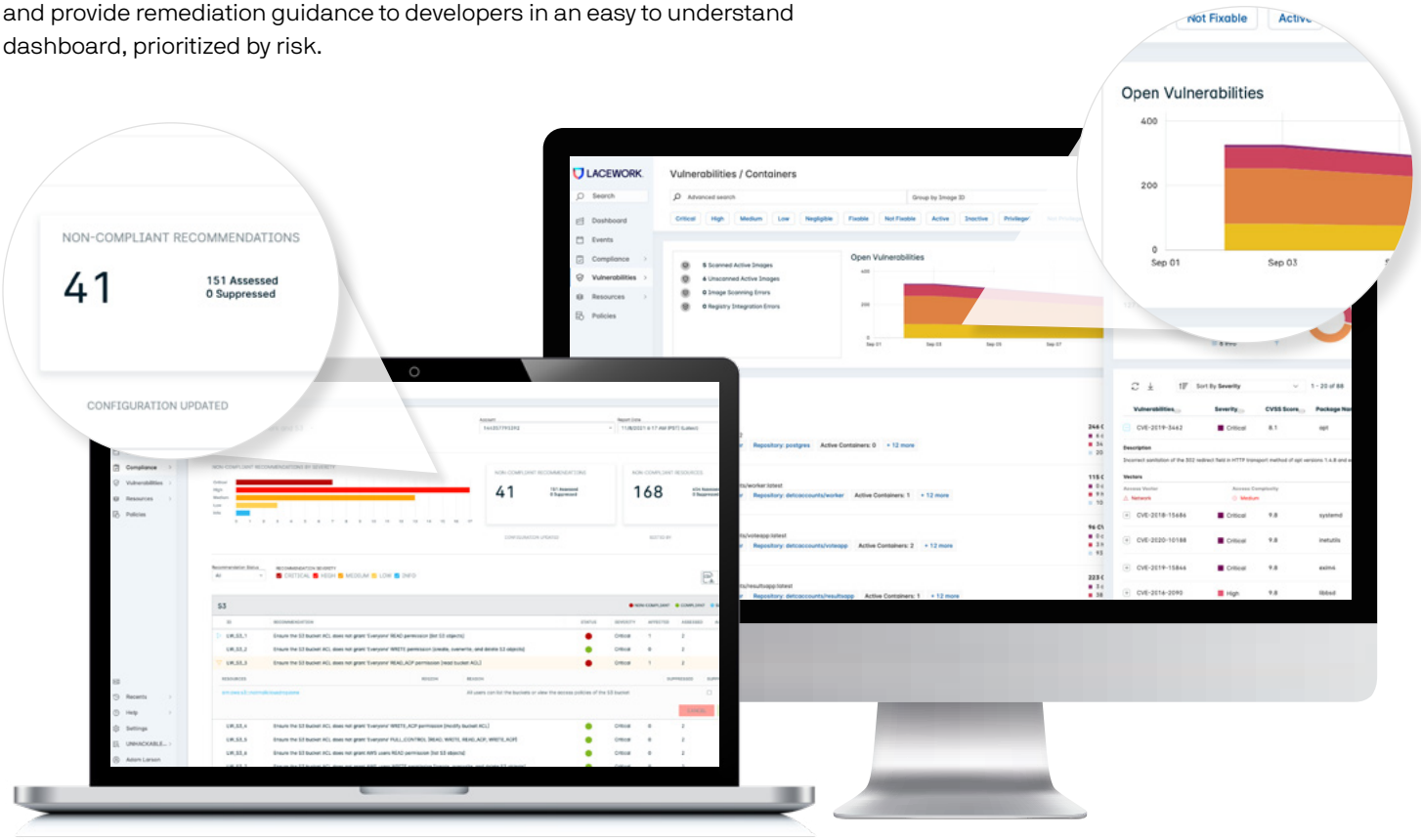


Figure 1 (left): Shows AWS Compliance Report. Easily understand posture with pre-built policy checks for AWS, Azure, and Google Cloud.

Figure 2 (right): Shows container vulnerability overview and additional details on the CVEs present. Better assess vulnerabilities and their severity in your environment.

3) Streamline threat detection

Unlike existing cloud workload protection platforms that require extensive tuning, Lacework detects deviations from normal behavior across your cloud infrastructure without generating excessive alerts. Lacework identifies malicious behavior during runtime at the cloud infrastructure level across AWS, Google Cloud, and Azure, as well as cloud activity in Kubernetes, VM workloads, and containerized workloads. Not only can your organization uncover a wide variety of threats such as cryptominer attacks, unusual logins, and escalation of privileges, but you can also proactively discover misconfigurations, as well as rare but legitimate changes in the use of your cloud resources. As threats are surfaced, security event details are provided in a comprehensive event card that displays the who, what, why, where, and when of each event along with a graphical representation to speed investigations. These actionable alerts enable organizations to streamline threat detection easily.

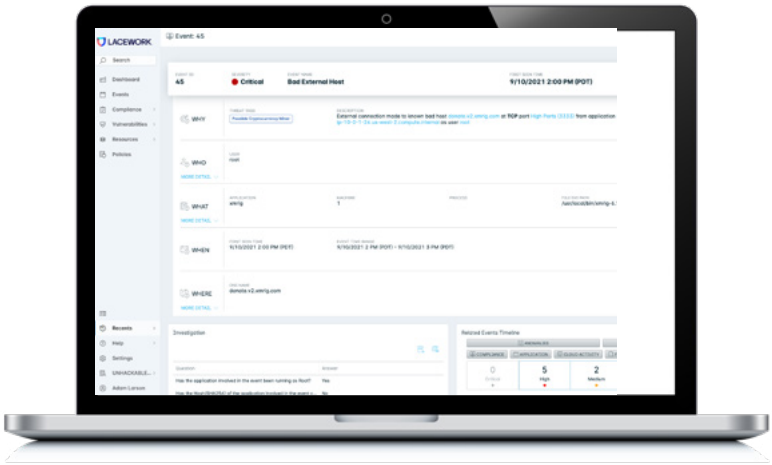


Figure 3: Shows critical event details. Get context—the five Ws—to speed incident response and investigation.

4) Interlace security with development

Multiple tools lead to data silos, finger pointing, and lost productivity. Lacework was designed from the ground up to bring security operations, security leaders, and developers together with a platform that makes security data accessible, improves communication, and makes it easier for everyone to share the responsibility of security. Lacework alerts are surfaced in the user interface, but can also be delivered via messaging and security ticketing tools. A modern alerting experience helps teams better collaborate to prioritize, investigate, and track the status of all alerts from one place. They can more easily organize alerts, view tags, search using advanced filters, comment on alerts, and change the state of an alert to indicate whether it needs to be investigated or closed. And they can make better decisions with context-rich insights that give a complete picture of what happened, associated events, timelines, etc. Configurable bi-directional sync between Lacework and Jira enables your teams to communicate about the status of alerts and tickets for faster investigation and response.

Lacework identifies malicious behavior during runtime at the cloud infrastructure.

Polygraph®: our data-driven "secret sauce"

Lacework was founded on the principle that security is a data problem, so we built our platform to ingest various cloud data sources from AWS, Azure, and Google Cloud activity in a visual way. Lacework Polygraph automates detections at scale and enables organizations to reduce complexity and focus valuable resources more effectively by alerting only on the events that matter.

A different no-nonsense, rules-optional approach

Not only does Lacework collect hundreds of millions of data elements about your cloud environment, but we automatically learn what's normal and only send alerts based on changes to your baseline. Lacework is a rules-optional platform that is capable of addressing 95% of an organization's use cases without writing a single rule. For specific use cases, we support the use of custom policies through our Lacework Query Language (LQL). Simply put, we eliminate guesswork, cut noisy alerts down to a whisper, and reduce investigation time by up to 80%.

How it works

Polygraph is our patented technology engine that processes billions of interactions and distills them down to a handful of critical alerts. In addition to creating visual representations of all the connections to make investigations easier for security and DevOps teams, Polygraph automatically provides the context required to remediate alerts effectively. Other tools produce hundreds of alerts per day. Lacework, on average, cuts that noise down to a handful of critical or high severity alerts per day. Despite the ever-changing cloud landscape, our machine learning recognizes patterns and deviations automatically to uncover new behaviors.

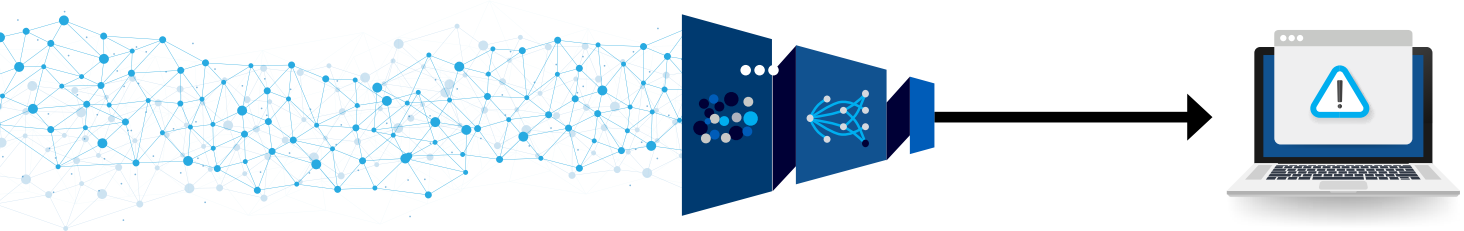
Massive data scale: In order to accurately analyze your cloud infrastructure and provide meaningful insights, Lacework collects high fidelity process, network, file, and user data along with cloud activity events from AWS, Azure, and Google Cloud to form a model of normal infrastructure behavior. Lacework also tracks changes in activity frequency and volume over time to detect unusual activities in existing cloud environments. By ingesting hundreds of terabytes of data each day from multiple data sources, we understand what your normal baseline looks like and can accurately and automatically detect anomalies in your environment.

Data modeling: The data produced by cloud service providers is often semistructured, unstructured, and constantly evolving. Adding to the complexity, each customer's environment is unique and normal activity varies dramatically between accounts. Therefore, it is critical to create data models that adapt to our customers' environments and can seamlessly identify even subtle changes at scale and with meaningful end-to-end context. To achieve this, Lacework has spent years perfecting a data modeling approach with careful data warehouse management to process our customers' data. Our cloud behavioral analytics engine uses a number of models, including time series analysis, to build baselines that are tailored to your unique environment.

The power behind Lacework: Polygraph® Data Platform

Lacework learns what's normal and alerts on anomalies — leaving rules optional

Ingest	Analyze	Detect
API, user, app, process, and network data in real-time	Autonomous machine learning, behavioral analytics, time series analysis, and anomaly detection	Anomalies and threats



Machine learning: Lacework has robust machine learning (ML) capabilities that automatically cluster processes into groups of related activity and identify the applications in use. We understand which entities are similar to each other and cluster them accordingly. We then use sophisticated analytics and machine learning techniques to detect anomalies that may indicate threats. This allows us to find the "needle in the needlestack" that no human could detect or even write a rule to detect. We can surface the one connection out of a billion that is anomalous and, just as importantly, not surface the events that would ordinarily trigger an event with other security tools but are actually considered typical for your environment.

Baseline your environment: Lacework can be deployed in your environment with a simple process and within a few days, the Lacework engine quickly builds a baseline that is indicative of your organization's "normal." Over time the baseline adapts as new data has greater statistical impact over a smaller sample size. The more data we ingest and the more activity we observe, the smarter the platform gets.

This allows us to find the "needle in the needlestack" that no human could detect or even write a rule to detect.

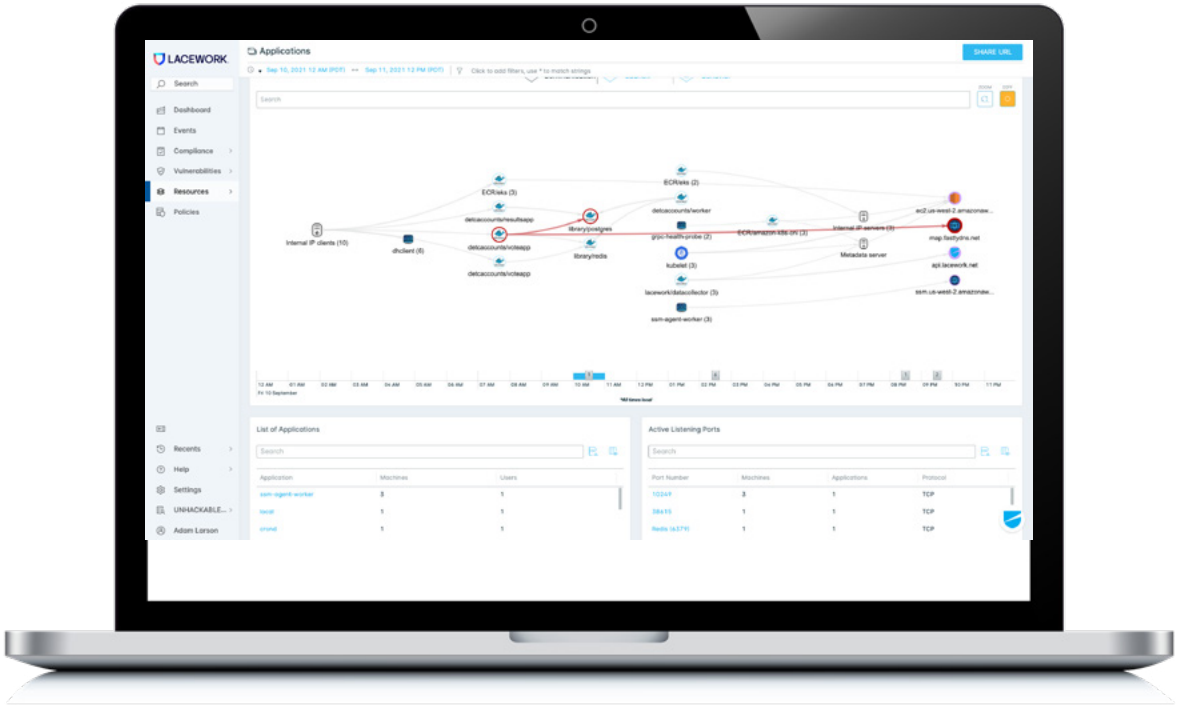


Figure 4: Shows Polygraph visualization. Quickly identify anomalous communication paths and malicious activity.

Extend visibility with a layered approach

At Lacework, we can help you cut complexity and achieve a comprehensive view across AWS, Google Cloud, and Azure by bringing multiple clouds into a consolidated dashboard. Lacework uses a combined agentless and agent-based approach to gather the right level of information. This includes industry best practice integrations directly to cloud providers' APIs, as well as gathering telemetry directly from your workload with the Lacework agent. Our agentless solution detects attacks, misuse, and misconfigurations in cloud accounts while our agent-based approach monitors for workload vulnerabilities as well as for known and potential threats related to users, applications, network connections, and files. This method provides greater visibility to your assets, their connections, and their compliance with industry, governmental, and institutional standards from build time through runtime.

The power of agentless and agents

Agentless coverage alone isn't enough. A layered approach provides the right coverage for the right environment and use case. The Lacework agentless coverage works side-by-side with our agent coverage to provide complete visibility across your cloud for the best protection possible.

The Lacework user interface guides you through setting up integrations with cloud accounts to quickly achieve agentless coverage. Once connected to AWS, Azure, and/or Google activity and configuration logs, you will have all of the data sources you need to achieve continuous configuration compliance and account-level threat detection.

Combined agentless and agent-based approach

The right level of data in the most effective way possible.

What's happening **in your cloud accounts**

Agentless

For Cloud Accounts

- AWS, Azure, Google Cloud
- Continuous monitoring of cloud configuration
- Compliance checks
- Account threat detection
- IaC and cloud account scanning for misconfigurations
- Custom policies for control plane
- Kubernetes activity log monitoring
- Kubernetes Admission Controller
- Container/host application language library/cloud workloads vulnerability assessment (software supply chain risk)

What's happening **on your systems**

Agent

For Cloud Compute

- Kubernetes, container, and workload runtime visibility
- Host intrusion detection
- File integrity monitoring
- User, app, process, and network behavior monitoring
- Container/host vulnerability (runtime correlation, CI/CD integration)

Agentless coverage: what's happening in your cloud accounts

- What services are being accessed?
- Who/what is accessing those services?
- What behaviors are different compared to your standard?
- What configurations have been deployed and are they compliant?

The Lacework "Un"Agent

Deploying our agents allows for deep and contextual insight into containers and hosts. They also provide enhanced visibility across users, processes and applications within cloud and container environments to improve threat detection, incident investigation, and triaging.

Lacework agents are adaptive and lightweight to meet the specific security needs of organizations dependent on rapidly changing clouds and containers. Designed with data security at their core, our agents enable efficient usage of resources for optimum performance.

Multiple microservices can run within a single host in a containerized environment. The data required to understand the properties within a container at the network level is only visible from within the host. Custom applications are also able to be monitored with agent-based monitoring due to the deeper data retrieval capabilities. Lacework agents only communicate unidirectionally (outbound), making it more secure and well-suited for a high-security environment.

Lacework agents give you access to:

- Processes running on the host
- Processes running in a container that make a network connection (server or client)
- All container internal servers and processes that are listening actively on certain ports
- File Integrity Monitoring (FIM) on the host
- Host vulnerability

Agent coverage: what's happening on your systems

- What is running?
- What's it talking to?
- Who's accessing what?
- What behaviors are different compared to your standard?
- What vulnerabilities exist and are the packages active?

This is not your parent's agent.

The Lacework agent is quick to install and can be deployed with configuration management tools (Chef, Puppet, Ansible, Salt) or via the Lacework installation script. Plus, it can be automatically updated when a new version is available for easy maintenance.

The Lacework agent utilizes approximately 250 MB of storage space on a machine. The number of connections made by the host determines the CPU impact on an individual system. For an average workload, Lacework has observed a CPU usage of 1-3% (250-300 MB), but this can vary depending upon the number of connections. It is also configurable so you can set a limit for agent memory usage. Furthermore, the impact on network resources is quite low, typically 1-2 Kbps, which translates to approximately 100-150 MB per system per day of data.

Designed with data security at their core, our agents enable efficient usage of resources for optimum performance.

Summary

Cloud security is a data problem. In the cloud, you're dealing with evolving technologies, adaptive infrastructure, and the need to deploy and scale quickly — traditional security approaches can't keep pace with the constant changes. It's time for a change.

To operate successfully in modern IT infrastructures, you have to reset how you think about security in the cloud. A shortage of security talent can make it even harder to cope with the increased threats and data security demands. Yet just adding more tools won't solve the problem. Point solutions plug holes, but they also create more blind spots, silos, and added complexity. With more tools comes more management and even more alerts to review. Trying to unify multiple disparate tools in order to focus on what matters most is challenging due to the explosion of data.

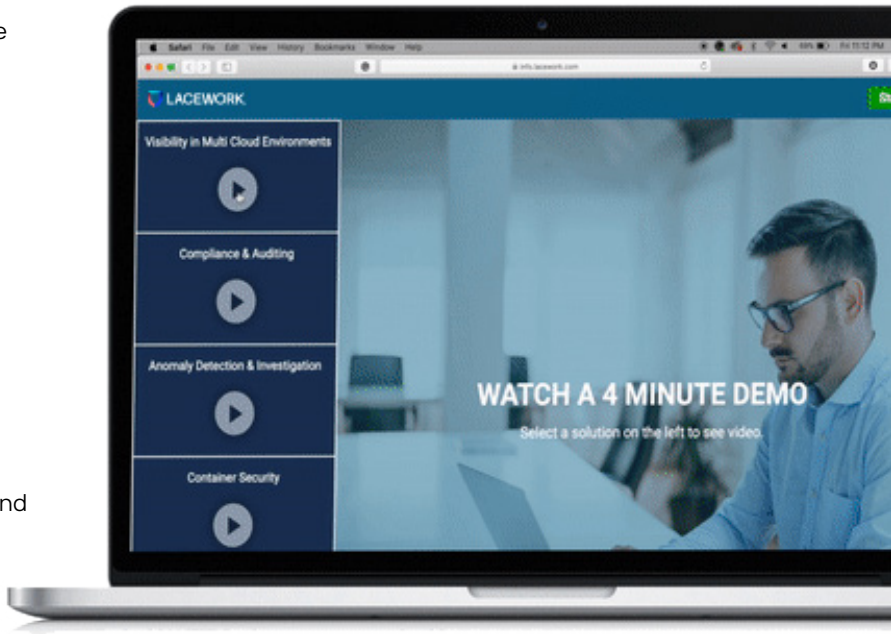
Lacework enables you to monitor cloud infrastructure and analyze and contextualize billions of interactions across cloud workloads and accounts. It brings development and security resources together by shifting security earlier into the development process and making activity data accessible to everyone. Lacework ingests, processes, and analyzes behavioral activity to provide the best visibility into exactly what's happening across your cloud environment. By analyzing data at scale, Lacework streamlines the noise and provides the right alert, at the right time, with the right context so you can take the right action for your business and safeguard your cloud data.

Next steps

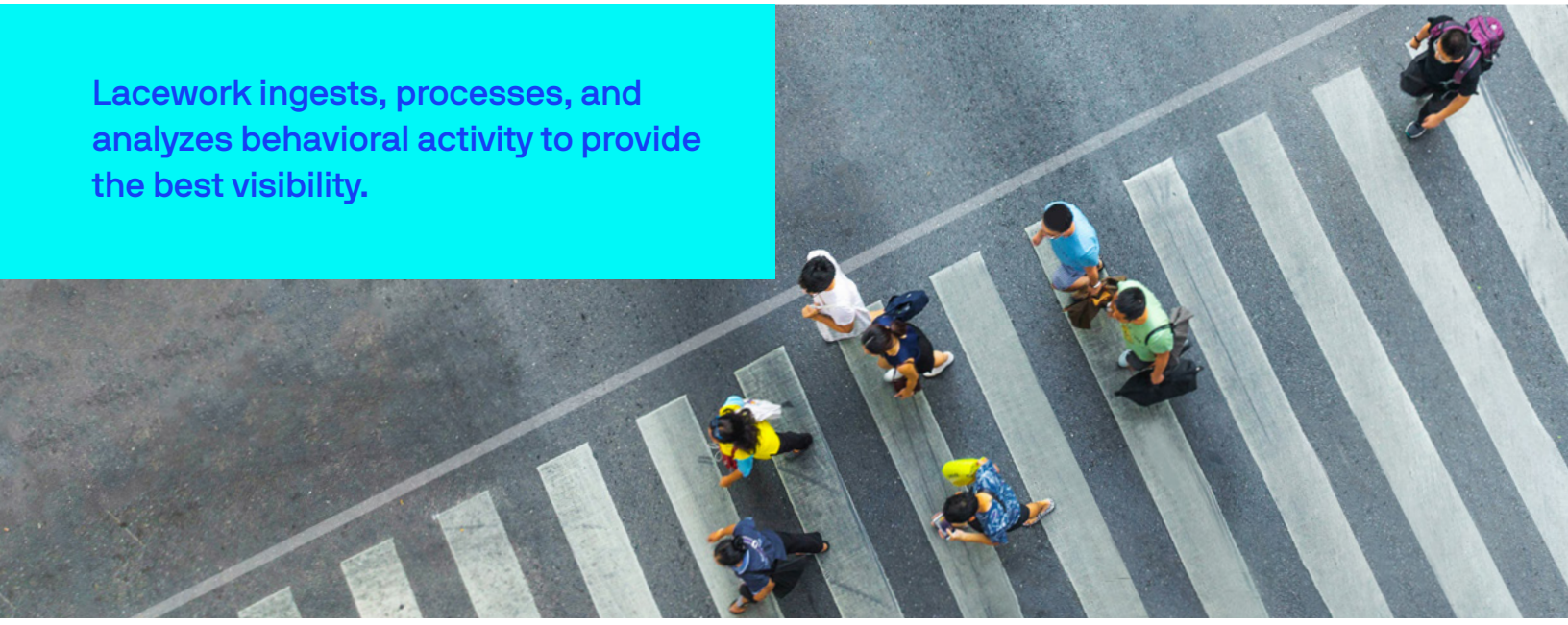
Engaged with our sales team already? If not, sign up to see how Lacework can help you automate security and compliance across AWS, Azure, Google Cloud and any private cloud:

Four-minute demo video:
https://info.lacework.com/4-Min-Demo-A-SEM.html

Request live demo:
https://info.lacework.com/contact



Lacework ingests, processes, and analyzes behavioral activity to provide the best visibility.



Consolidate tools and amplify existing investments

Lacework is built to work seamlessly in your existing environment. If you're using a Security Incident and Event Management (SIEM), you can pre-process cloud logs to eliminate rule writing, reduce the amount of alerts, and decrease the associated cost consumption component of your SIEM by up to 40%. Lacework enables customers to consolidate multiple tools for greater efficiency. With Lacework you can simplify management tasks, accelerate workflows, improve analytics, and free up budget to focus on innovation, not repairs.

For a complete list of all of the supported operating systems, please visit: https://support.lacework.com/hc/en-us/articles/360005230014-Supported-Operating-Systems

Cloud Platforms	X86 Architecture Operating Systems	ARM64 Architecture Operating Systems	Container Runtime Support
AWS	Alpine Linux (General beta support)	Amazon Linux	ContainerD
Google Cloud	Amazon Linux	CentOS	CRI-O
Azure	Amazon Linux AMI	Debian	DockerD
	CentOS	Fedora	
	Container-Optimized OS from Google	Redhat Enterprise Linux	
	Debian	SUSE	
	Fedora	Ubuntu	
	Kali GNU/ Linux Rolling	Rocky Linux	
	Oracle Linux		
	Redhat Enterprise Linux		
	SUSE		
	Ubuntu		
	Rocky Linux		

Ready to chat?

Request a demo