FORRESTER®

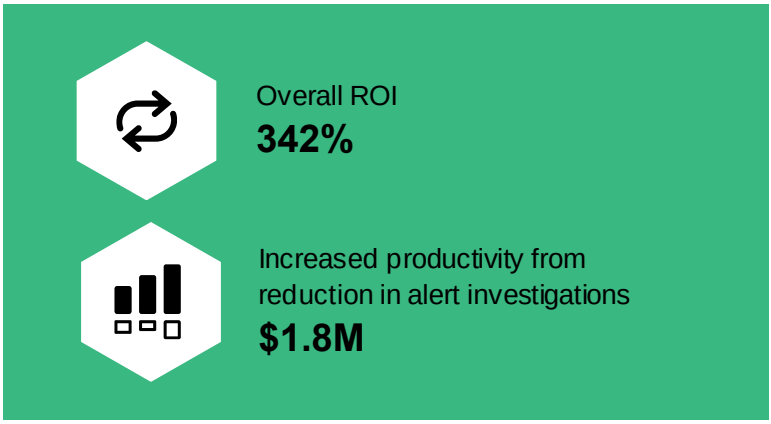
Lacework Uncovers Unusual Behavior In Cloud Environments, Increasing Productivity And Reducing Alert Investigations

Cloud-enabled businesses face ever-evolving cybersecurity risks. They receive a high quantity of security alerts daily but typically lack an intelligent automated solution that can filter out extraneous alert noise and easily identify unusual behavior that may indicate compromise.

The Lacework Polygraph® Data Platform uses data and automation to provide end-to-end visibility across businesses' cloud environments to identify threats, misconfigurations, vulnerabilities, and unusual activity.

To better understand the benefits, costs, and risks associated with the platform, Lacework commissioned Forrester Consulting to interview seven decision-makers and conduct a Total Economic Impact™ (TEI) study.[1]

This abstract, built from the experiences of the seven interviewed customers, will focus on Lacework's ability to reduce alert investigations and increase security team productivity.



CHALLENGES

Some of the challenges interviewees' organizations faced prior to implementing Lacework included:

- **High volume of unactionable and time-consuming security alerts.** Interviewed customers' security professionals were experiencing alert fatigue from investigating countless, often unactionable, alerts.
- **Lack of real-time and unified visibility over infrastructure.** Interviewees had limited visibility across their cloud environments. They often had to wait more than 24 hours for results from alternative solutions that provided periodic risk assessments.
- **Managing numerous legacy tools.** Multiple tools and monitoring applications provided overlapping functionality. This caused personnel to waste time searching for information they could otherwise consolidate.

WHY LACEWORK

Interviewees' organizations that implemented Lacework were searching for a solution that could:

- **Provide a unified way of seeing what was running across different services in a consolidated view.** Lacework supplied

READ THE FULL STUDY HERE

interviewees' organizations with unified, end-to-end monitoring of their cloud environments.

- **Enable a robust, instant detection capability**. A chief information security officer at a communication platform noted, "Across 90 days, Lacework has processed 31.9 billion events, yielding about 250 events [that required further] investigation by our team."
- **Improve compliance readiness to win contracts.** A VP of DevOps and cybersecurity at an AI enterprise software firm said that because of Lacework, "[Our organization] achieved the necessary compliance to win more than $10 million in new business."
- **Increase speed of deployment, time-to-value.** One interviewee, a chief information security officer at a communication platform said, "Lacework took only a couple hours to fully deploy to our entire technology stack, providing immediate insight and value."

KEY RESULTS

The deployment of Lacework produced curated alerts that reduced alert noise, fatigue, and workload for the interviewees' organizations' security teams. Additionally, findings revealed that Lacework provided greater context for faster and more effective investigations by consolidating related security event information into alert dossiers. These reports helped reduce manual burden on staff and provided organizations with:

- **Increased productivity from reduction in alert investigations.** Lacework's Polygraph Data Platform helped organizations realize an increase in productivity by learning how their environment runs and taking the guesswork out of writing static rules. Lacework used patented machine learning to collect and analyze terabytes of data, bring anomalies to light, and provide a history and visualization to streamline investigations.
- **Automated alert aggregation processes.** Consolidating alert information across the interviewees' organizations' entire cloud environments allowed security personnel to achieve higher levels of productivity. This was done by minimizing time spent on relatively unproductive manual tasks and allowing them to focus on actionable alerts.
- **Reduced the total number of alerts.** The interviews for the TEI study found that Lacework's curated security alerts reduced notifications for security teams by 86%. A VP of DevOps and cybersecurity at an AI enterprise software firm, noted, "We were able to immediately start getting actionable alerts and auditing our environments." By reducing the total number of alerts, Lacework curtailed security professionals' less productive activities, allowing them to focus on more value-added activities, such as threat hunting.
- **Improved context of alerts for prioritized and quicker action.** Interviewees noted that in addition to reducing the total number of alerts, the alerts Lacework provided were actionable. This resulted in a more robust approach to threat detection and a secure cloud environment. A VP of DevOps and cybersecurity at an AI enterprise software firm said: "[Lacework's platform is] not noisy, we can easily look at the raw data to see what's going on. We're getting more high-quality events — about three [actionable] alerts a day."
- **Increased focus on strategic security initiatives.** With Lacework's automated alerting and anomaly detection, the security team could dive into more strategic initiatives that require human expertise. A director of security operations at an email and SMS marketing automation company commented, "[Lacework allowed our team] to focus on advanced threat hunting and risk reduction."

- **Increased confidence in deployment.** Lacework continuously monitored changes in the client's cloud and infrastructure-as-code (IaC) environments and assessed the posture and compliance against security and industry standards such as PCI (Payment Card Industry), HIPAA, NIST, ISO 27001 and SOC2 (Service Organization Control 2). Lacework provided the security operations teams assurance that it would identify modifications that might introduce risk to a compliant environment. A cloud security architect at a cloud-based platform noted, "[Lacework gave us] the ability to confidently rollout into new environments while [compliant] with GDPR."
- **Harmonized security and development team relationships**. Lacework allowed checks and controls to be integrated into development's continuous integration (CI) tooling, giving development teams access to vulnerability details, an understanding of which vulnerabilities were most important to fix, and the context to correct issues. Security was no longer the bad cop chasing development teams to fix issues. They could be a partner that helps developers remediate issues. As a VP of DevOps and cybersecurity at an AI enterprise software firm noted, "[Lacework] democratized access to security event data and incorporated security directly into the development process."

TOTAL ECONOMIC IMPACT ANALYSIS

For more information, download the full study: "The Total Economic Impact™ Of Lacework," a commissioned study conducted by Forrester Consulting on behalf of Lacework, January 2022.

STUDY FINDINGS

Forrester interviewed seven decision-makers at organizations with experience using the Lacework and combined the results into a three-year composite organization financial analysis. Risk-adjusted present value (PV) quantified benefits include:

- Increased productivity from reduced alert investigations, worth nearly $1.8 million over three years.
- Reduction in cost of licenses for legacy tools, worth $230,000 over three years.
- Avoidance of hiring additional security compliance professionals, worth $291,000 over three years.

Return on investment (ROI)

342%

Net present value (NPV)

$1.79M

Appendix A: Endnotes

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

DISCLOSURES

The reader should be aware of the following:

- The study is commissioned by Lacework and delivered by Forrester Consulting. It is not meant to be a competitive analysis.
- Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in Lacework.
- Lacework reviewed and provided feedback to Forrester. Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning.
- Lacework provided the customer names for the interviews but did not participate in the interviews.

ABOUT TEI

Total Economic Impact™ (TEI) is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders. The TEI methodology consists of four components to evaluate investment value: benefits, costs, risks, and flexibility.

© Forrester Research, Inc. All rights reserved. Forrester is a registered trademark of Forrester Research, Inc.

FORRESTER®