SOLUTION BRIEF

LACEWORK

Why Lacework for fintech

How our platform can ease the burden of financial data security

"The security threat landscape is constantly evolving. We have to approach situations much differently these days than we have prior."

John Turner, Senior Security Architect at LendingTree, is no stranger to the challenges of securing cloud data. "Cloud security for us is critical. We try to build the foundations of security into everything we do, from the earliest stage possible... to both protect our consumers' data and our company's brand reputation."

Today, fintech companies like LendingTree are on the rise. Experts predict the fintech market will be worth $332.5B by 2028 — nearly 3 times its value today.[1] Yet, in the face of growth, fintech companies face a unique two-pronged challenge.

First, the same cloud that helped fintech companies gain a unique advantage is being exploited by cyberattackers. In 2021, finance was the second-most attacked global industry.[2] Second, finance — like healthcare — is an industry where trust can be broken in an instant. Sixty-six percent of consumers said that they would stop using a financial institution if there was a data breach affecting their data.[3]

Every day, Lacework helps fintech companies secure consumer trust through a different approach to cloud security. For fintech companies, Lacework can help:

- Drastically cut down on threat dwell times
- Address risks while building code, without slowing down development
- Automatically benchmark against compliance standards

"Lacework helped us deal with this firehouse of information that we were getting out of our cloud environments, almost out of the gate. We were able to go from a couple of hundred alerts a day down to just a handful. I'm talking less than 5."

JOHN TURNER, SENIOR SECURITY ARCHITECT, LENDINGTREE

WATCH THE LENDINGTREE STORY >>

Limit the damage of cyberattackers

Reduce mean time to detect (MTTD) from 207 days to immediate

Visibility is a major issue for companies of all sizes and industries. When cloud resources live seemingly everywhere, it's difficult to identify risks and pinpoint threats that may already be living in your environment. Many modern cloud security vendors are focusing solely on vulnerability discovery and cloud security posture management (CSPM) to gain visibility into cloud environments.

Vulnerability discovery involves scanning infrastructure as code (IaC) configurations and application code for vulnerabilities pre-deployment. In production, vulnerability discovery involves identifying risks by monitoring container images, application dependencies, and/or host packages. CSPM involves identifying risks in production by monitoring infrastructure configurations within cloud accounts.

Lacework supports both of these important use cases; the advantages of each are discussed later in this brief. However, as cyberattackers become more sophisticated, one cannot assume that proactively identifying vulnerabilities in a cloud environment is enough to ward off bad actors. After a breach occurs, what happens then?

According to the *IBM Cost of a Data Breach Report 2022*, the average amount of time to identify a data breach is 207 days.[4] That is 207 days of an active threat secretly extracting data from your cloud environment. Given the elusive nature of modern threat tactics like cryptojacking and data exfiltration, this average is likely to increase. And a tenth of this dwell time is enough time for bad actors to steal private customer data and put it up for sale.

With Lacework, you can cut down MTTD from 207 days to real-time — something that many other vendors cannot claim.

The power of behavior-based threat detection

The Lacework platform — what we've termed the Polygraph® Data Platform — collects high-fidelity machine, process, and user interactions over time and combines these into behavior models. Polygraph can then monitor your infrastructure for any activities that fall outside of those normal behavior models, in real-time.

These abnormal actions are flagged as anomalies, which are raised up as alerts. Within every alert, Polygraph plots the abnormal action within a map of your typical behavior model and helps users quickly visualize key contextual information for remediation — who triggered the event, what was the event, when did it happen, where did it happen, and how far did it reach.

Polygraph uses deviation from a temporal baseline to detect changes in behavior, which results in meaningful alerts. Alerts are either due to a desired change, a misconfiguration, or malicious activity. Polygraph then automatically scores the alerts based on severity and threat.

This behavior-based approach is fundamentally different from any other cloud security product on the market. Rather than applying rules and policies against what we "think" might happen, we generate events based on deviations from what we actually know to be "normal." This approach, combined with third-party feeds identifying "known bads," can spot even the most elusive of threats in a fraction of the average MTTD.

With Lacework, you can bank on higher quality events, lower false positives, and less alerts.

Don't sacrifice development speed for security — you can have both

While financial services is the second-most attacked global industry, fintech is also extremely competitive. Pressures to ship code fast can lead to accidental mistakes, misconfigurations, or security gaps that open the door for malware.

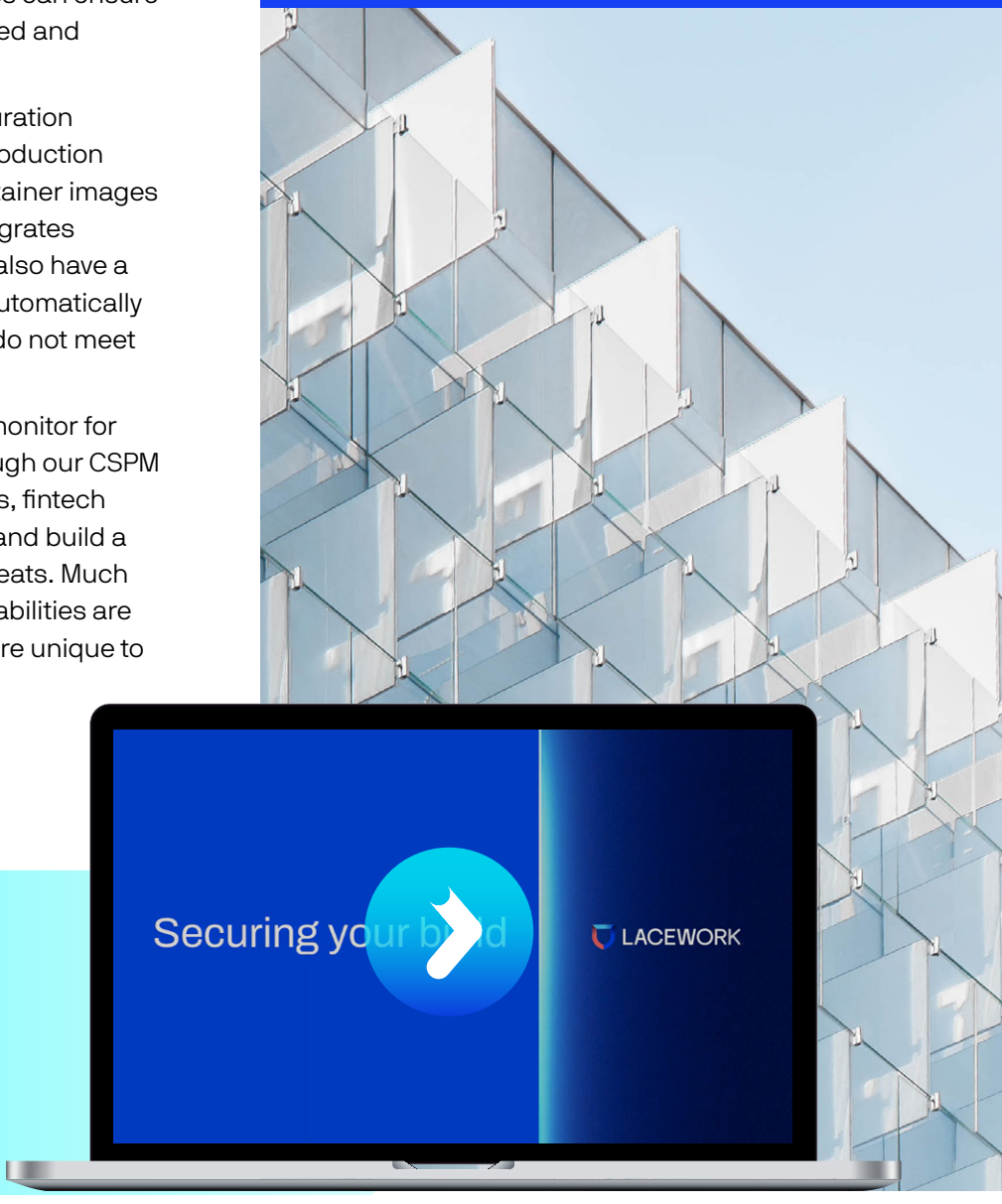
A recent study showed that finance was joint last with two other industries when it comes to the lowest proportion of software flaws that are fixed. According to the study, 18% of applications in the financial services industry contain a serious vulnerability that remains unaddressed.[5]

The most inexpensive place to fix security flaws is in the build phase, yet pressures to build and ship fast keep fintech developers from implementing the right security protocols. With Lacework, fintech companies can ensure that both of these aims — development speed and security — are met.

Our IaC scanning can identify cloud configuration issues in development before they reach production environments. Our platform can check container images in build time with an inline scanner that integrates with continuous integration (CI) tooling. We also have a Kubernetes admission controller that can automatically block or notify you when container images do not meet security standards.

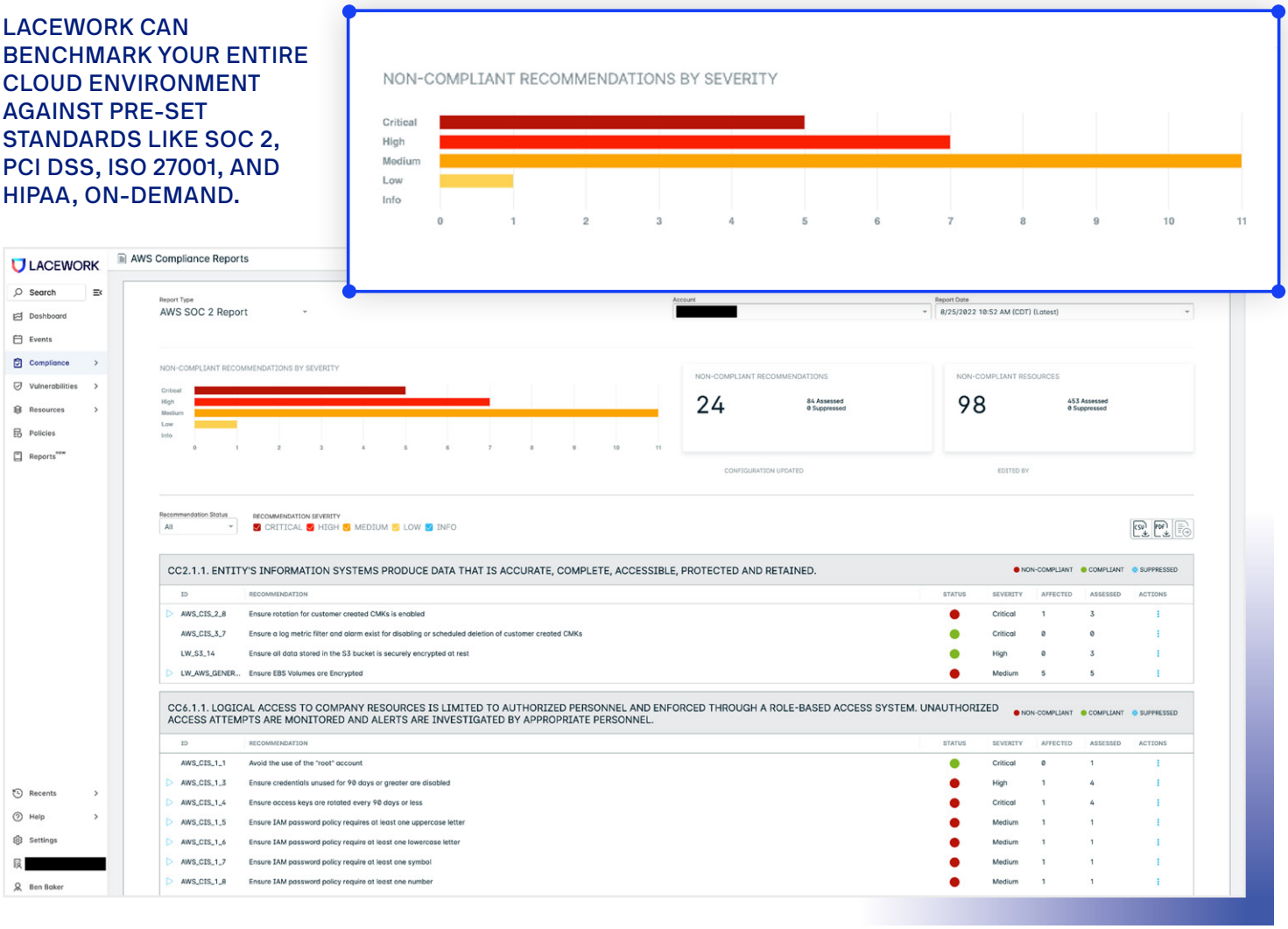
Beyond build time, Lacework continues to monitor for vulnerabilities and misconfigurations. Through our CSPM and container image monitoring capabilities, fintech companies can monitor and address risks and build a reliable line of defense against potential threats. Much like our threat detection capabilities, vulnerabilities are presented in a prioritized list, with a risk score unique to your unique cloud environment.

Lacework provides cloud and multicloud protection by automating cloud security and compliance across AWS, Azure, Google Cloud, and private clouds, while providing a comprehensive view of risks across workloads and containers.



WATCH HOW LACEWORK CAN SECURE YOUR BUILD >>

LACEWORK CAN BENCHMARK YOUR ENTIRE CLOUD ENVIRONMENT AGAINST PRE-SET STANDARDS LIKE SOC 2, PCI DSS, ISO 27001, AND HIPAA, ON-DEMAND.



Take some pain out of compliance

Cloud dependence comes with cloud complications. A critical one for nearly everyone — and one that is pivotal for a highly regulated industry like finance — is compliance. For fintech companies, demonstrating compliance can be especially challenging, since financial regulation varies from country-to-country and can be seen as an inhibitor to innovation. Regardless, compliance is necessary, as lack of compliance can carry hefty penalties.

To satisfy customers and auditors, businesses must demonstrate compliance with standards like SOC 2, PCI DSS, ISO 27001, HIPAA, and GDPR on a regular basis. Cloud services change too fast to be accurately reflected in any kind of manual reporting. And many processes running in high-velocity hybrid and multicloud computing environments are simply not visible to standard compliance reporting tools.

Much (though not all) of the pain of compliance can be solved through automation. Lacework can automate these types of audits by gaining a comprehensive view of your cloud environment and mapping the associated controls to the required cloud security controls.

Lacework reports can be run at any point in time to review compliance against your multicloud and multi-account environment, allowing your compliance team and cloud team to work together to ensure continued compliance to those standards.

Lacework reports can also be run and reviewed over different time periods, so any compliance drifts can be reviewed and investigated. Our platform saves you time and money by preventing issues before the audit and by reducing the evidence gathering time during the audit.

The rewards of securing enterprise cloud infrastructure

The positive outcomes benefit the entire enterprise:

Security Visibility
Get deep observability into and across 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 take 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 and security best practices that could put your company at risk.

Endnotes
1 Vantage Market Research. (2022, May). Fintech market size USD 332.5 billion by 2028.
2 Singleton, C., DeBeck, C., et al. (2022, February). X-Force Threat Intelligence index 2022. IBM Security.
3 Principato, C. (2022, June). Most Trusted Brands 2022 - Trust in banking, investment and payments. Morning Consult.
4 Ponemon Institute LLC. (2022, July). Cost of a Data Breach Report 2022. IBM Security.
5 Veracode Inc. (2022, August). State of Software Security, Volume 12: The Progress We've All Made.

Want to see more?

Watch demo videos

Get a live demo