Lacework

Visit Website

Lacework is a SaaS security solution for containers and multi-cloud deployments.

#data-security

REVENUE
$90,000,000
2022

VALUATION
$8,300,000,000
2022

GROWTH RATE (Y/Y)
125%
2022

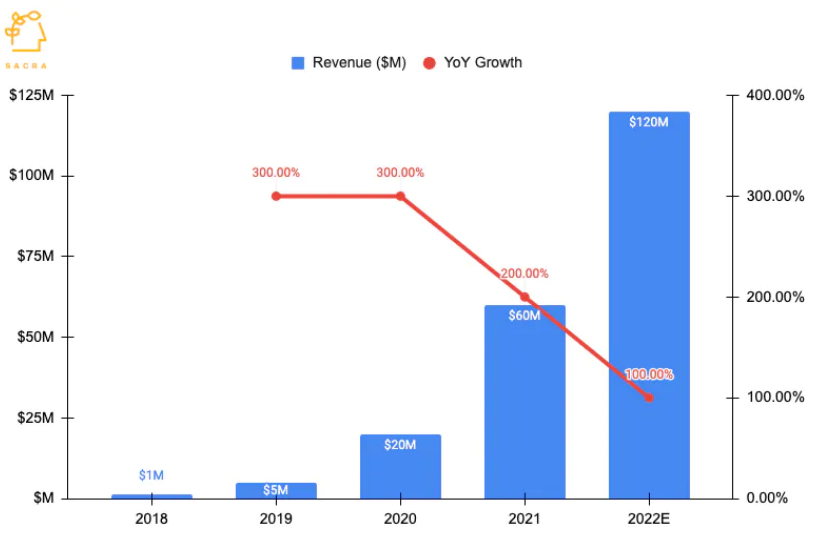
FUNDING
$1,900,000,000
2022

Details

HEADQUARTERS
San Jose, CA

CEO
David Hatfield and Jay Parikh

Revenue

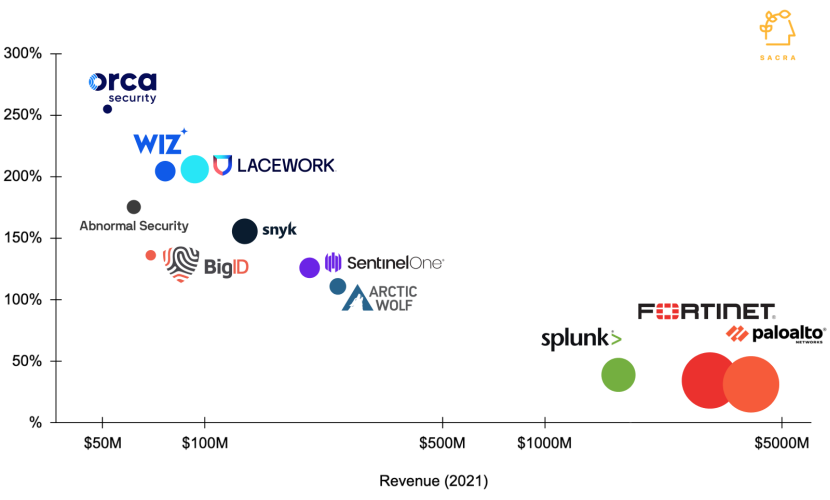


Today, Lacework is at approximately $90M ARR, having crossed $60M ARR at the end of 2021. We estimate 2022E revenue at $120M.

Lacework did $20M ARR in 2020, growing 300% from $5M in 2019 and about $1M in 2018.

Two big factors driving Lacework's growth are aggressive hiring in sales & marketing and ARPU growth from a shift upmarket towards bigger enterprise deals. The team grew from around 250 people at the end of 2020 to 700 people by November 2021. Their average deal size grew from $100,000 in 2019 to $150,000 by the end of 2021.

Valuation



Bubble size corresponds to valuation.

Lacework was last valued at $8.3B after raising $1.3B in a November 2021 round led by Sutter Hill Ventures, Altimeter Capital, D1 Capital Partners and Tiger Global Management.

Lacework was originally incubated at Sutter Hill Ventures, the same firm that incubated Snowflake—Sutter Hill MD Stefan Dyckerhoff was the company's original CEO, while Sutter Hill's entrepreneur-in-residence Vikram Kapoor joined as technical co-founder.

Other investors in the company include Dragoneer, Snowflake Ventures, Coatue, Franklin Templeton and Counterpoint Global, Morgan Stanley's investment wing.

Overall, private cybersecurity companies are comparable on valuation multiple, when adjusting for amount of revenue and their overall growth rate. Wiz and Lacework are roughly comparable as end-to-end cloud security platforms and are at 80x and 92x valuation/revenue multiples respectively (2021 data).

Business Model

Customers pay for Lacework as a SaaS product that's like insurance, where they pay a consistent amount on a monthly basis to prevent a catastrophic event from happening. Lacework captures the value of that service through usage-based pricing, charging customers as a function of their number of cloud accounts and the amount of resources they use.

The ongoing shift from on-premises computing to cloud and multi-cloud computing is a major tailwind. That shift to multi-cloud is exponentially increasing companies' attack surfaces by making computing itself more interconnected and interdependent.

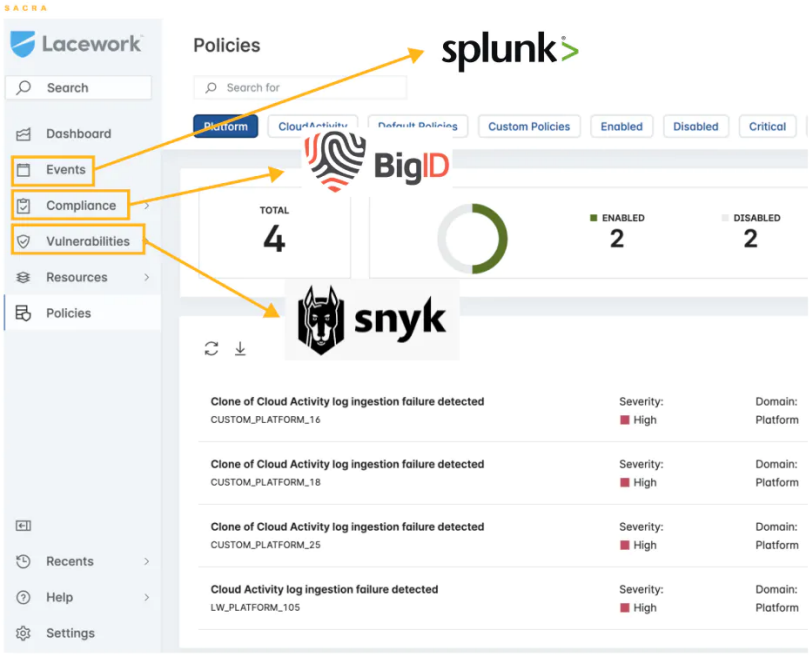
In addition to driving increased demand for security products built for multi-cloud, that shift is part of Lacework's expansion motion: customers pay more, and Lacework makes more money, as teams deploy more of their resources and compute to the cloud.

Lacework customers

SNOWPLOW · Scurri · AB Tasty · sliide · POCKETGEMS · greenlight guru · dreem · DRIFT · sift · nylas

Lacework's product uses machine learning to eliminate much of the manual, rules-based work of cloud security, making it attractive to smaller teams with less dedicated devops and infosec resources. While a competitor like Wiz touts the 20% of Fortune 500 companies that use its product, Lacework has grown to $90M ARR selling to the Fortune 5000: hence they have a significant expansion opportunity in going upmarket and selling to customers that have far greater amounts of resources and assets to protect.

Product



Lacework uses ML to bundle together the logging capabilities of a Splunk, the compliance tools of a BigID and the vulnerability assessment and management of a Snyk for a multi-cloud world.

Rather than needing to stitch together several different tools to get the right security coverage across Azure, AWS, Google Cloud and Kubernetes, infosec and devops teams get a single platform and a single view into the security posture across all their different deployments.

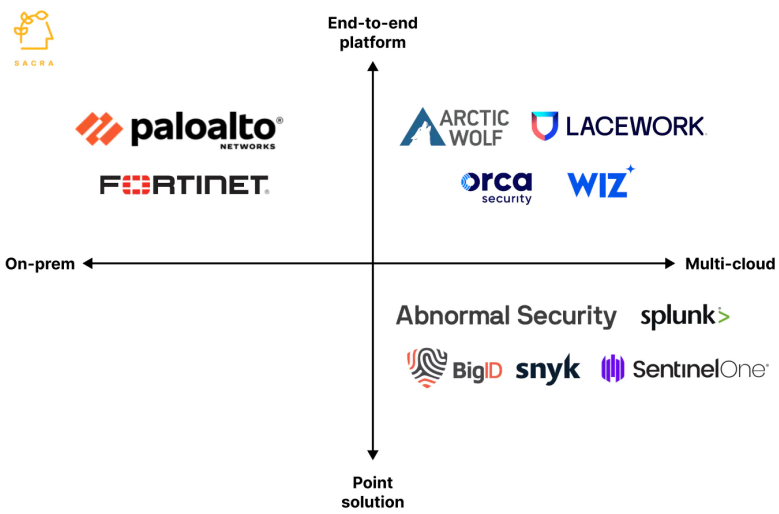
That reduces costs for teams by consolidating their spend, it eliminates the redundant alerts and security holes that can result from layering on multiple tools, and it cuts out the manual work of writing cybersecurity "rules" that has been the traditional paradigm in the space.

How Lacework works is by ingesting data from all of a customer's cloud APIs (e.g. AWS CloudTrail) as well as runtime environments (EC2 instances, Kubernetes clusters, ECS clusters) and using ML to detect anomalous behavior across them.

That's in contrast to the rules-based approach, where a company's infosec or devops engineers would have to write suites of "if this, then that" tests to check for bad behavior across their servers.

That approach worked well in an on-premise world—in a world of cloud and multi-cloud, it results in false positives (from overly aggressive rules that flag innocuous developer activity) and vulnerabilities (from incomplete coverage).

Competition



Cybersecurity has been one of the hottest markets of the last few years. Between 2020 and 2021, VC investment in cybersecurity startups grew from $12B to $29.5B, and the number of startups raising at $1B+ valuations went from 6 to 30.

Demand has been driven by a few key tailwinds:

- Enterprise workloads migrating to the cloud: As more and more companies go through digital transformation and move computing resources to the cloud rather than on-premise servers, it drastically expands their attack surface, making them more vulnerable.

- Increasing sophistication of cyberattacks: Criminals are trending away from low-value attacks and towards higher-value strategies. 93% of all global enterprise cloud deployments were estimated to be affected by 2021's "borderline apocalyptic" Log4j vulnerability, which compromised all of AWS, Google Cloud, and Azure.

- Security budget expansion: Security leaders have seen their cybersecurity budgets expand rapidly over the few years amidst growing interest from the entire executive team in preventing cyberattacks. According to CSO, 26% surveyed at the end of 2021 expected their 2022 budget to grow by 10% or more —they estimate total spending of $172B for 2022.

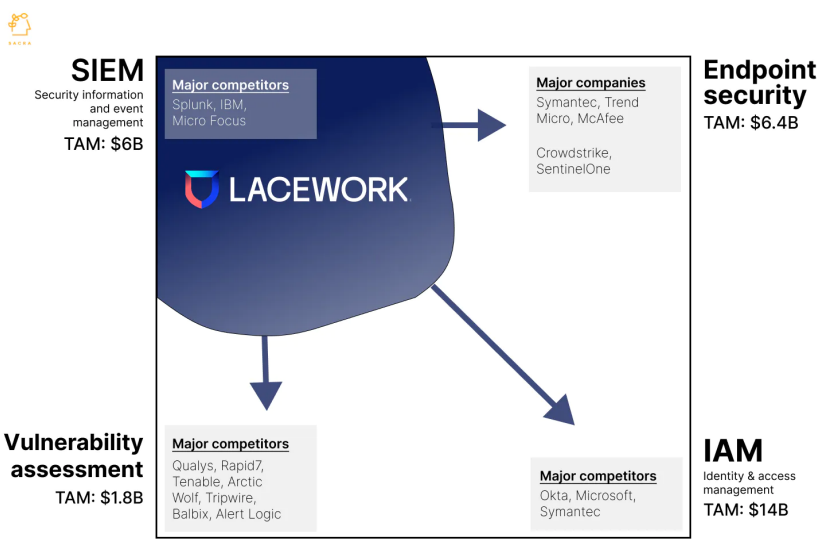
In this market, we're seeing a growing distinction between vendors as to whether they're point solutions or platform providers. Competing directly with **Lacework** are other platform companies focused on security in the cloud like **Arctic Wolf** ($4.3B valuation), **Wiz** ($6B valuation), and **Orca Security** ($1.8B valuation).

Palo Alto Networks ($49B market cap) and **Fortinet** ($47B market cap) still have some of the most widely-used security platforms in the Fortune 100 and the high-end of the market more generally. Though they were designed and built for an era of on-premise servers, they've also adapted to the rise of platforms like Lacework and Wiz. Palo Alto Networks's Prisma Cloud, which is their cloud security SaaS for hybrid and multi-cloud environments, did $270M of ARR in Q4'21.

At the same time, we're seeing fast growth and good traction for companies at the point solution end of the spectrum. That includes companies like **Snyk** ($8.5B valuation) which is focused specifically on vulnerability management and discovery and helping developers write secure code from the start, and **Abnormal Security** ($4B valuation) which uses AI to protect organizations against email-based phishing and ransomware attacks.

Developer-centric security companies like Snyk, by selling into the CTO or VP of Engineering rather than a CSO or CIO and embedding itself into companies' existing IDEs and workflows, could prove to have an interesting wedge into other adjacent cybersecurity use cases.

TAM Expansion



Lacework's core product maps out a customer's entire runtime environment and all of their cloud workloads. The upside of doing that challenging engineering work upfront is that Lacework now have the ability to use that mapping of data elements as a foundation from which to launch new types of products.

As cybersecurity vendors become more mature, they tend to move into adjacent markets to expand TAM, drive more growth and become more platform-oriented solutions. Palo Alto Networks launched in 2005 with a better firewall; since then, they've grown to a $50B market cap by expanding into incident response, network security, endpoint security, security operations, and cloud security.

Lacework has a similar opportunity ahead of it. Today, its core data mapping product is being used to provide better interpretation of security logs and spot vulnerabilities in the cloud, but they have line of sight to applying that same approach to a customer's entire network ala CrowdStrike—and to using their visibility into all of the users in that network into a full-fledged identity management solution.

One of the core advantages for Lacework here is the ability to build these new functionalities on top of their existing platform rather than having to build them out through acquisitions, which PAN and other incumbents have to do because they weren't designed originally for a multi-cloud use case.

Risks

Moving upmarket: Their average deal size at Lacework grew from $100,000 in 2019 to $150,000 by the end of 2021. Big deals were recently signed with Epic Games and Airbnb. However, competitors like Wiz have been showing better ability to sell upmarket into the enterprise—to continue to compete, Lacework will have to keep working to put together more enterprise-centric offerings and sell against companies like Wiz and Orca Security.

High valuation: At the end of 2021, Lacework exceeded $50M in ARR, meaning they last raised at about a 166x ARR multiple—relatively high even in the frothy cybersecurity space. That high valuation has implications for new investors to be able to generate a sizable return and it could also have implications on Lacework's ability to recruit high-quality talent, though the prestige of Sutter Hill and Snowflake are likely to be helpful to Lacework in this regard.

Fundraising

Round	Date	Amount	Valuation	Investors
Series E	11/2021	$1.3B	$8.3B	Sutter Hill Ventures, Altimeter Capital, Tiger Global Management, D1 Capital Partners
Series D	1/2021	$525M	$1.5B	Sutter Hill Ventures, Altimeter Capital
Series C	09/2019	$42M		Liberty Global Ventures, Sutter Hill Ventures
Series B	08/2018	$24M		Sutter Hill Ventures
Series A	05/2015	$8M		Sutter Hill Ventures

Team

David Hatfield

Co-CEO

Jay Parikh

Co-CEO

Vikram Kapoor

Founder, CTO

Andy Byron

President, CRO

Amy Cronk

CCO

Mike Staiger

CFO

Disclaimers

Published on May 24th, 2022