LACEWORK.

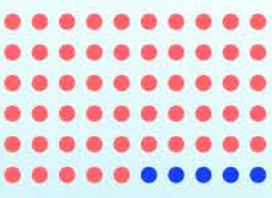
Fixing vulnerabilities

3 tough truths, 3 simple questions, 3 fun facts

Today, no company can assume it's immune from security vulnerabilities. For the DevOps and security teams that think they can rough it out, here are three tough truths:

1

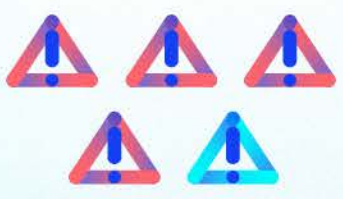
Security teams find new vulnerabilities every day



55 security vulnerabilities were published each day in 2021

2

False alerts create confusion and noise



1-in-5 critical alerts is a false positive

3

Bad actors thrive in the gaps

31% of cyberattacks in early 2022 stemmed from unaddressed Log4j vulnerabilities

Too many vulnerabilities to patch. Too many alerts to address. An era of unknown threats. Peace of mind may seem out of reach. But, with Lacework, peace of mind is only three simple questions away:

1

What are you missing?

With Lacework, continuously scan container images and hosts across every stage of the CI/CD lifecycle, shifting security practices left and into the build process for early detection and risk reporting. Lacework supports multiple scanning options including inline scanner, proxy scanner, platform scanner, and admission controller.

2

What are you finding?

With Lacework, continuously monitor and assess environments from build to runtime to catch anomalies — be they known or unknown threats. Keep watch over your runtime containers to assess newly reported vulnerabilities.

3

What do you fix & block first?

With Lacework, cut down security alerts and figure out what's most important by correlating runtime observations with risk data to give you actionable, prioritized insights. Automatically prevent the deployment of risky container images into production environments using the Kubernetes Admission Controller.

It's not rocket science. It's Lacework. And in case that all sounds too good to be true, here are 3 fun facts. With Lacework, on average:

1

Customers experience a

342%

return on investment.

2

Customers see an

86%

reduction in security alerts.

3

Customers save

$1.79M

in increased productivity from reduction of alert investigations.

With Lacework, identify your vulnerabilities within hours. Then keep the bad guys out.

Learn more. Read the eBook.

Sources:
55 security vulnerabilities - https://www.computerweekly.com/news/252510662/2021-another-record-breaker-for-vulnerability-disclosure
1-in-5 'critical' alerts is a false positive - https://info.lacework.com/rs/016-ATL-295/images/2022-cloud-security-outlook_vol1.pdf
31% of malware stemmed - https://technologymagazine.com/cloud-and-cybersecurity/lacework-report-confirms-31-of-malware-infection-are-log4j
Forrester TEI report - https://www.lacework.com/resources/forrester-tei/

LACEWORK.