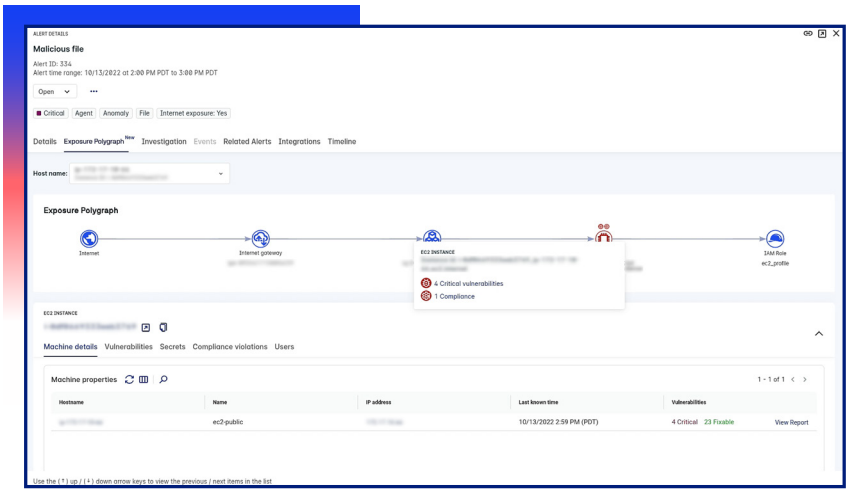
FEATURE BRIEF

Attack path analysis

OVERVIEW
What is the feature?

Lacework provides attack path analysis, which helps teams fully understand how an attacker could successfully compromise a cloud environment. This analysis is visualized through an Exposure Polygraph that correlates different risk factors including host reachability, critical vulnerabilities, exposed secrets, misconfigurations, and other risks within a cloud environment. These attack paths can pinpoint exactly what assets could be targeted and how.

To form these possible exposure paths, the Polygraph® Data Platform correlates data from multiple sources including (but not limited to) configuration data, activity data (cloud audit logs), vulnerability and secrets scanning, and runtime data. For example, with a single alert view, teams can view the Exposure Polygraph, quickly investigate alerts with full context, and collaborate with team members on remediating those items. This information helps teams understand the connections between their riskiest assets and take action to reduce the greatest threats facing their organization.



Benefits

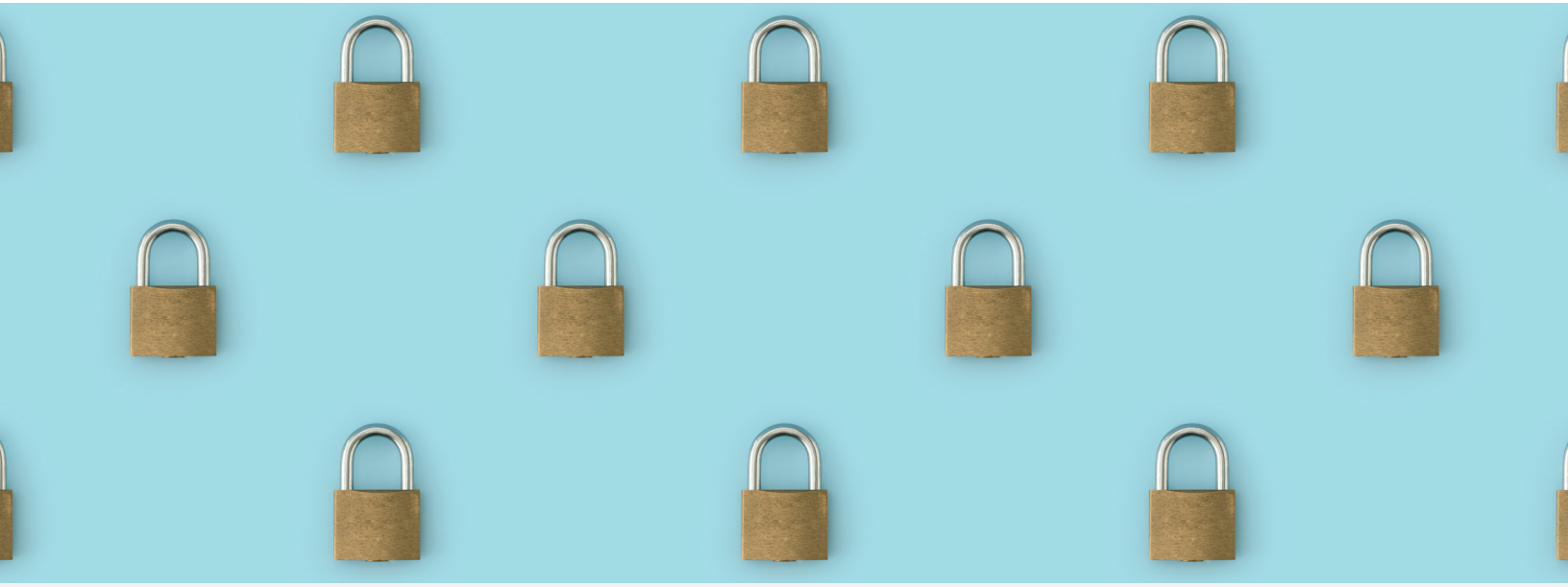
- **Fix what matters most**
  In one platform, view exposure path visualizations alongside real production data to prioritize fixes based on what's actually exploitable within at-risk workloads. Communicate the importance of work items more easily with the broader organization to reduce risks and improve security hygiene. Use the enhanced vulnerability reporting for hosts, which includes internet exposure as a factor for risk scoring, to determine which vulnerabilities should be prioritized over others.
- **Provide rich context to enable faster triage and investigation**
  Equip incident response teams with accurate and reliable information served up in a single alert view for faster triage and investigation.
- **Bolster compliance and standardization initiatives**
  Quickly identify policy violations and the associated risk context to reduce exposure and improve overall compliance.

VALUE

Why is the feature important?

Cloud environments are incredibly complex, and attackers seeking to compromise a system will look for the path of least resistance. They lurk in these environments, waiting for just the right moment to strike by exploiting vulnerabilities, exposed secrets, misconfigurations, excessive privileges, internet exposure, and more. Once they are in, attackers rarely use a single loophole to breach a system. In fact, they take advantage of multiple, successive risks to infiltrate a system, escalate privileges, and compromise cloud environments and sensitive resources.

To successfully defend a cloud environment, security teams must think like an attacker. To uncover and prevent malicious behavior, attack path analysis is essential. Analyzing and correlating multiple risk factors across your environment can help pinpoint where — and why — these paths exist, showing the greatest risks and configurations that attackers can misuse for lateral movement and privilege escalation.



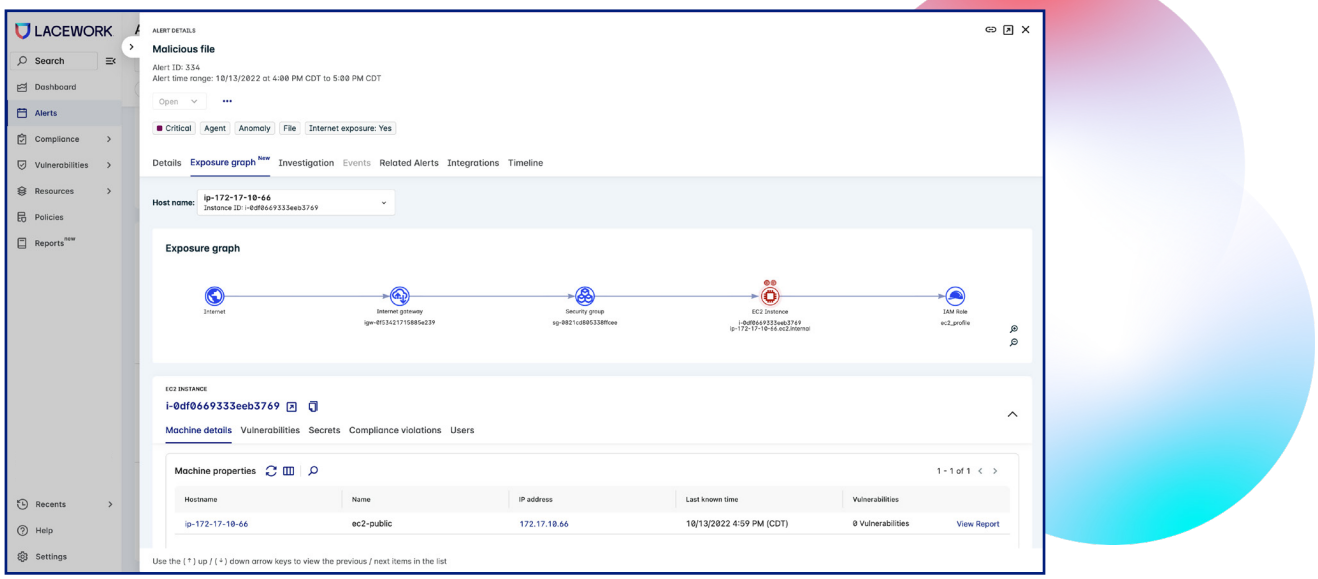
Solved challenges

- **Exploitable risks are buried in alert noise**
  As cloud threats continue to grow in volume and sophistication, security teams with limited resources struggle to identify the “true” risks that can be exploited in their environment. Prioritization is key, as cloud environments will never be free of all risk.
- **Lack of context delays investigation**
  Security alerts must include the risk factors related to the event, the risky configurations that could have triggered the alert, and if any of the risks have been exploited in their environment. Without full context, it is challenging for security teams to investigate alerts and fix issues before it’s too late.
- **Friction between teams slows risk-based remediation**
  Different teams with different incentives and goals often struggle to prioritize work items properly without a single source.

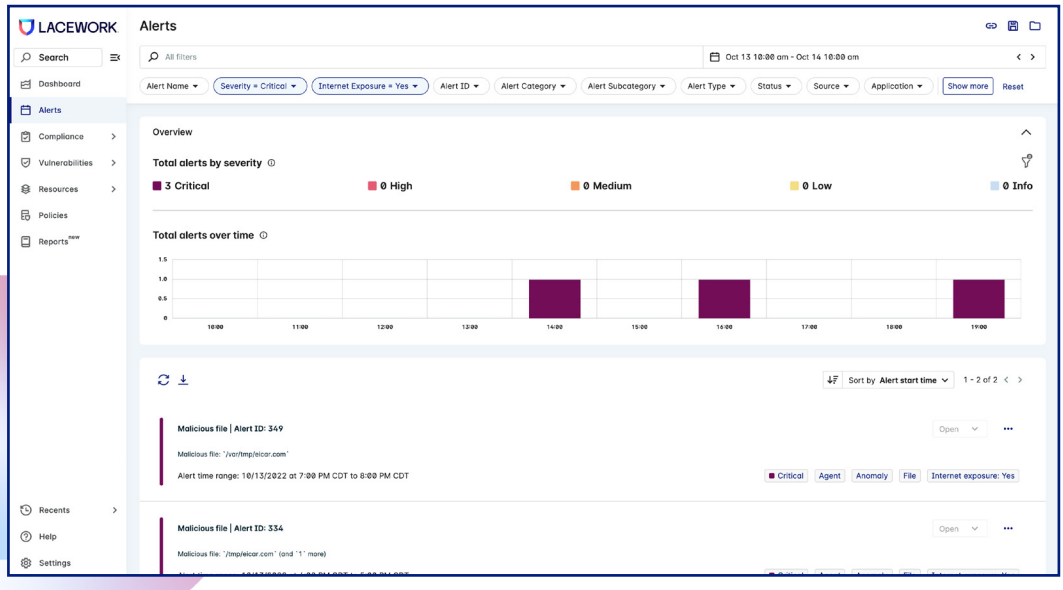
DEPLOYMENT

How is the feature implemented?

To map attack paths, Lacework uses a combination of insights from cloud audit and configuration data, workload context from our agents, and the additional vulnerability and security scanning capabilities of our agentless collection.



When an alert is triggered for an anomaly or policy-related event, the Exposure Polygraph provides the associated risk context to the alerts. This can include known vulnerabilities on the affected host, compliance violations related to the involved entities, internet exposure, and discovered secrets like SSH keys. Visual cloud context shows the attack path from the internet to the internet gateway, including the security group instance and any associated IAM roles, in a single alert view.

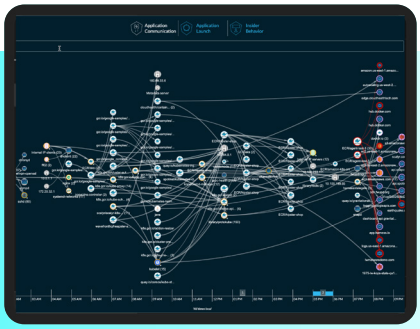


From the Lacework console, administrators can filter by critical severity and/or internet-exposed alerts. Attack surface context provides key details including the why, when, and what — for instance, the machine details and file hash. The Exposure Polygraph visually displays the pathway from the internet through to our internet gateway into the security group, correlating associated attack vectors, including vulnerabilities, compliance violations, and IAM roles so you can instantly see the risks associated with that instance.

It's just as easy to identify critical vulnerabilities and compliance violations to prevent attackers from exploiting these gaps with privilege escalation or lateral movement. Through the console, you can view machine details including the IP address, the host name, and any associated vulnerabilities. The vulnerabilities tab displays the CVE, criticality, associated CVSS score if available, and the vulnerability impact score.

Agentless scanning capabilities enable discovery of secrets like SSH private keys on a host, as well as detect any compliance violation in a single alert view to maintain compliance and support standardization initiatives.

The Lacework console also uses the exposure context to update the vulnerability reporting for hosts. The risk score now includes internet exposure as a risk factor. This can help organizations determine which vulnerabilities should be prioritized over others.



Explore our agentless capabilities

Read the brief

Book a live walkthrough

Schedule demo

LACEWORK

Lacework is the data-driven security company for the cloud that delivers end-to-end visibility and automated insight into risk across cloud environments. Trusted by enterprise customers worldwide to reduce risk, Lacework significantly drives down costs so you can securely innovate in the cloud with speed.

 | 888.292.5027 | lacework.com 11/22