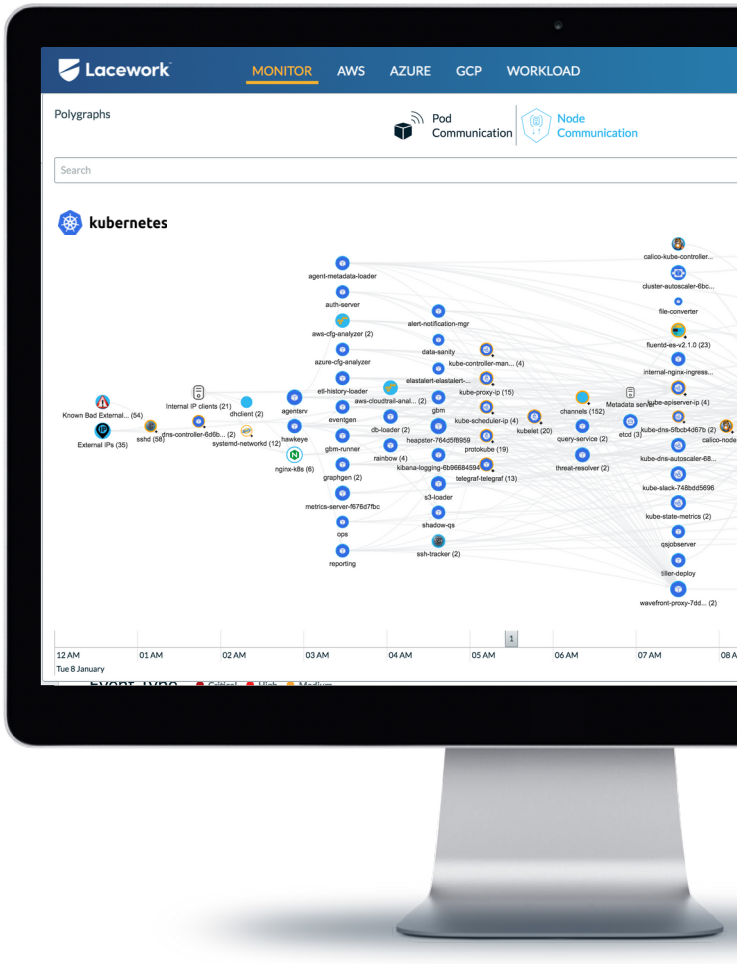

Lacework™
SECURITY FOR KUBERNETES
Application visibility, threat detection, and forensics

Lacework

SECURITY FOR KUBERNETES

APPLICATION VISIBILITY, THREAT DETECTION AND FORENSICS

Lacework provides comprehensive threat detection for Kubernetes dashboards, pods, management nodes, and clusters, in addition to end-to-end security for their public cloud infrastructure workloads, accounts, and containers.

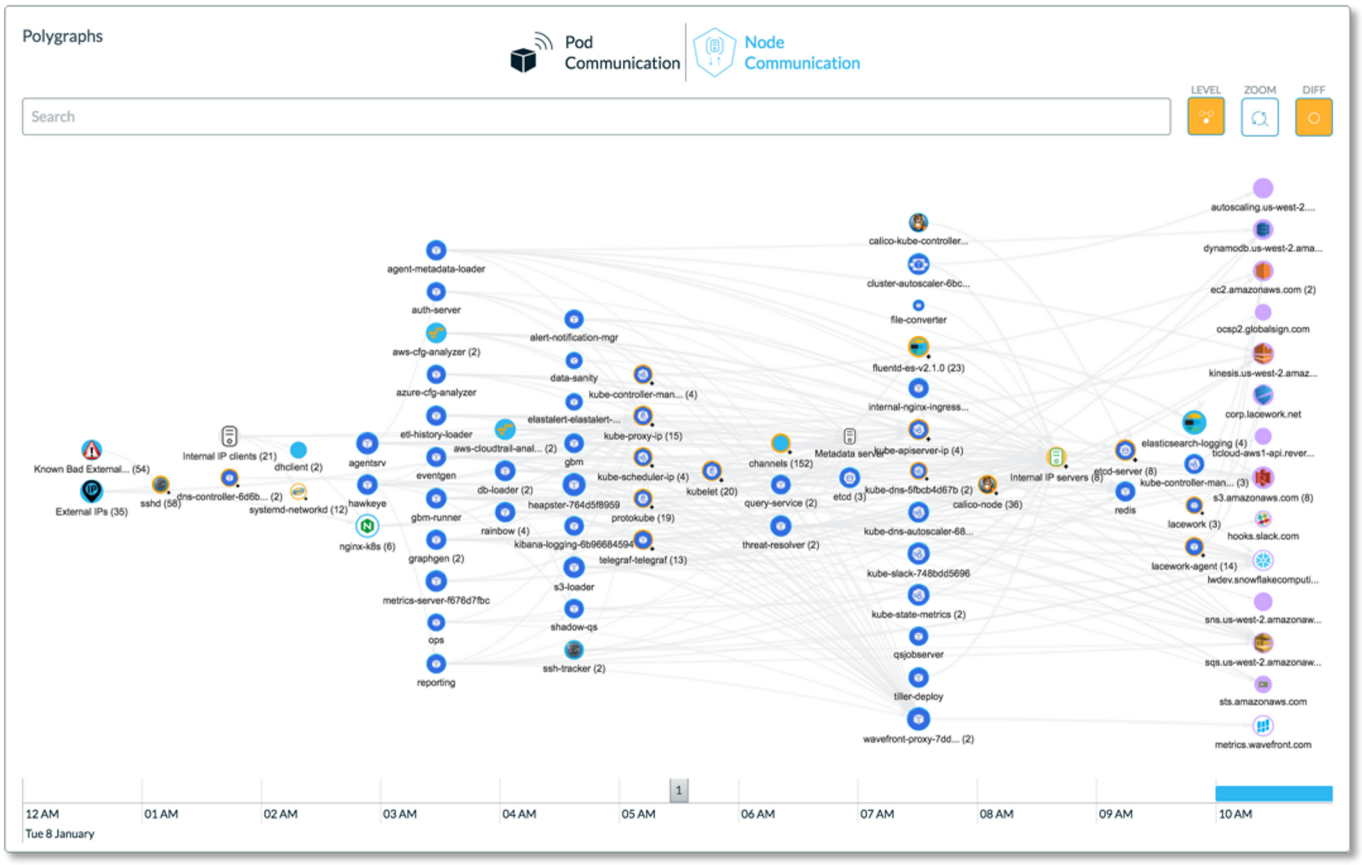


With the rapid adoption of Kubernetes for application and infrastructure orchestration, there's a corresponding increase in the risk associated with data exposure and vulnerabilities throughout the application lifecycle. Without proper detection of threats, organizations could unwittingly be granting unauthorized access to Kubernetes clusters, applications, and customer data. Lacework identifies the risks and threats for Kubernetes-deployed infrastructures, including publicly exposed and unsecured API servers and management consoles.

Lacework was among the first cloud security vendors to highlight the need for rigorous container security. The company's original research was published earlier this year in a report titled, **Containers at Risk: A Review of 21,000 Cloud Environments.** Some of Lacework's customers, like Fintonic, have already started using Lacework as a critical component of their cloud security.

APPLICATION VISIBILITY

Lacework provides deep visibility into your Kubernetes deployment. This includes high-level dashboards of your clusters, pods, nodes, and namespaces combined with application level communication between all of these at the application, process, and network layer.

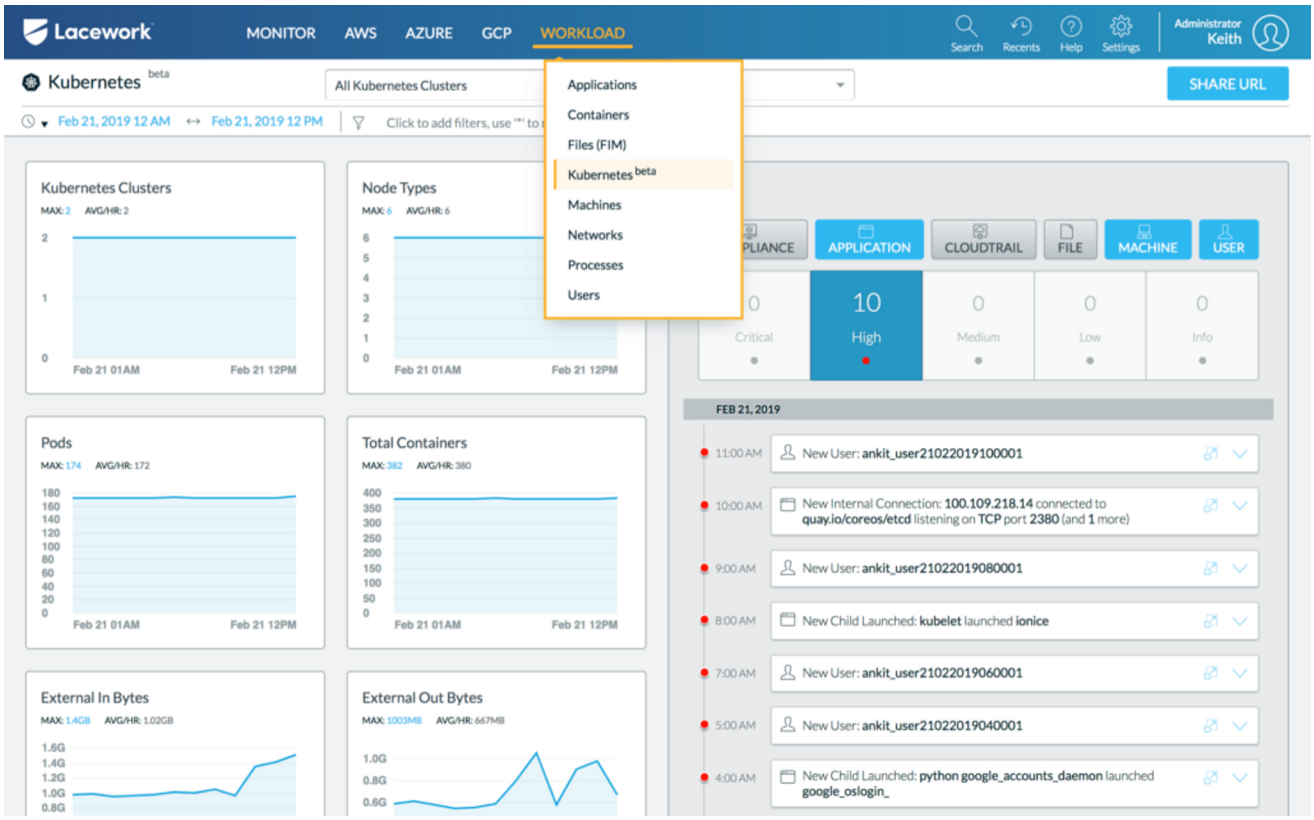


THREAT DETECTION

Backed by the power of Lacework's Polygraph technology, this solution includes detection of both risks and threats that may be specifically designed to breach a vulnerability within Kubernetes, a possible miss-configuration, or a threat that can affect your infrastructure by installing malicious code onto one of your containers.

The Lacework Polygraph is designed to detect both known and unknown threats through detection of IOC's and Lacework's behavioral analysis and machine learning classification.

Risks and threats are visible within the Lacework dashboard, are ranked by risk severity, and can be delivered through the most common modern methods such as a Slack channel or a Jira ticket.

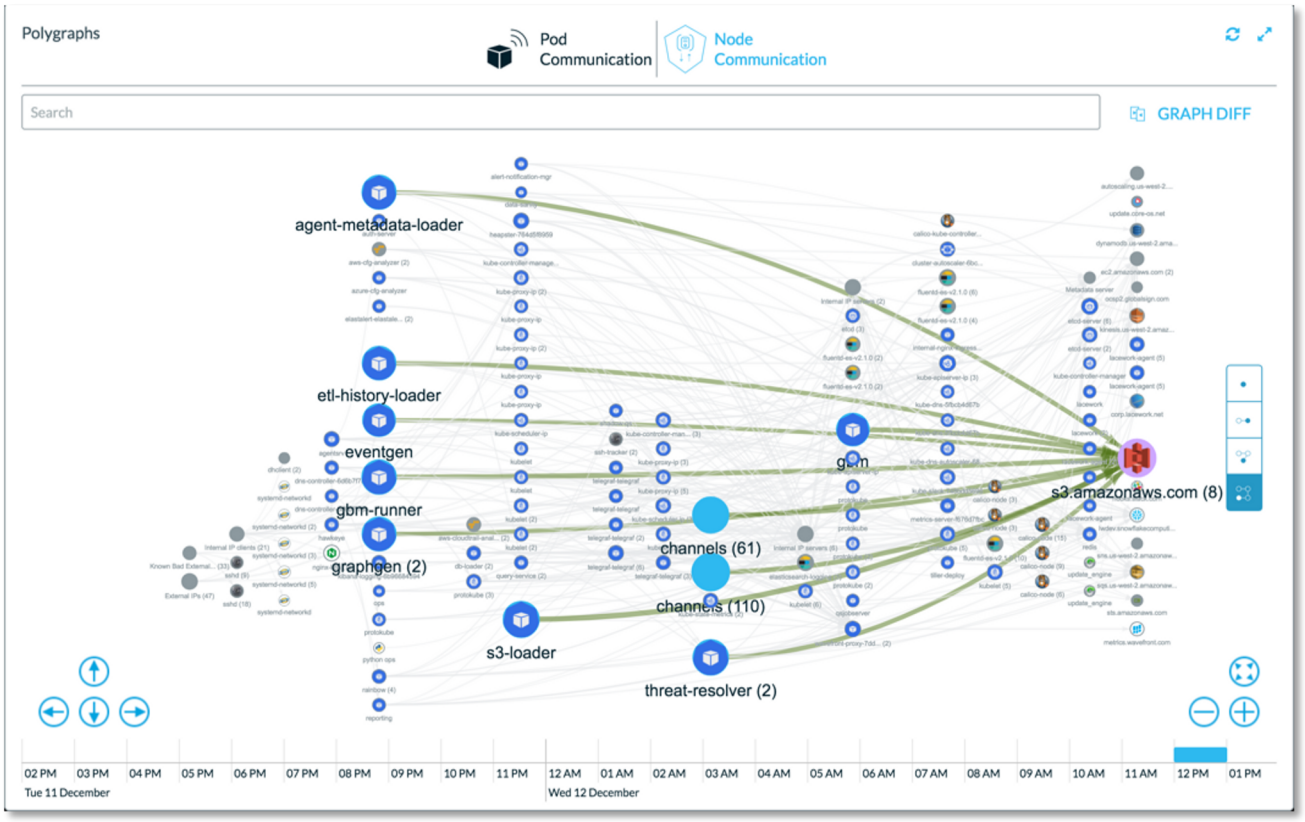


FORENSICS FOR KUBERNETES

Whether you are triaging and alert or digging into deep details around the cause and effect of a change, Lacework for Kubernetes has all the information. Our SaaS service allows you to go back in time and look at all related events across your Kubernetes infrastructure that may have caused a breach or exposed you to an unknown risk.

Detailed information about your containers, your applications, and your infrastructure are all available and include information related to Kubernetes such as; pods, nodes, labels, namespaces, and all network information. All this information is available both within the UI and from our API.

Lastly, Lacework creates hourly Polygraphs which can demonstrate the change of relationships and events over time. This is a critical tool for understanding and triaging your events.



SECURITY VISIBILITY

Get deep observability into 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 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 & security best practices the could put your company at risk.