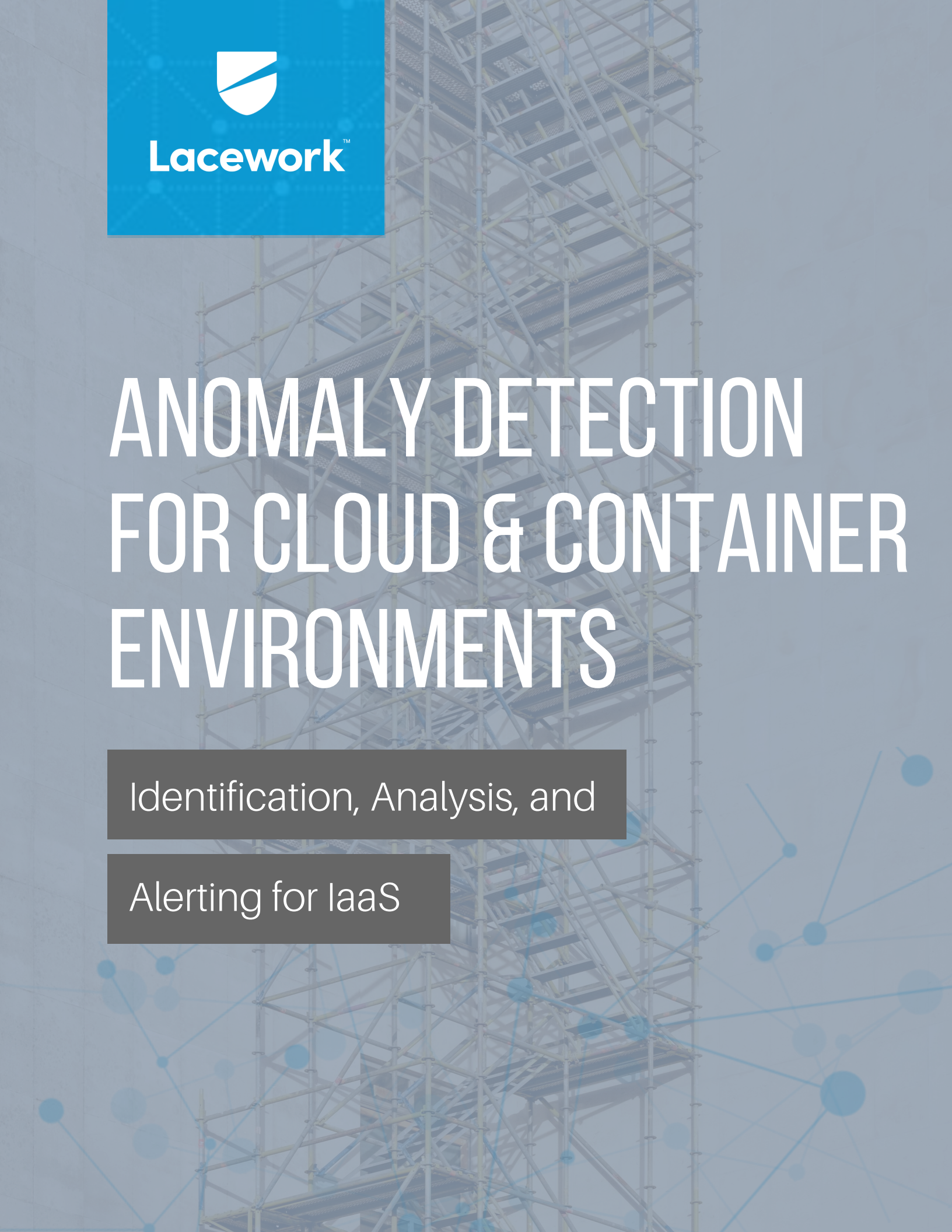


ANOMALY DETECTION FOR CLOUD & CONTAINER ENVIRONMENTS

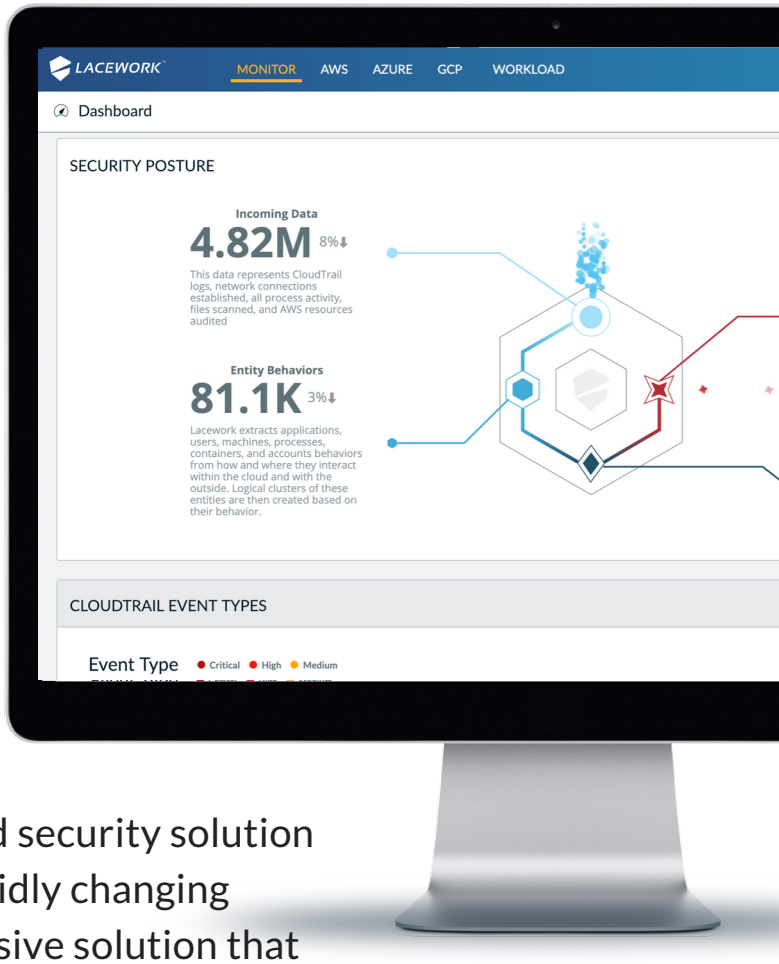
Identification, Analysis, and Alerting for IaaS

Lacework

Anomaly Detection for Cloud & Container Environments

Identification, Analyzsis, and Alerting for IaaS

Public clouds enable enterprises to implement infrastructure-as-code and allows them to rapidly develop, test, and deploy services at scale. In this environment, network, storage and compute resources are in constant flux to adapt to business needs. While this agility and flexibility provide many business and technological benefits, the cloud is also more susceptible to new forms of threats and cyber attacks. Unfortunately, legacy security solutions are unequipped to handle these and leave organizations vulnerable.



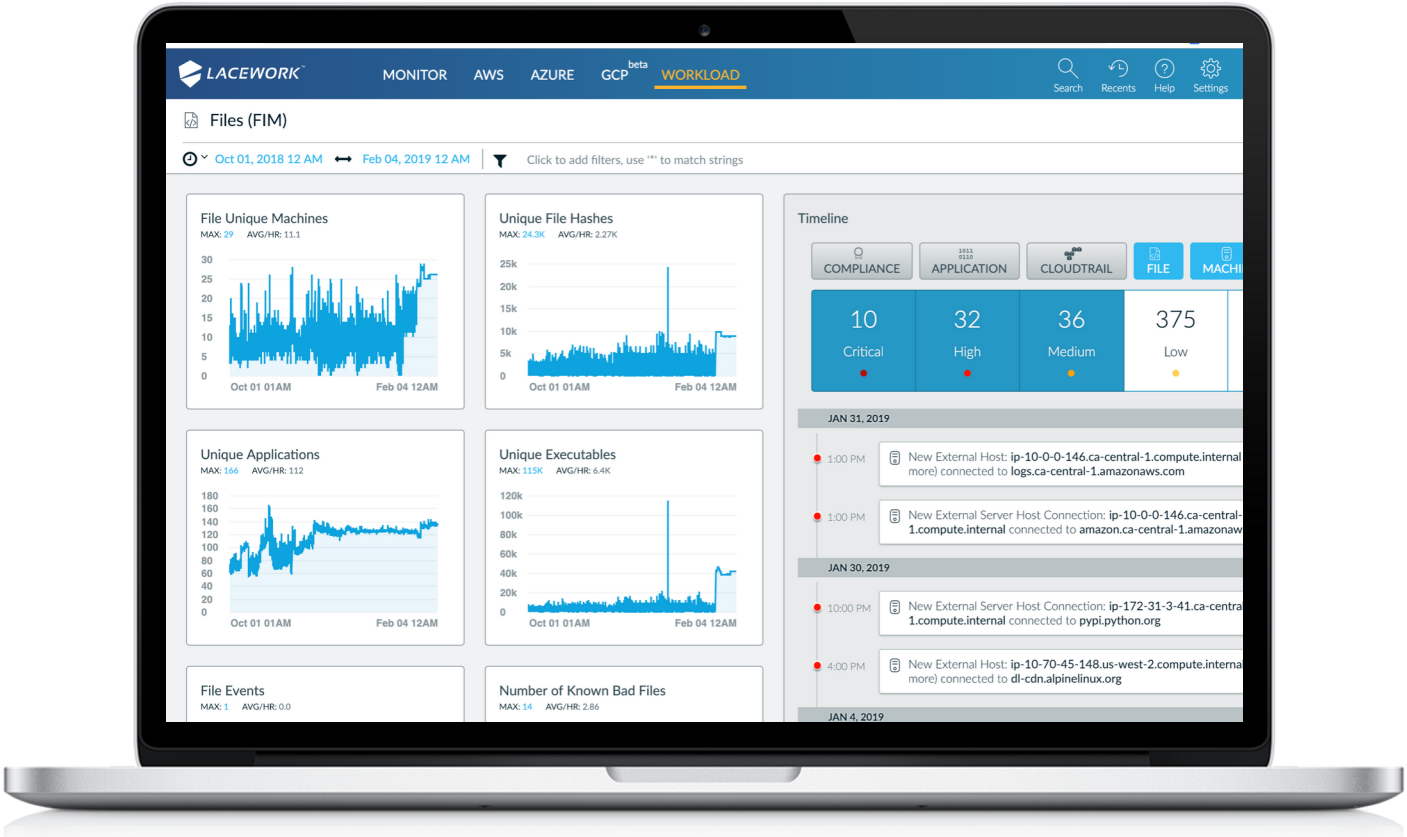
At Lacework, we developed our end-to-end security solution from the ground up, specifically for the rapidly changing cloud. Our platform provides a comprehensive solution that encompasses cloud configurations, account activities, workload/runtime analysis, and automated anomaly and threat detection.

BIG DATA & ANOMALY DETECTION TO SECURE THE CLOUD

Traditional security solutions rely on signatures or rule-based approaches. The advantage of these solutions is that the rules are readily understandable. However, the drawbacks are that these rules are manually entered and catch known attack profiles. These rules do not catch new attack profiles and require constant manual maintenance. In addition, to reduce false positive rates, the rules are typically written for very well defined threat scenarios, limiting their effectiveness in actual production environments.

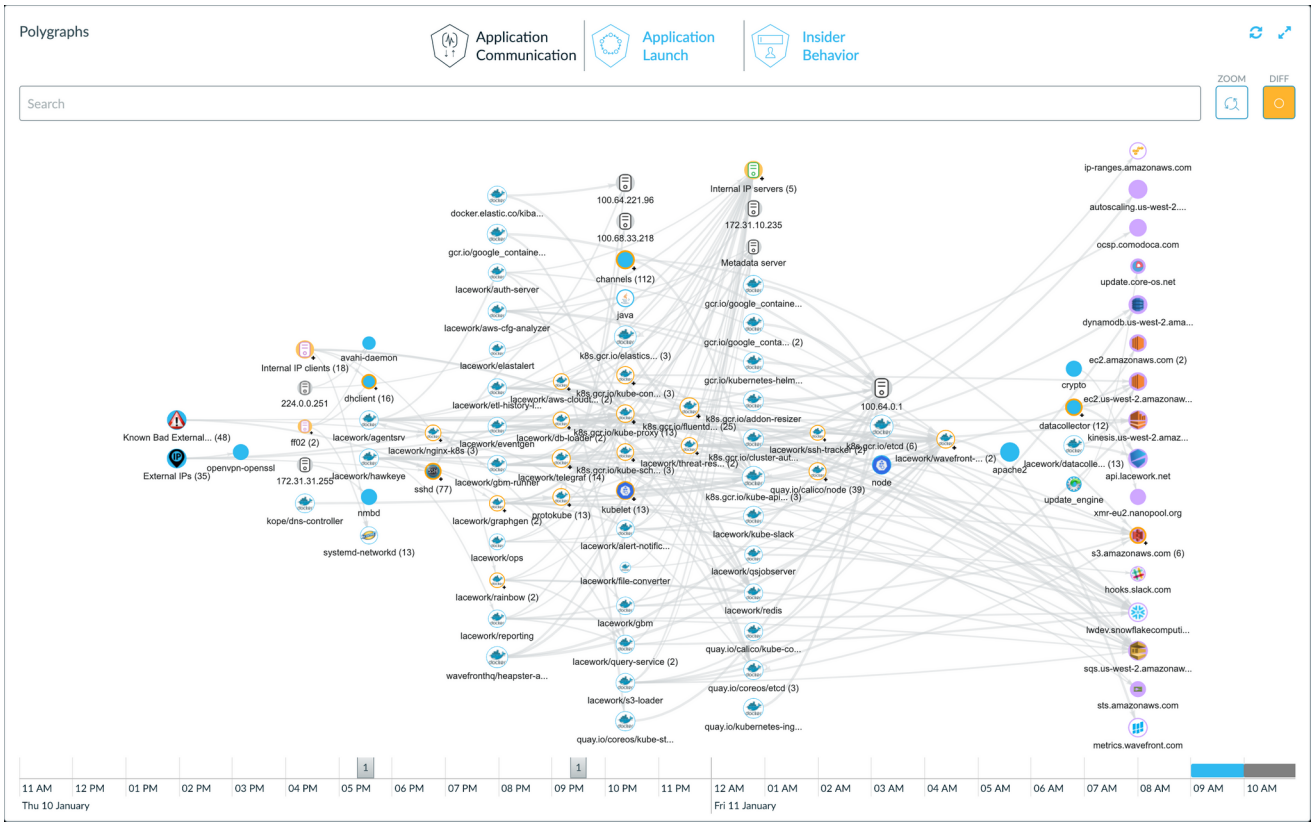
Lacework takes a completely different approach. Our approach is to collect high fidelity process, network, file, and user data to form a base model of normal infrasture behavior. We then use sophisticated analytics and machine learning techniques to detect anomalies which are indicators of threats.

With this approach, the Lacework system is adaptive as your environment changes. In addition, because these baselines are generated automatically (not manually created), our system can be fined tuned to reduce false positives at the same time, return high yield alerts to our customers.



THE POWER OF POLYGRAPH

Lacework's foundation is Polygraph, a deep temporal baseline built from collecting high fidelity machine/process/users interactions over a period of time. The polygraph is used to detect anomalies, generate appropriate alerts, and provide an tool for users to investigate and triage issues.



Fundamentally, the polygraph technology dynamically develops a behavioral and communication model of your services and infrastructure. The model understands natural hierarchies (processes, containers, pods, machines, etc.) and aggregates them to develop behavioral models. A behavioral model is, in some sense, the essence of how a customer's infrastructure operates. With this model, Polygraph monitors your infrastructure for activities that fall outside the model. In addition, the polygraph continually updates its models as your data center behavior changes.

INTEGRATED AND COMPREHENSIVE

- Pinpoint exactly how a file changed: content, metadata, and whether the file was modified or simply appended
- Extended information on executables, such as files created without a package installation, command lines used at launch, currently running processes (with users and network activity), and suspect versions
- Expanded file intelligence with integrated threat feeds from ReversingLabs' library of 5 billion files
- One-click investigation of events and activities related to FIM signals
- Cloud-wide capabilities for search, file type summaries, and detection of new files

CLOUD SCALE AND SPEED

- Automated configuration, file discovery, and operations
- Scalable architecture with no added complexity or performance penalties
- Included with all Lacework Cloud Security agents

MEET COMPLIANCE MANDATES

- Protect log and configuration files against tampering
- Daily re-check of all monitored files
- Pre-defined directory maps monitor critical files and directories
- Easily configurable; users can add directories to the watch list

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.