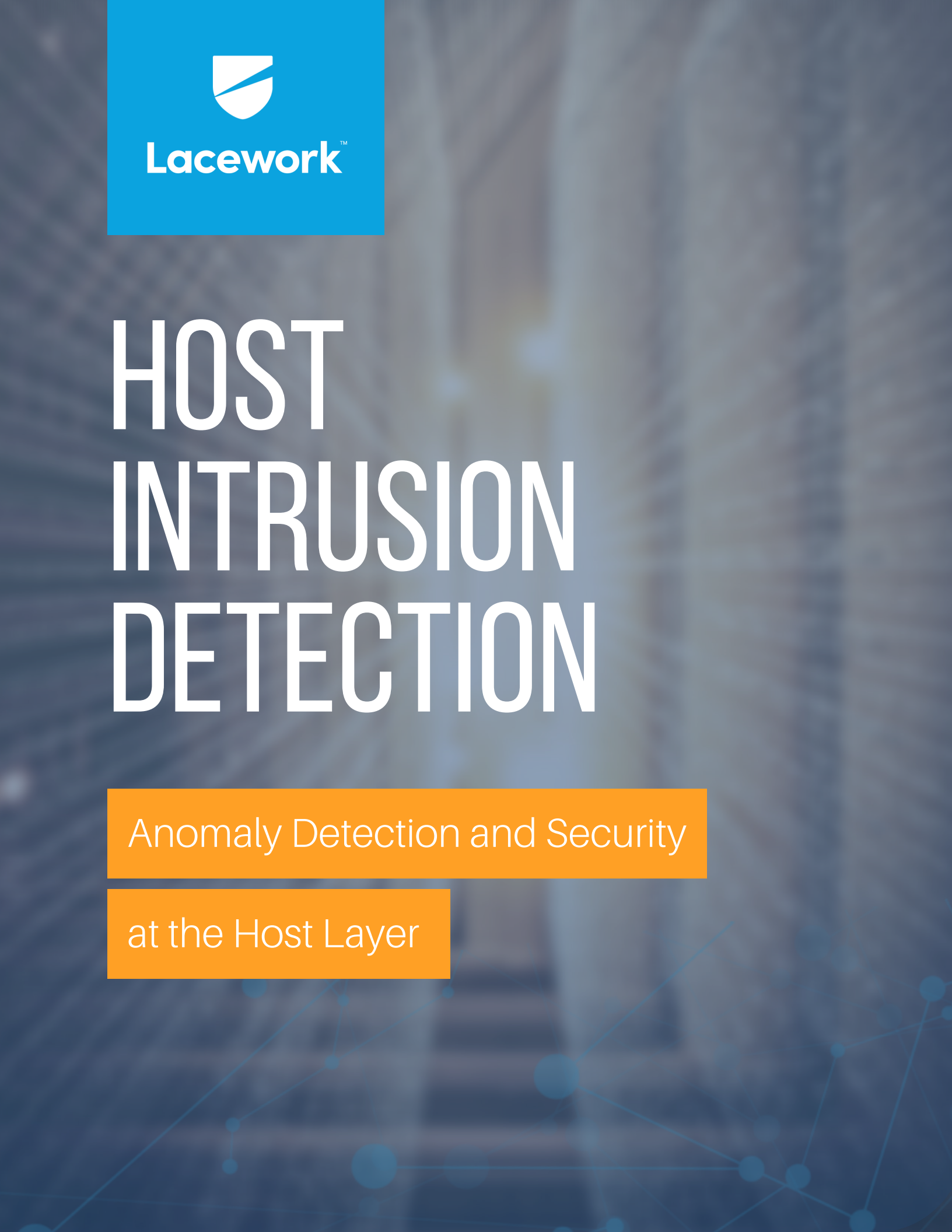


HOST INTRUSION DETECTION

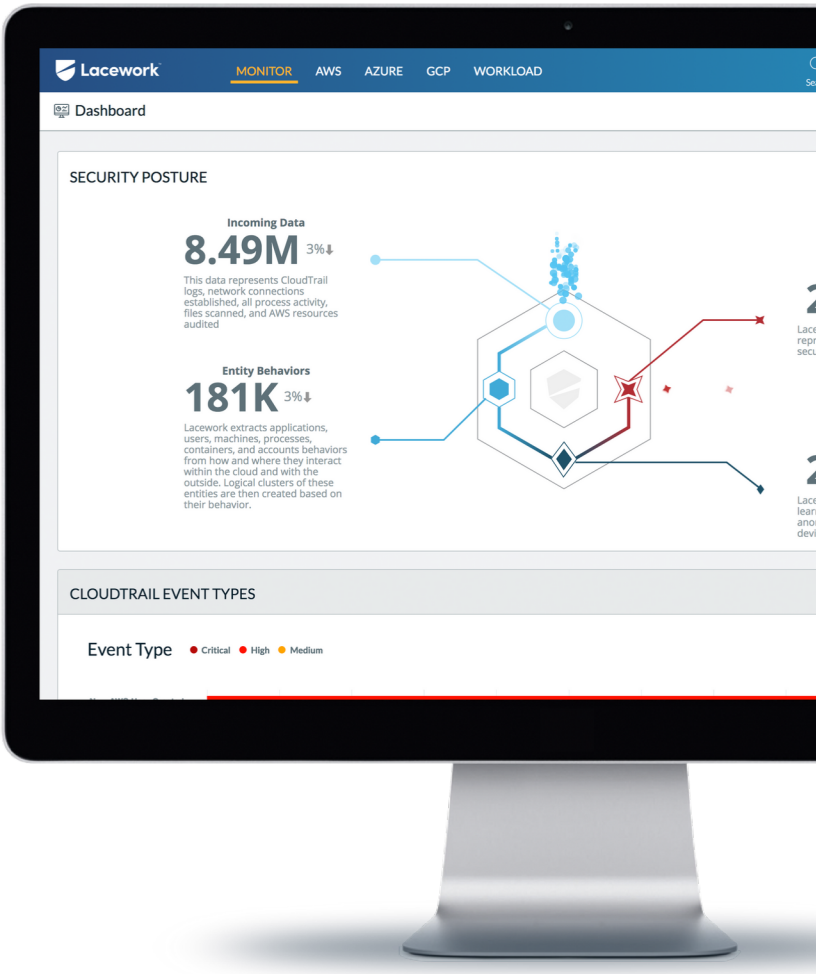
Anomaly Detection and Security at the Host Layer

Lacework™

HOST INTRUSION DETECTION

ANOMALY DETECTION AND SECURITY AT THE HOST LAYER

Lacework enables organizations to strengthen their cloud security with an anomaly-based intrusion detection system that operates at the host-level. Because data is collected at the host level, security teams can more accurately and effectively detect insider attacks that others wouldn't be identified in network traffic. Instead of using the same signatures and rules that hackers already know about, host intrusion detection (HIDS) operates far beyond the limitations of a network-based system to identify all activity happening across all workloads and accounts.



Security of your workloads depends on how well your HIDS solution can detect insider attacks that otherwise won't be caught in the network traffic, and how well you can investigate an infected host or application based on the data that has been collected.

Host intrusion detection overcomes the limitations of network intrusion detection systems that are traditionally used in an enterprise data center or non-cloud based infrastructure. Intrusion detection originally looked only at ingress and egress traffic on an enterprise's network. But to address the constantly changing nature of cloud and containerized environments, a new, agile, and far more comprehensive solution was required.

ACTIONABLE, EASY TO NAVIGATE INFORMATION ABOUT EVERY INCIDENT

- Visualize interactions and communications between cloud entities
- Review incidents at any level of detail
- Integrated information from third-party threat databases
- Global search finds related events anywhere they occur across your cloud

COMPREHENSIVE DATA COLLECTION

- Continuous and automatic
- Telemetry available from every cloud process
- Deeply integrated with available cloud services and compliance metrics

ACCURATE ALERTS

- Summarized alerts provide visibility and context
- Aggregation, risk scoring and customization minimizes alert "noise"
- Links and additional information make it easy to get to the bottom of each alert

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.