RedLock™

RedLock™ Cloud 360™

Implement the RedLock™ Cloud 360™ platform in minutes by providing API access to your public cloud infrastructure (no agents or proxies) and see results immediately:

Visualize your entire public cloud environment, including across multiple cloud service providers	Enable DevOps by setting guardrails and monitoring for issues, without impeding productivity	Discover anomalies across your entire cloud environment with RedLock's advanced machine learning capabilities
Receive contextual alerts to prioritize issues and respond appropriately	Playback the state of your environment for any given period of time and quickly pinpoint issues	Report on security and compliance posture across your entire public cloud environment to your management, board, and auditors

A Threat to Digital Business

Security and compliance risks involved in cloud computing threaten an organization's ability to drive digital business. In order to inject security into the DevOps process, security provides education, training and best practices to protect public cloud infrastructure such as Amazon AWS, Microsoft Azure, and Google Cloud Platform. But DevOps teams are not security experts, leaving security of the environment as a best guess or ignored altogether. By the same token, security teams are not developers and cannot be expected to have a deep understanding of the infrastructure needed to protect it. Cloud service providers provide access to configuration, activity, and network data but it is up to security teams to correlate and glean meaningful insights from it. The problem is amplified in heterogeneous environments with multiple cloud service providers and massive volume of cloud workloads.

Existing security solutions were not designed with an understanding of the dynamic nature of cloud infrastructure. They rely on creating static policies based on IP addresses which do not translate to cloud environments where workloads are dynamically being created and destroyed, and IP addresses are constantly changing. Solutions that rely on agents create blind spots in environments which contain workloads that do not allow agents to be installed; AWS S3, ELB and RDS for example. Point security tools provide siloed views into configuration data, user activity, network traffic, and threat intelligence data rather than a holistic view, making it a challenge to easily assess risk. SIEM tools were built to reactively search through massive volumes of data to investigate issues but they do not help visualize cloud infrastructure activity or support continuous monitoring, making it difficult to accurately assess risk.

True Cloud Infrastructure Security

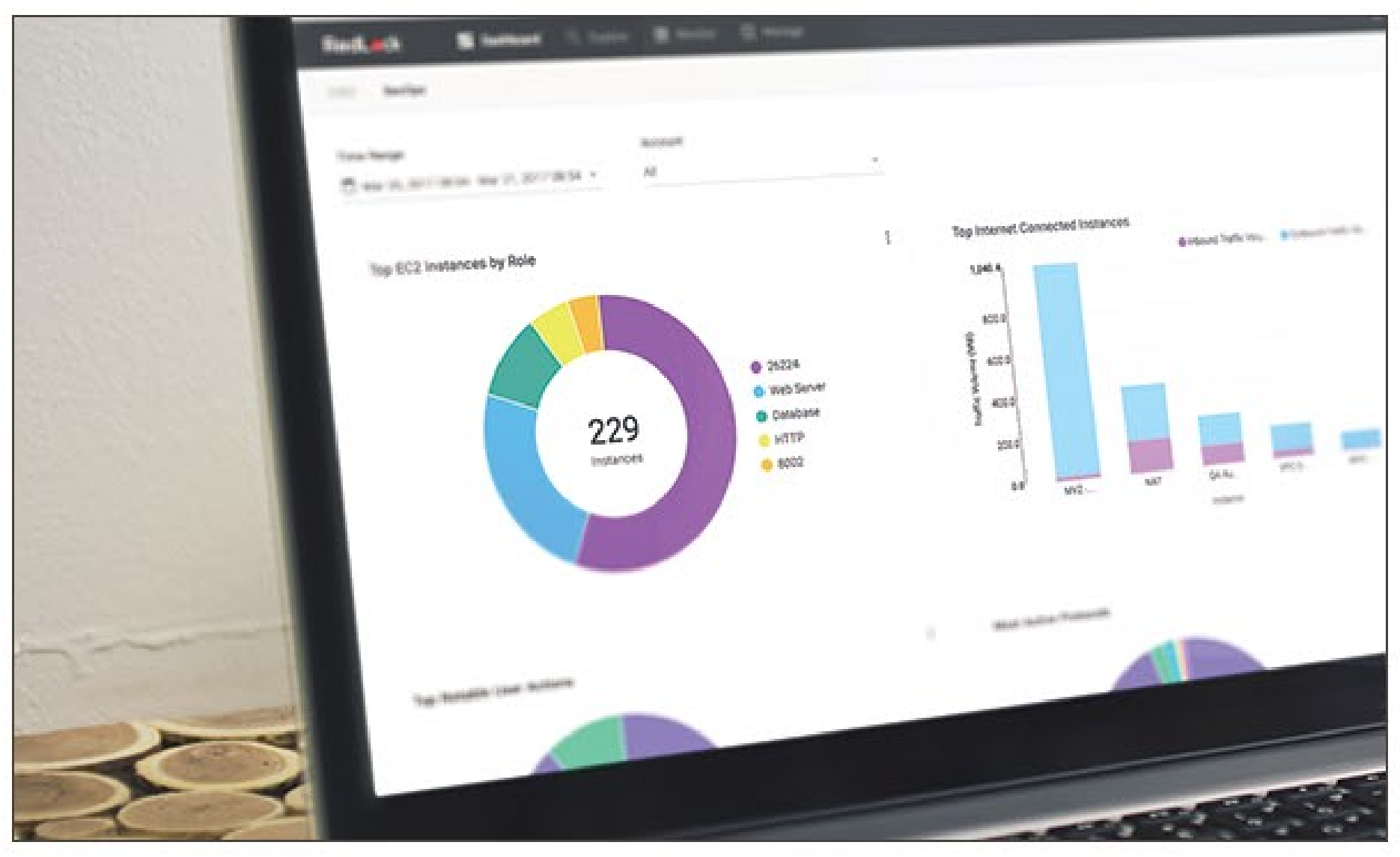
To get true visibility and control over cloud infrastructure security, organizations must rethink their process and technology. Rather than restrict or slow down development, the goal should be to provide development with the guardrails to move with speed and agility while providing security teams with solid technology to build security into the entire process with appropriate visibility and control.

True cloud infrastructure security provides organizations with a holistic view of cloud infrastructure security risk. It dynamically discovers changes and continuously correlates raw, siloed data sources including user activity, workload configurations, network traffic, threat intelligence, and vulnerability scans to give a complete view of cloud infrastructure risk. Most importantly, it does so in a frictionless manner without impeding DevOps.

RedLock Cloud 360 Platform

RedLock enables organizations to accelerate digital transformation by managing security and compliance risks within their public cloud infrastructure. For the first time, security teams can see a true picture of their risks over the entire cloud infrastructure, across multiple public clouds, and down to every component within them - all in a single view. The RedLock Cloud 360 platform enables automated monitoring, anomaly detection, cloud forensics, adaptive response, and compliance reporting.

The RedLock Cloud 360 platform can be implemented in minutes by connecting to public cloud environments via 50+ APIs, without impeding DevOps. With RedLock, security and DevOps teams can confidently move together at the speed of business.

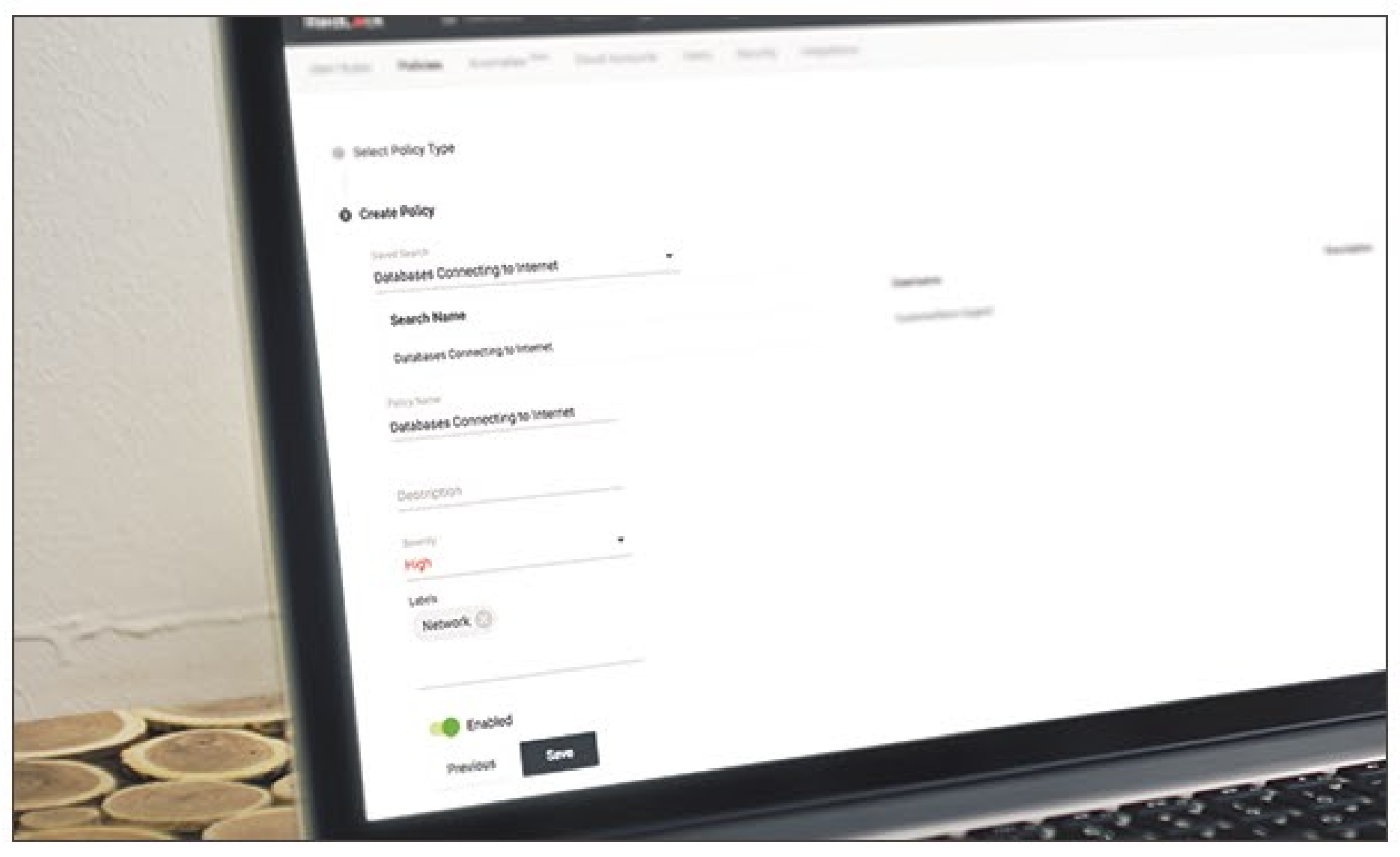


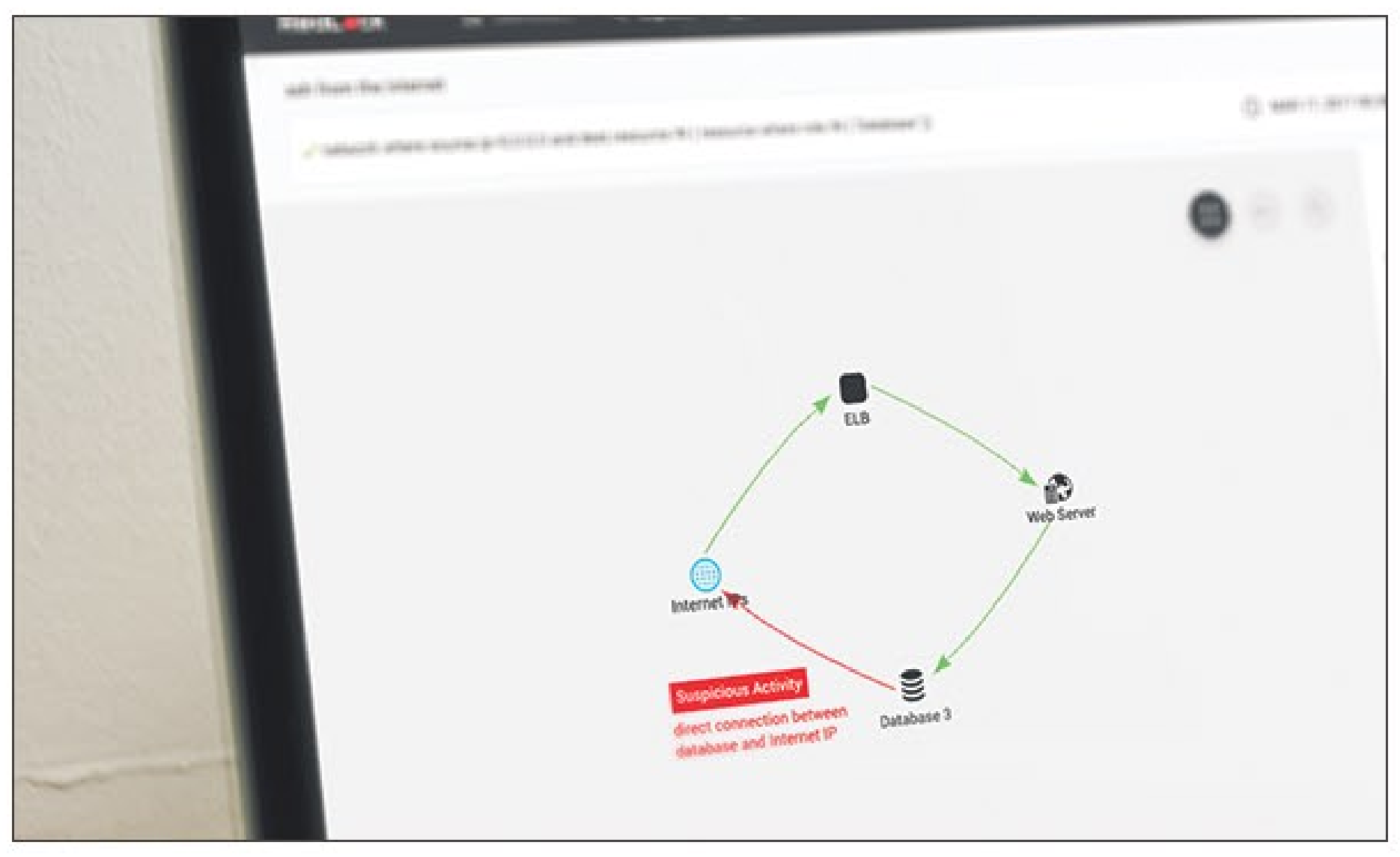
Comprehensive Visibilty

The RedLock Cloud 360 platform enables you to visualize your entire public cloud environment, across multiple cloud providers and down to every component within the environment. The platform dynamically discovers, maps, and visualizes the entire cloud infrastructure by aggregating and correlating configuration, user activity, and network traffic data. Combining this deep understanding of the cloud infrastructure with machine learning enriches the view with data from external sources such as threat intelligence feeds, vulnerability scanners, and SIEMs. This comprehensive visibility lets you accurately and easily pinpoint risks. For example, you may notice databases running in your cloud environment and will want to ensure that they do not communicate directly via the internet.

Automated Monitoring

The RedLock Cloud 360 platform lets you set guardrails for DevOps and enables them to be productive without compromising on security. The platform comes prepackaged with policies that adhere to security best practices for workload configurations and access control. You can also create custom policies based on your organization's specific needs. The platform continuously monitors for violations to these policies by existing workloads as well any new workloads that are dynamically created. Using the example above, you could implement a policy to automatically determine if any databases are communicating directly via the internet.



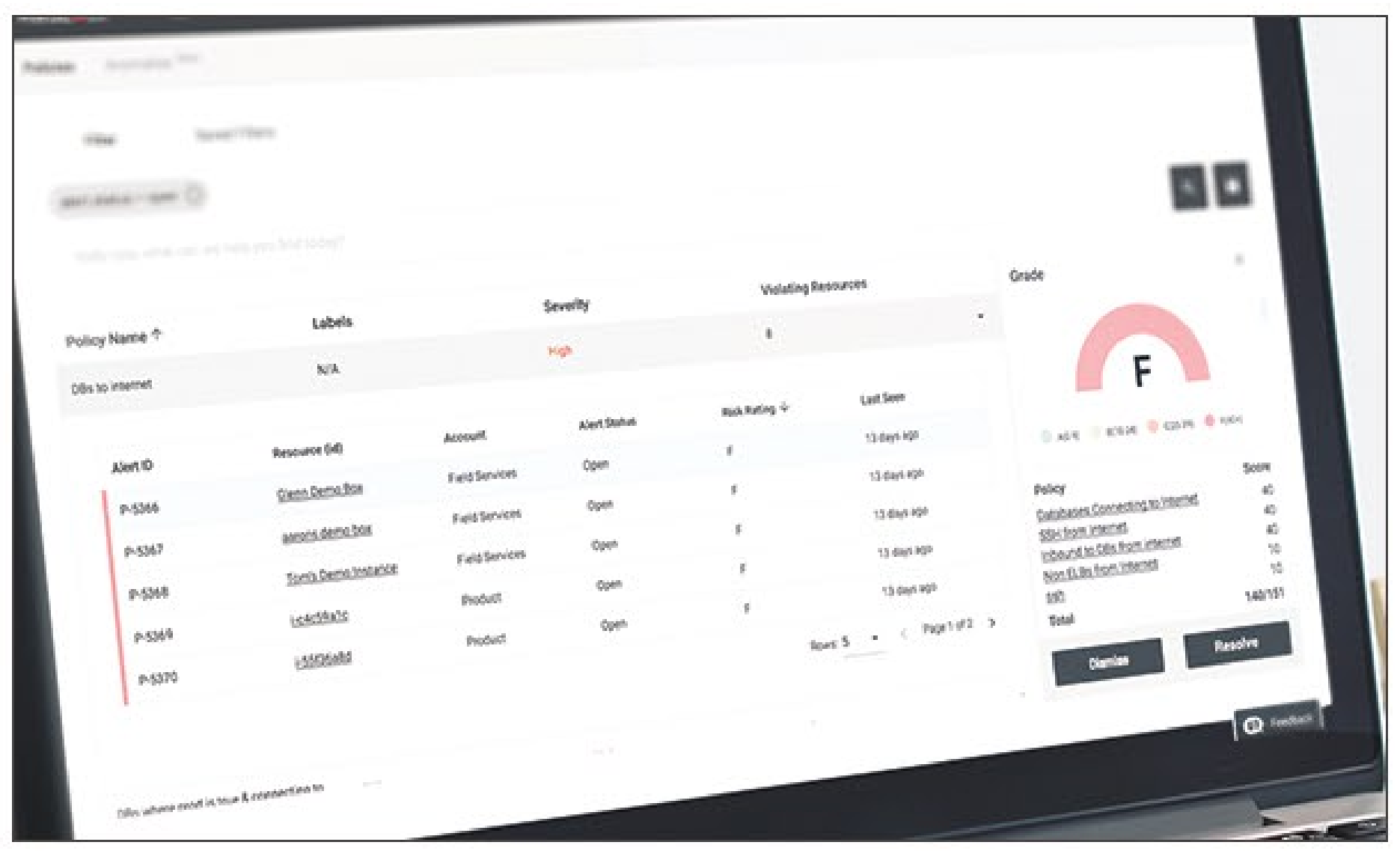


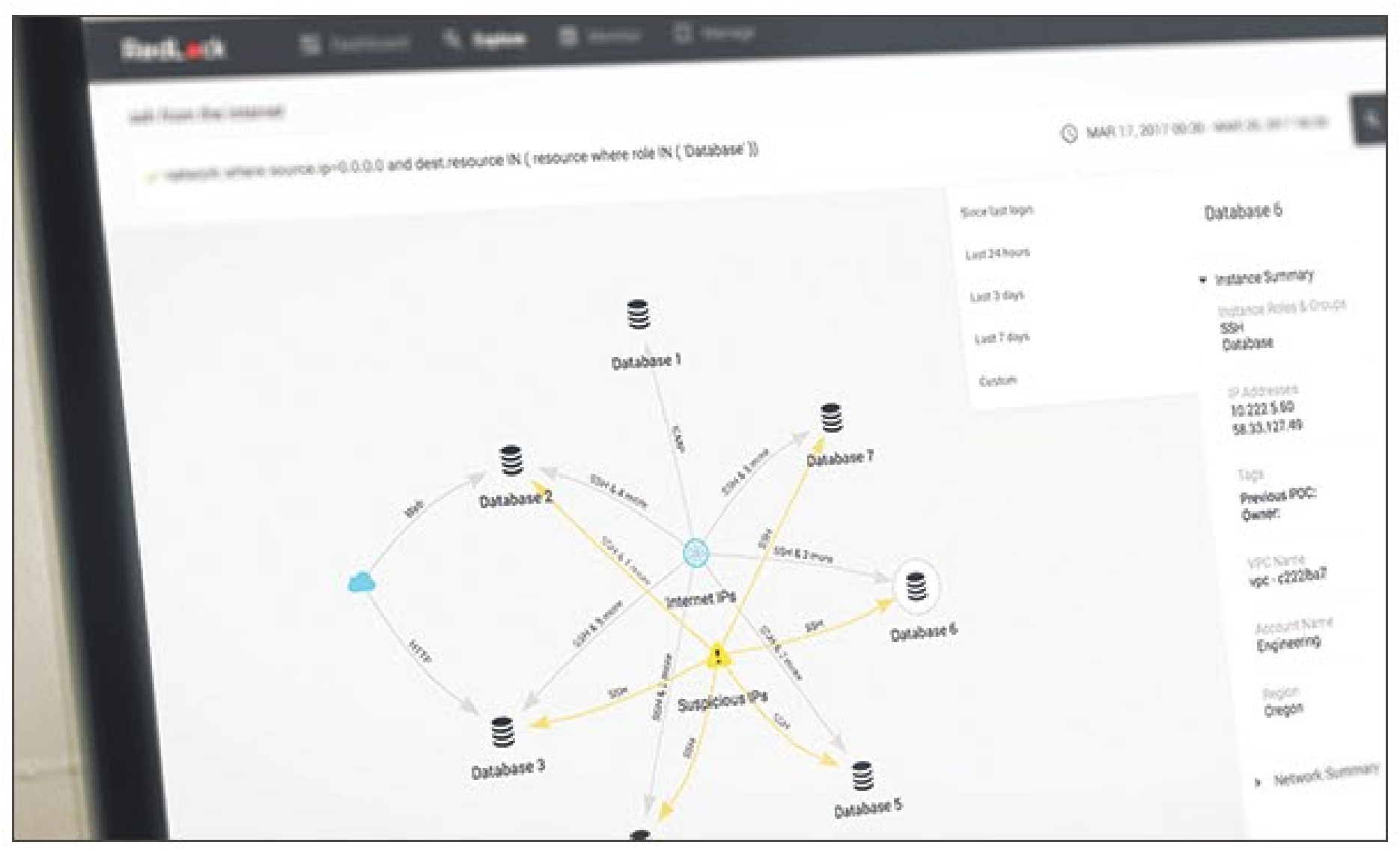
Advanced Anomaly Detection

The RedLock Cloud 360 platform automatically detects user and network anomalies across your entire cloud environment. The platform combines a deep understanding of the cloud environment and its dependencies, correlation with third party data sources such as threat intelligence feeds, and machine learning using baselines. For example, unusual traffic patterns to a database relative to its baseline activity indicates a potential anomaly.

Contextual Alerting & Adaptive Response

The RedLock Cloud 360 platform enables you to quickly respond to an issue based on contextual alerts. Alerts are triggered based on patent-pending risk scoring methodology and provide context on all the risk factors associated with a workload. This makes it simple to prioritize the most important issues first. You can send alerts, orchestrate policy, or perform auto-remediation. The platform data can also be passed to a third-party tool such as a SIEM to provide context around the alert, help determine if it is real or a false positive, and quickly identify the scope and appropriate response to remediate the issue. In the case of the risky databases example, a policy violation would be detected and a contextual alert was generated with information on risk factors. The issue can be resolved appropriately with a simple click of a button.



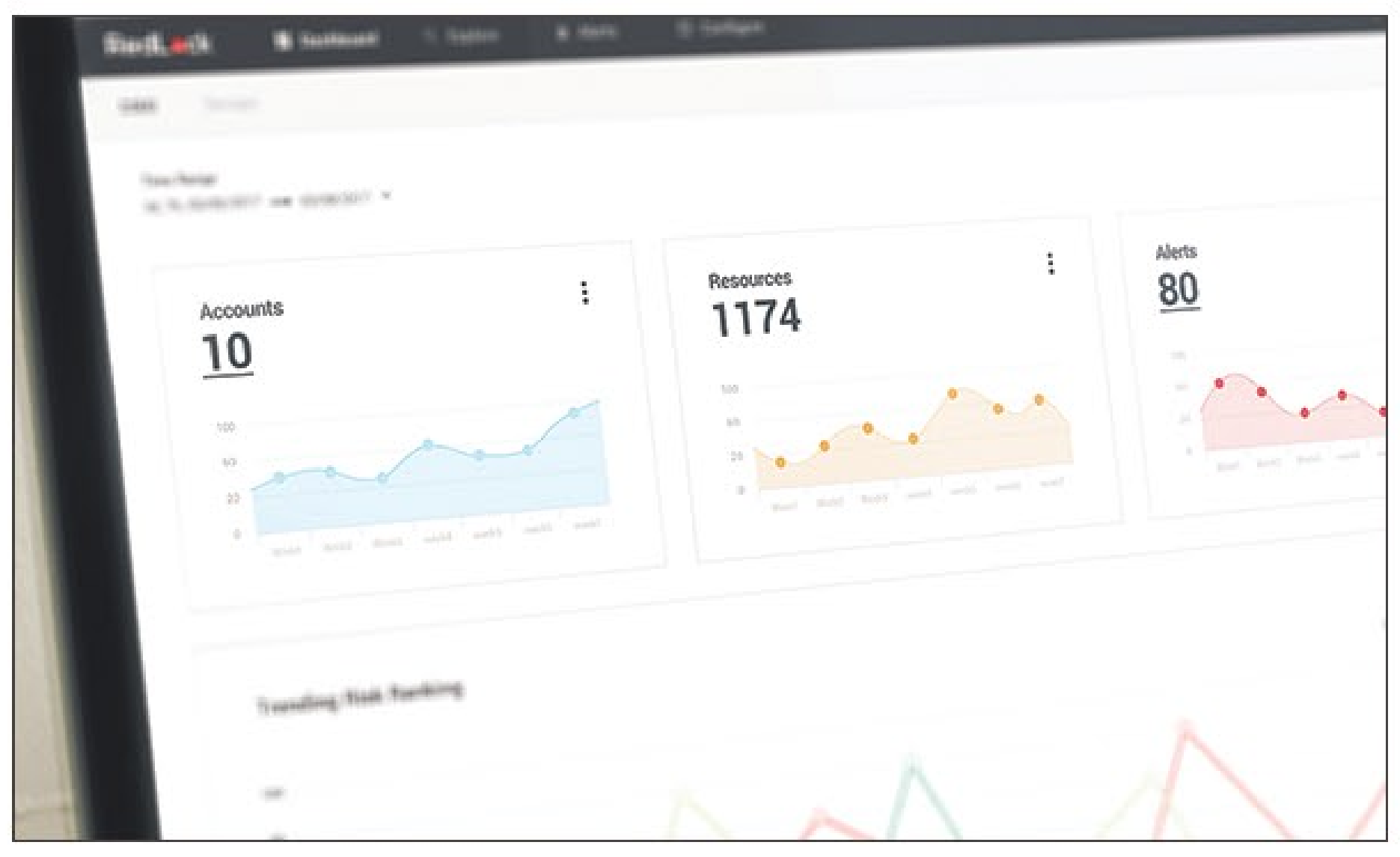


Cloud Forensics

The RedLock Cloud 360 platform's deep understanding of the cloud environment, reduces investigation time from weeks or months to seconds. You can use the platform's interactive map to quickly pinpoint issues and perform upstream and downstream impact analysis. The platform provides you with DVR-like capability to view time-serialized activity for any given workload. You can review the history of changes for a workload and better understand the root cause of an incident, past or present. For example, you can run a query to find all databases that were communicating directly via the internet last month. The resulting map will not only find all such instances but also highlight the workloads that are active threats. In this case, they are communicating with known malicious IP addresses.

Audit & Management Reporting

The RedLock Cloud 360Cloud 360 platform enables you to produce security and compliance reports across your entire cloud infrastructure environment. Similar to a credit score, the platform computes risk scores for every workload based on the severity of business risks, violations and anomalies. It then aggregates the risk scores to enable you to benchmark and compare risk postures across different departments as well as across the entire environment. The RedLock Cloud 360 platform lets you quickly identify the riskiest users or workloads and report on your overall security posture to management or the board. You can also easily report on the compliance posture of your environment to auditors.



To learn more:
Call: +1.650.665.9480, Visit: www.redlock.io