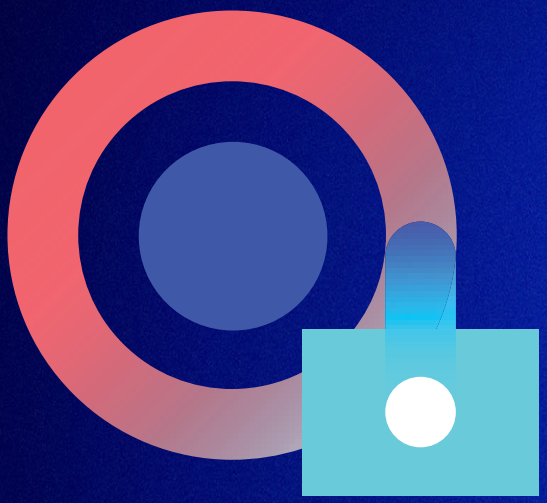
Defend against ransomware in the cloud with Lacework



LACEWORK®

Cloud infrastructure has become a potential target for ransomware groups.

With more businesses storing business-critical data in the cloud, there is no doubt the cloud will only increase as a target for hackers. Lacework helps organizations identify risks, detect potential attacks, and efficiently protect and respond to these types of threats.

Due to the nature of cloud environments, most breaches in the cloud are caused by misconfigurations and vulnerabilities — all of which can be taken advantage of in a ransomware attack. In the cloud, the lack of traditional perimeter security can make those mistakes very costly. For example, a misconfigured S3 bucket could allow an attacker to steal and encrypt data. Insecure services, accounts, or APIs could be left open to the public and could be discovered and exploited during an attack. These types of errors expose cloud workloads as targets that attackers quickly discover with simple publicly available and open-source tools.

Tactics, techniques, and procedures

Cloud ransomware has multiple known attack vectors, often targeting numerous resources in an attempt to access customer data or company secrets. MITRE ATT&CK™ documents tactics, techniques, and procedures used by attackers and explains how attackers attempt to gain access to an organization's resources running in the public cloud. Cloud ransomware has taken a different approach to other types of attacks and often skips many of the typical kill chain steps. The focus is more on what's exposed, what they have access to, how they can move around within a cloud infrastructure, and ultimately what actions can be taken. This equates to a subset of tactics, techniques, and procedures, including reconnaissance, initial access, discovery (post-exploitation), exfiltration, and the impact of the ransomware. Let's take a deeper look into these steps.

The cloud provides more than just compute power. It has also become a storage facility for all types of sensitive and business-critical data. Backups, configurations, and cloud logs are all stored within object storage, making it an attractive target for attackers.

Even securely configured workloads can expose all of their data via backups and become a target. Cloud workloads may be vulnerable to unpatched vulnerabilities at runtime and could provide a pivot point into the cloud control plane.

Reconnaissance

Cloud asset discovery is where attackers look for opportunities to gain access to your infrastructure. Recon can be in the form of finding insecurely configured applications, vulnerabilities, or an admin/developer's endpoint that has been infected.

Discovery / lateral movement

This stage can only be done post-exploitation, where they gain initial access. Attackers begin to discover what resources they have access to and what level of access they have. If the attacker does not have sufficient privileges, they will attempt to escalate their privileges in order to complete their attack. If sufficient privileges are already in place, they will move on to the next phase.

Initial access

Attackers will attempt to exploit their findings from the recon stage to gain access to an organization's public cloud. This access can be from compromised credentials, brute force attacks, misconfigured cloud configurations, or exploiting web apps.

Exfiltration / impact

These actions primarily rely on the resources the attacker was able to gain during the discovery / lateral movement phase. Once the attacker reaches this point, they will likely exfiltrate and delete from storage or encrypt in place to cause disruption to the business. Data exfiltration and encryption in the cloud often occurs on cloud storage, such as AWS S3 buckets, but is standard across all major cloud providers.

NIST cybersecurity framework

Identify

Protect

Detect

Repond

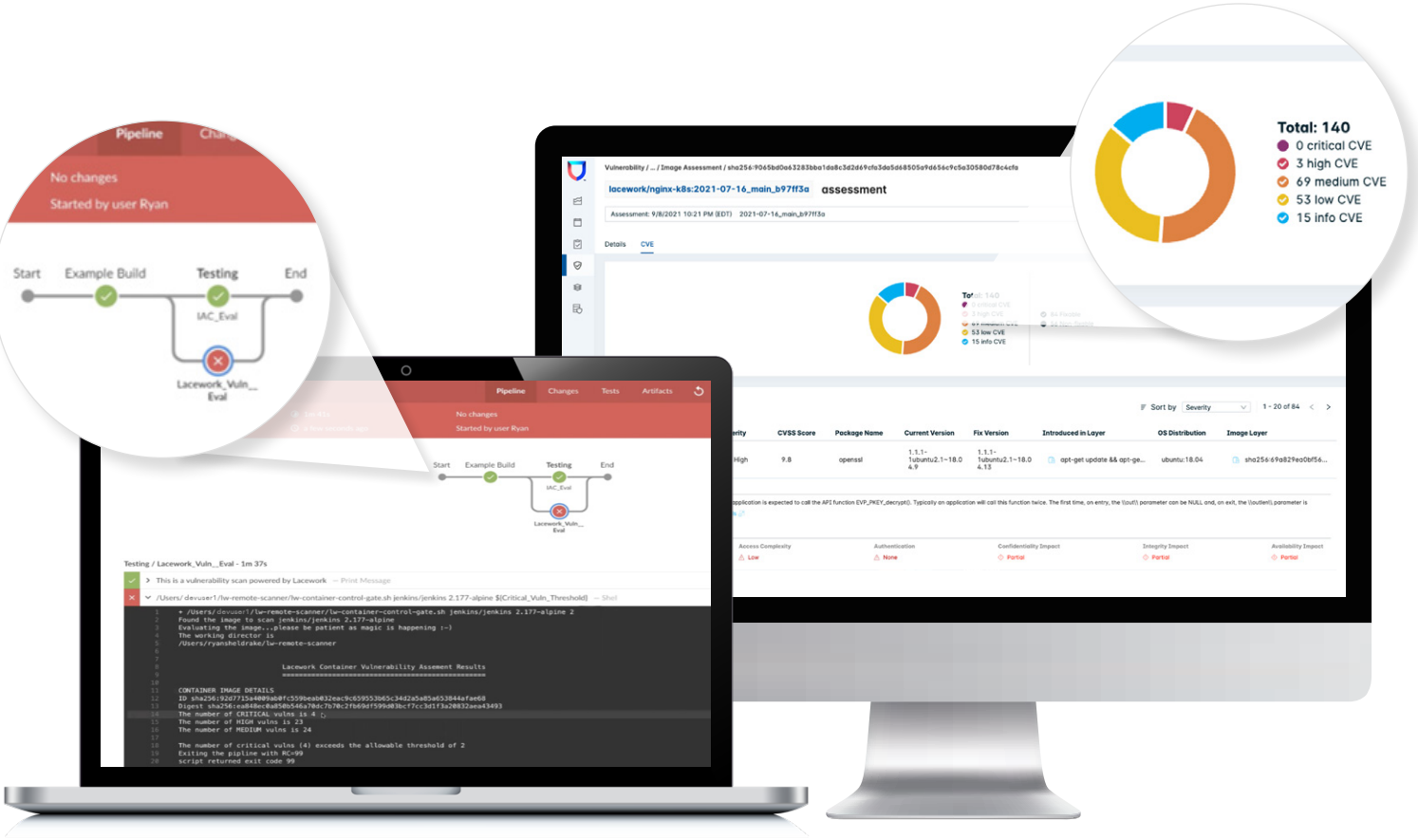
How Lacework helps

With Lacework, organizations can gain the visibility needed to help secure their environment before an attack is attempted, identify an attack as it's happening, and investigate afterward. Many organizations implement a security framework such as the NIST Cybersecurity Framework to manage and reduce risks for their business. Let's take a closer look at how Lacework helps defend against ransomware based on this framework.

Identify

Organizations need visibility across their cloud assets and infrastructure to identify active exposures based on vulnerabilities and misconfigurations. Lacework offers vulnerability management capabilities that enable you to scan cloud environments, containers, non-OS packages such as Python, Ruby, Go, and workloads for vulnerabilities. Identification exposes any critical vulnerabilities that may be used as an initial attack vector to compromise a cloud workload. With Lacework, you can identify vulnerabilities during the development process and in production, especially for externally exposed workloads.

When it comes to ransomware in the cloud, "prevention is protection." By focusing on best practices for vulnerability management, hardening your systems and infrastructure, and gaining visibility into identity management and access controls, you can reduce the risk of infiltration and potential ransomware attack of your cloud. Lacework helps you focus on the appropriate safeguards and best practices, including guidelines and control frameworks like the ones provided by the Center for Internet Security (CIS) Benchmarks, NIST, PCI, HIPAA, ISO, SOC 2, etc., and identifies potential risks as early as possible.



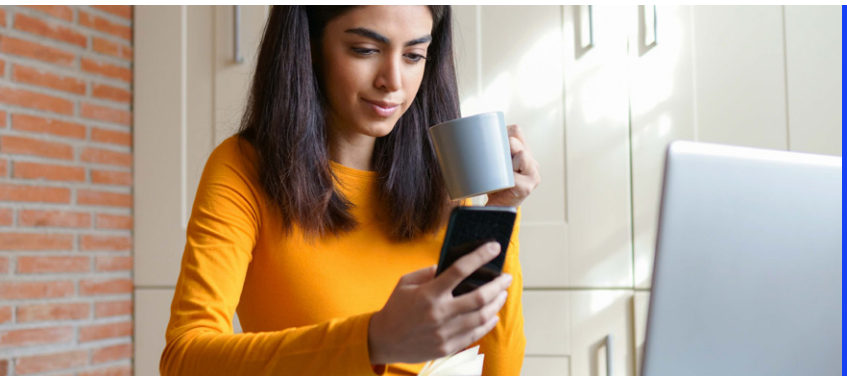


Figure 1 (right): Visual of container vulnerability found during inline scan. Discover and prevent vulnerabilities as early as possible.

Figure 2 (left): Vulnerability assessment overview. Better assess vulnerabilities and their severity in your environment.

Protect

By connecting Lacework with your cloud providers, you gain visibility into cloud controls that leverage the CIS Benchmarks and custom Lacework policies that understand your cloud posture immediately after implementation. Some of these controls can be considered mitigations against potential breaches in the cloud and ransomware if implemented correctly.

For example, within AWS, there are two pre-built custom Lacework policy checks, "S3 Object Versioning" and "MFA Delete." S3 Object Versioning allows S3 objects to be "versioned," which means that if a file is modified, both copies are kept in the bucket as a historical record. The same thing happens if a file is uploaded with the same name as a file that already exists in the bucket. An example scenario here would be a versioned bucket where CloudTrail logs are stored. If an attacker modified a log file to remove traces of their activity, the defender could compare the old version of the file and the current version to see exactly what the attacker removed. S3 Object Versioning is not enough on its own, though, because, in theory, an attacker could just disable the versioning and overwrite/delete any existing versions in the bucket without worrying about a new version being created.

Lacework offers a policy to track "multi-factor authentication (MFA) delete" in S3 buckets to combat this. Having this feature enabled forces MFA to be used to do either of the following two things: change the versioning state of the specified S3 bucket (i.e., disable versioning) or permanently delete an object version if both versioning and MFA delete is enabled on a bucket. This means an attacker would need to compromise the root user and their MFA device to disable versioning and MFA delete on the bucket. This is possible in theory, but in practice is very unlikely.

Lacework continuously monitors all activity and delivers the proper alert at the right time, with all the context needed to take the right action and surface the potential impact. Not only do we uncover known threats, but even unknown attacks that leverage zero-day vulnerabilities. If you want to look for something specific, perhaps based on a unique indicator of compromise, Lacework gives you the ability to create custom policies with the Lacework Query Language. Lacework has the ability to automate correlation, pinpoint vulnerabilities, graph communication paths, and understand behaviors gives organizations a leg up in the fight against ransomware. By identifying these misconfigurations and vulnerabilities across your cloud environment, you can reduce the risk of a ransomware attack compromising your cloud infrastructure.

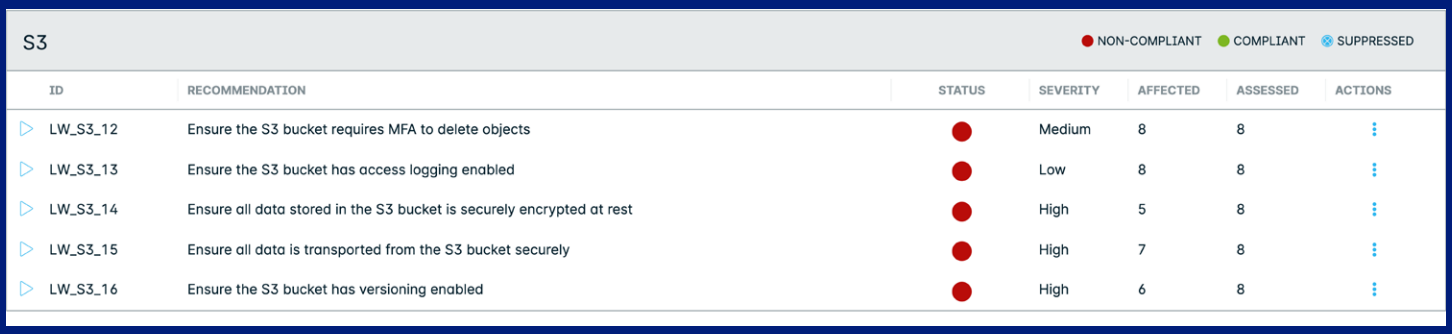


Figure 3: AWS S3 log. Easily understand cloud posture with pre-built policy checks for AWS.

Detect

Early detection is critical in the cloud. It is far less expensive for an organization to remediate an attack prior to exfiltration and encryption of their confidential data. Ransomware is not usually executed immediately after the initial compromise. The attacker needs the time to discover and plan their next move. The average dwell time of an attacker can range anywhere from 5 days to over 100 days. During this time, an attacker makes noise within the cloud environment, which Lacework uncovers using patented machine learning. By automatically learning activities and behaviors unique to your environment and runtime detection, Lacework uncovers abnormal activity and alerts on those unexpected changes, giving the organization an opportunity to be alerted before the attack is complete.

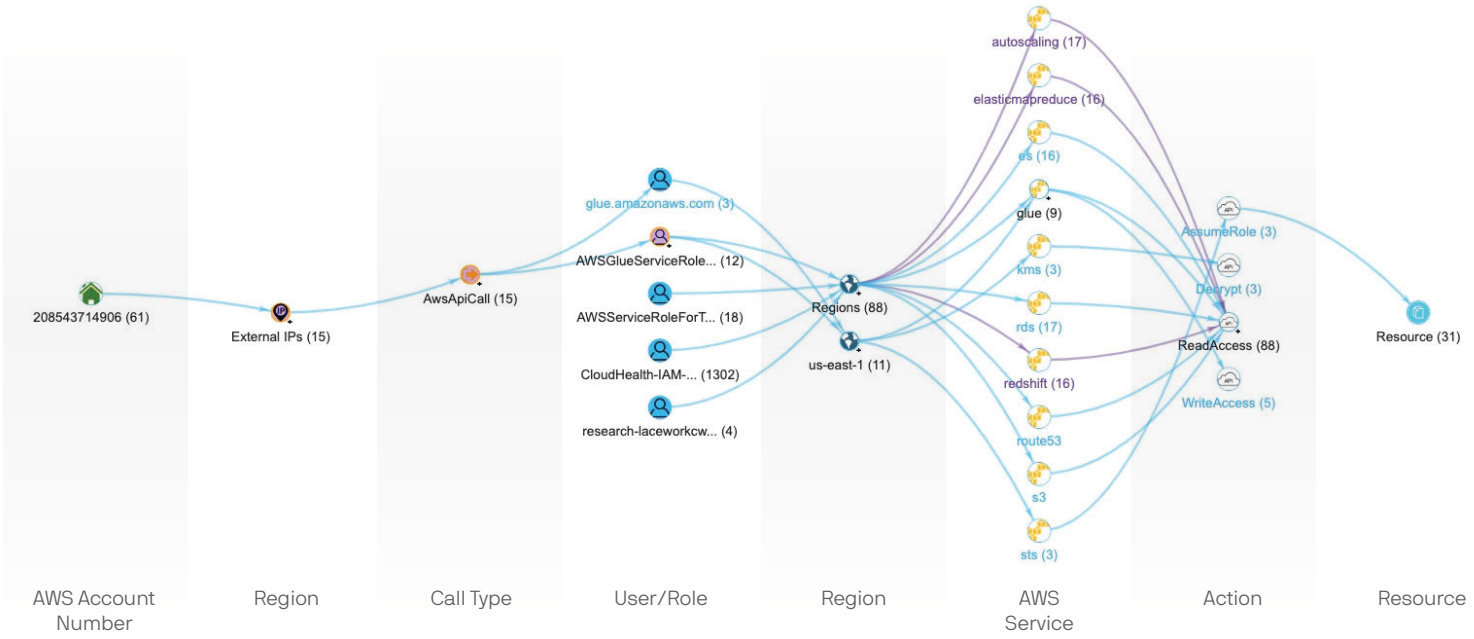


Figure 4: S3 bucket ransomware attack. For CloudTrail, use Polygraph visualization to identify misconfigurations & malicious activity for API behavior.

Respond

Response activities can take many different forms in an organization, depending on the stage at which an incident is discovered. For example, if Lacework uncovers active software and library vulnerabilities, security teams can respond by engaging operations to patch the exposure in their cloud environments. Most response activities happen in production environments and post-breach / attack when security teams take appropriate action for a detected incident. When it comes to a ransomware attack, the security team will need to effectively detect and respond in order to conduct a forensic investigation and determine the impact of the incident, and also support recovery activities. Lacework provides full incident response capabilities with data retention for up to 6 months of unique behavioral and raw infrastructure historical data. Lacework capabilities enable organizations to query across any timeframe, machine, app, or container to understand what was executed and view our patented Polygraph visual representation of the attack chain to aid in the investigation.

Why
the event was triggered

Who
user and/or machine triggered the event

What
user and machine triggered the event

When
time the event occured

Where
cloud region or source IP address

Five W's allows organizations to:

- Determine if the actual cause of the incident was identified and identifying the vector of attack, the vulnerabilities exploited, and the characteristics of the targeted or victimized systems, networks, and applications
- Calculate the estimated monetary damage from the incident (e.g., information and critical business processes negatively affected by the incident)
- Determine if the incident is a recurrence of a previous incident
- Measure the difference between the initial impact assessment and the final impact assessment
- Identify which measures, if any, could have prevented the incident

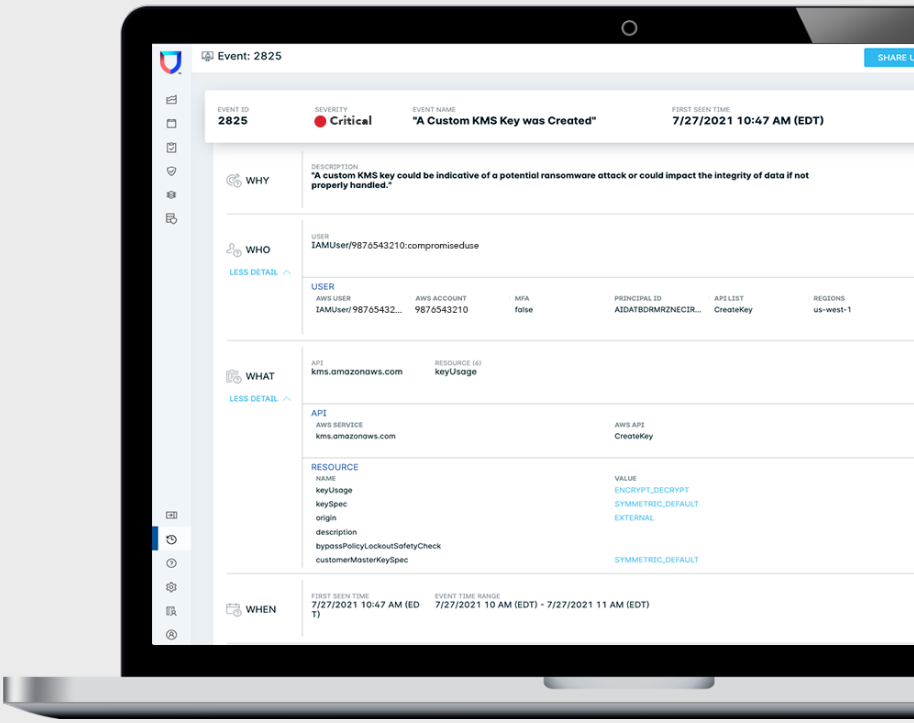


Figure 5: An alert for ransomware attack. Get context –the five W's– to speed incident response and investigation.

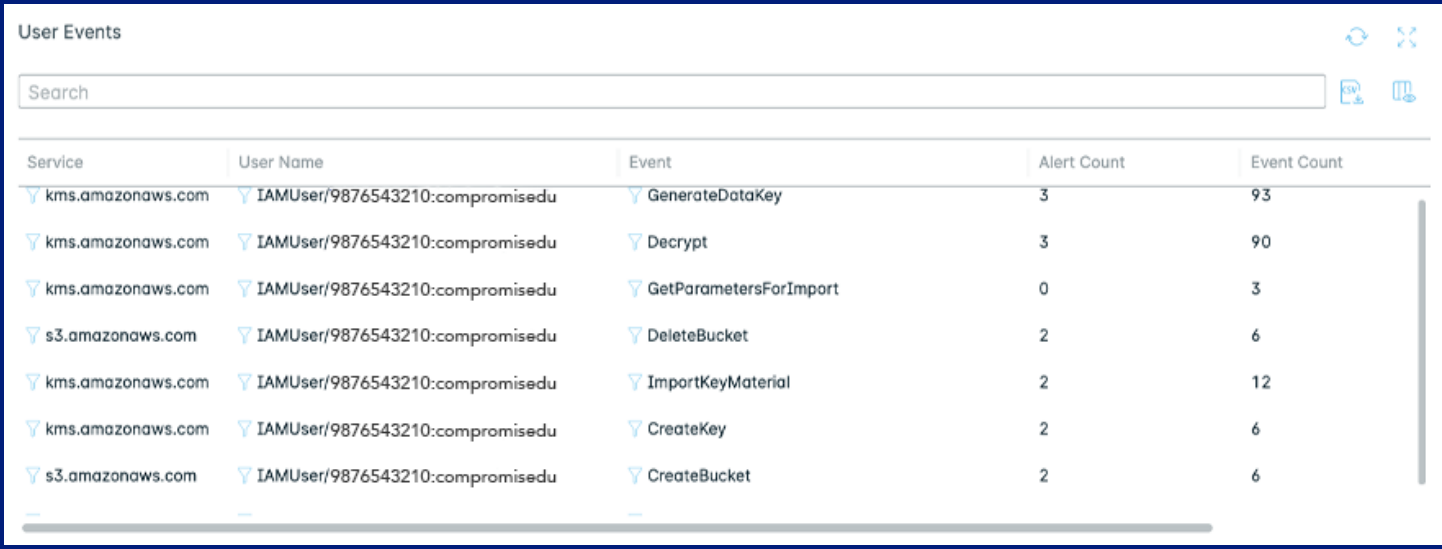


Figure 6: Events during a ransomware attack. Make informed decisions based on attacker activity.

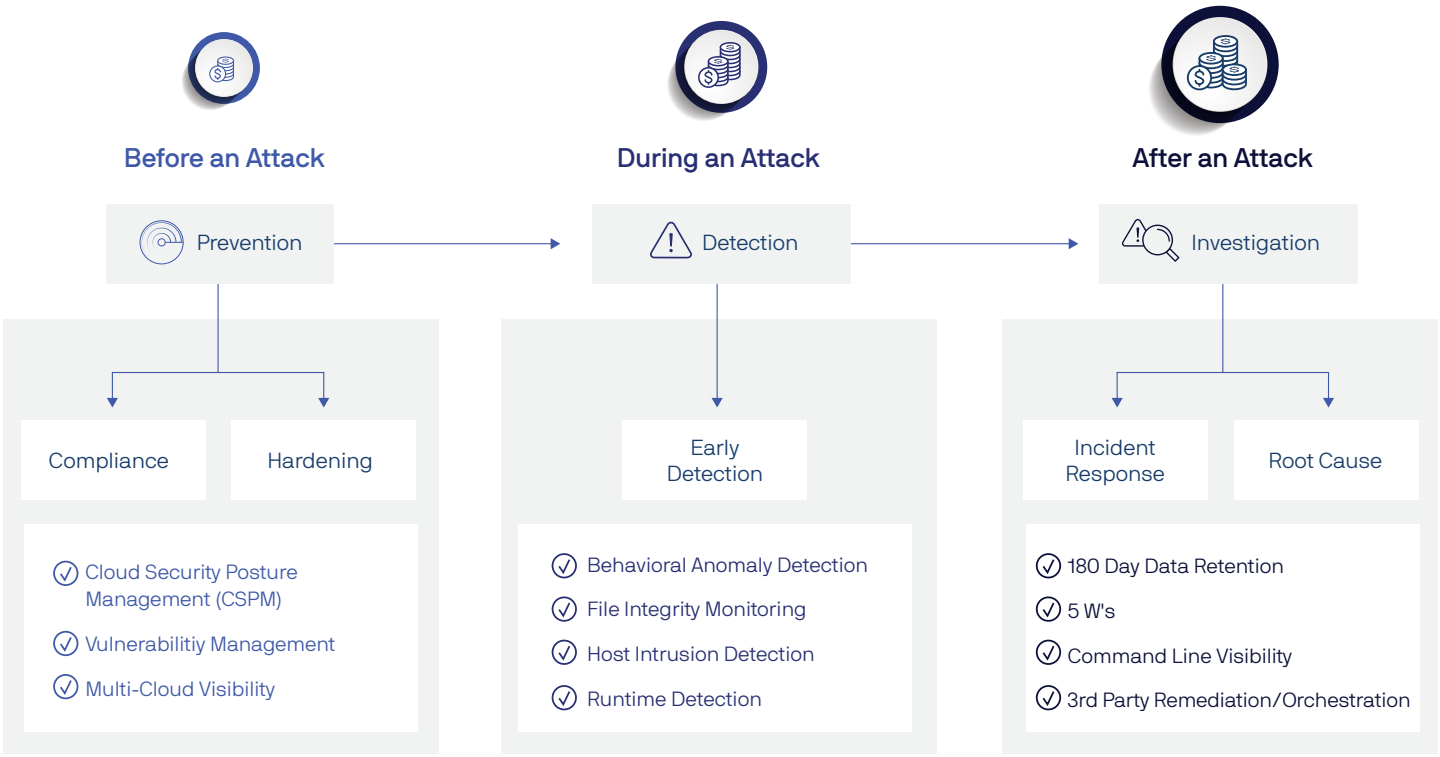
Summary

Lacework believes cloud infrastructure and control planes are vulnerable to these types of attacks. While backups and recovery are easier to achieve in the cloud, our platform focuses on preventing completion of the attack by providing configuration monitoring to alert defenders if a door is open, vulnerability management to allow developers to identify complex software that can be exploited, malware detection to alert users of unwanted software, and anomaly detection to detect if an attacker is accessing an environment. The Lacework platform allows organizations to have the insights to prevent initial entry and the tools to react quickly if an intrusion occurs, ultimately giving organizations the capability to disrupt the attacker before they accomplish their attack. This makes it difficult for the adversary to gain access to resources that would otherwise be exposed. The goal is to tighten and enforce security controls proactively, reduce the attack surface by patching known vulnerabilities before production deployment and minimize cloud misconfigurations.

Here are some other best practices to mitigate the risk of ransomware in the cloud:

- Ensure multi-factor authentication is in place for all external-facing assets
- Rotate master keys regularly – every 45 days is recommended and can be automated
- Restrict the use of customer-managed keys unless specifically required. Customer-managed keys and be abused by an attacker to encrypt S3 server-side data
- Implement instance, billing, and utilization threshold limits with alerting and prevention
- Monitor for internet-exposed vulnerabilities and patch quickly
- Follow compliance standards and enable ongoing tracking with notification of changes
- Alert on never-before-seen IP addresses accessing
- the infrastructure
- Look for changes in permissions, particularly new grants added to master keys
- Implement a cloud workload protection solution that baselines routine activities and alerts on deviations
- Detect the presence of known threats within your environments with automated threat intelligence correlation
- Alert when there are unexpected changes to behavior such as a new location or lateral movement to a new workload
- Enforce the principle of least privilege access in provisioning IAM permissions

Ransomware decision tree tied to cost



Visibility

Extensive visibility across your entire cloud environment

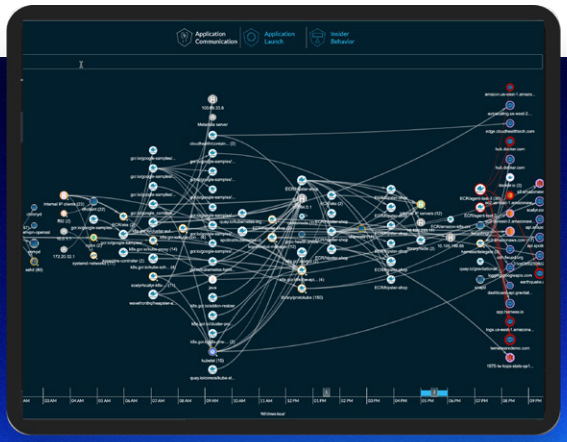
Detection

Comprehensible, accurate detection of what matters most

Context

Automate the understanding of your cloud to make investigations faster

Figure 7: Depicts the measures available to you to prevent, detect and investigate ransomware. It also references the cost your organization will likely incur if a ransomware attack successfully evades prevention ($), takes 5 to 100 days to detect ($$), and requires a lengthy investigation ($$$). This is meant to help you weigh the required approach and cost of the attack to determine what your business might need.



Get a demo to take back your SIEM expenditure and redirect it toward improving your security posture, business agility and value at www.lacework.com/demo.