JupiterOne

CASE STUDY

How Aver Achieves Streamlined, Reliable Threat Modeling

aver®

Aver is an industry leader in value-based healthcare technology providing software, analytics, and services. Their Bundle Benefit Management (BBM) offering provides end-to-end solutions for initiating and operationalizing bundle programs, saving clients 15-20% in medical spend as well as more than a 40% reduction in complications for bundle cases.

How Aver Achieves Streamlined, Reliable Threat Modeling

Proactively assessing your organization's vulnerability to threats requires piles of spreadsheets, dozens of hours poring over cloud security groups, and assembling snapshots of your entire environment. Even then, the confidence in your results is shaky.

The steps and time required to capture detailed metadata of your environment, map the relationships between resources, and ensure the use of the most up-to-date data are some of the reasons assessing your attack surface takes significant time and effort and leaves potential gaps in confidence.

"Manual threat modeling, regardless of the analyst's diligence, is prone to errors," highlighted Zack, who heads up security at Aver Inc., the industry leader in value-based healthcare technology. "On the flip side, there is little appetite for errors when it comes to this sort of analysis."

Threat modeling, though, is something security teams should prioritize and complete routinely. So, finding efficiencies and reliability in such analysis is critical, especially when considering the complexity of the analysis increases exponentially as your company grows.

Zack and the security team at Aver sought to reduce the burden of work required to perform threat analysis without sacrificing the reliability of their takeaways and then generate a detailed report for the senior management team to review.

Challenges

- Needed to reduce time and resources spent on manual threat modeling and analysis
- Desired a solution that could generate consumable and detailed report for the senior management team to review

Results

- Streamlined reporting for executive team to understand organization's overall security posture
- Achieved proactive analysis on potential vulnerabilities and public breaches in single powerful query with JupiterOne
- Improved security team's operational efficiency and robust analysis of potential issues

Key Integrations

- AWS
- GitHub
- Okta
- Tenable
- Slack

"Manual threat modeling, regardless of the analyst's diligence, is prone to errors...there is little appetite for errors when it comes to this sort of analysis."

Zack, Security Lead

Using JupiterOne to Streamline & Centralize Analysis

Improving Data Hygiene

Before leveraging JupiterOne to model threats or assess the risk of similar data breaches, Aver was able to use JupiterOne's automated resource identification, classification, and centralization to spot stale resources across their environment. In addition, improving cloud hygiene drastically reduced noise in the data.

Once the data was up to date, Zack used JupiterOne to model threats and build reports.

Centralized Analysis

Organizations leveraging the cloud are often surprised how resources living in the same ecosystem are siloed from each other. This complexity results in difficulty when it comes to understanding the scope of an organization's environment.

Combining JupiterOne's graph model with deep integrations with dozens of cloud services provides clear cloud visibility for the Aver security team. Exposing vulnerabilities for remediation is simplified because the analysis occurs in one place rather than assembling reports from various places.

Reliable Takeaways

Confidence in the data you've assembled requires accuracy and detail. These details live in the metadata of resources – configurations, settings, permissions, etc. Without a tool, a security analyst must pore over security groups and policies, assess relationships between resources, and assemble concise takeaways.

Unfortunately, human involvement at this level is prone to mistakes as oversights can occur without notice.

Security teams must present accurate and reliable information to senior leadership. The stakes are simply too high when it comes to assessing your organization's attack surface.

The Aver security team turns to JupiterOne, which routinely pulls the specific metadata and relationship details regarding their environment. As a result, Zack and his team can be confident that the picture they see is complete, accurate, and up-to-date.

> **A tool like JupiterOne is critical to completing a robust threat analysis.**

Streamlined Reporting

Along with the analysis, security teams own the deliverable of a detailed report that highlights their organization's security posture.

Unfortunately, building reports is painfully tedious. Rarely can reports be templatized because the analysis and takeaways are unique to each situation. That means creating visualizations and detailing analysis begins from scratch more often than not.

"A tool like JupiterOne is critical to completing a robust threat analysis," said Zack.

JupiterOne Streamlines & Centralizes Reporting

Identifies stale resources & improves cloud hygiene, to reduce noise

Centralized graphDB gives clear visibility & simple analysis of all cloud assets

Automated data collection & relationship mapping provides a complete picture

Reports are automatically generated, removing the need for manual creation

From Modeling Threats to Post-Breach Analysis

The increased coverage around large-scale public data breaches has increased executive scrutiny on their own environments.

When a major breach hits the news cycle, senior management's eyes shift towards security and IT teams. The question is simple: are we vulnerable to the same sort of attack? Unfortunately, the answer to that question can be elusive. Not because the data doesn't exist. The challenge security teams face is that the data exists, mixed into a haystack of complex relationships.

For Zack, as is the case with most security teams, report requests assessing his own organization's susceptibility to similar attacks occur regularly. "I would say news of large public data breaches happens once a quarter, with smaller requests occurring monthly – both of these require assessments of our own risk."

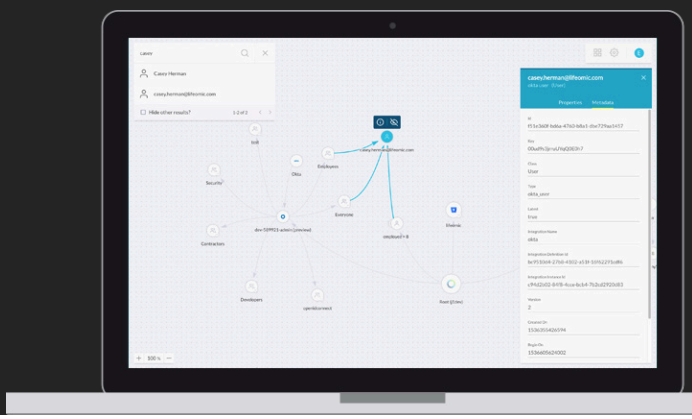
With the demands for post-breach analysis and reliable threat modeling not going away, how can security teams assess their risk exposure to similar attacks when environments cover dozens of services and tools?

Power in a Single Query

The insights Aver derives from JupiterOne regarding their environment rely on queries of data and relationships. These queries provided by JupiterOne offer a universally reliable and flexible way to view their environment.

Following the recent, largely publicized CapitalOne data breach, Zack reached out to the JupiterOne team and asked, "is there a single query I can run to assess my organization's risk to similar attacks as a result of overly broad permissions?"

Within a few hours, a query was assembled and distributed, allowing companies who use JupiterOne to ask the simple question: is my environment exposed to vulnerabilities similar to the Capital One data breach? This query is capable of producing a complete list and relationship view of any critical resources that need to be addressed – in seconds.



The Value of Speed and Reliability

Increasing the reliability of threat modeling and reducing the time and effort to assemble the reports directly impacts Zack's and the security team's operational efficiency. Robust analysis can happen quickly through JupiterOne without disrupting the organization but still provides the detail and insights needed to present confidently to the leadership team.