MixMode™

MIXMODE CUSTOMER STORY
LARGE GOVERNMENT ENTITY

CUSTOMER STORY: HOW A GOVERNMENT ENTITY SWITCHED TO MIXMODE AND DECREASED DATA STORAGE COSTS BY 50%

Key Benefits:

- Significantly lower storage costs over a SIEM solution.
- Real-time network oversight.
- Transparent pricing structures.
- Eliminating legacy log data issues.

"Through the process with this large municipality, they were able to save 50% on their overall costs versus their previous SIEM. This was accomplished by MixMode filling their need on SIEM, NTA/NDR and UBA in one platform, coupled with the storage savings that we were able to deliver."

The Challenge

Data is the beating heart of every modern organization, but it's only valuable when it's accessible, understandable, and most importantly, protected.

Well-intentioned municipalities and enterprises work toward these goals by attempting to craft sound network architecture, deploying security software and designating repositories for sorting and storing data.

As discussed in our recent white paper, "The Data Overload Problem in Cybersecurity," many organizations find that as they grow and scale, the systems they've put in place are not able to fully manage and protect constant incoming and outgoing streams of data. Networks become overloaded, vulnerabilities appear and bad actors swoop in to take advantage.

Over time, enterprises turn to solutions like Security Information and Event Management (SIEM), which, vendors promise, will allow them to maintain control and oversight of their data, at a reasonable cost.

> *"Aside from license costs, storage is very expensive due to the all-consuming nature of these products. The additional benefits of recording everything on the network are typically weighed down by large-storage problems and sub-optimal event management."*
> - SolarWinds Whitepaper

Unfortunately, more often than not, SIEM platforms outright fail at achieving what they promise and they end up costing enterprises significantly more than originally budgeted.

64%

of organizations pay more than $1 million annually for external consultants and contractors to assist with SIEM configuration and management.

- Cyphort

"Once the log storage limit is exceeded, customers have two options: lose your data or upgrade to the next level."

Because SIEM is completely reliant on log data and enterprise data is constantly expanding, organizations are often hit with storage bills that far exceed initial cost projections. At the root of this spiraling cost issue is the inherent nature of the solutions large enterprises use to police their networks.

SIEM vendors promise to meet client needs for years to come, and even explain how they will use logging techniques, but often fail to fully disclose just how much "hot/warm storage" it will take to fulfill those needs — and just how much it will cost.

Traditionally the customer pays a license cost that ends up turning into a bill that's three or four times that base license cost by the end of year one.

This was exactly what happened to a large government entity that recently turned to MixMode when their chosen solution fell short. Despite an arduous three-year long ongoing SIEM deployment, and a two-year User Behavior Analytics (UBA) tool deployment, these platforms proved incapable of providing the necessary real-time insight into their network behavior that was necessary for effective threat detection and remediation. Looking ahead, it became clear that log storage costs were sure to continue spiraling beyond what they could afford.

The Solution

MixMode helped the government entity deploy a next-generation SOC platform based on patented Unsupervised Artificial Intelligence (AI) capable of comparing real-time behavior against a self-learning and adapting baseline of expected behavior. This approach allowed them to address their SIEM, UBA, and NTA needs, free from the obligation of never-ending log storage increases.

Their originally chosen third-party UBA/SIEM solution was dependent on rules-based alerts, queries and dashboards designed to provide threat intelligence. Because these SIEM and UBA deployments (like almost every other cybersecurity platform currently available) had a dependence on historic log data to identify threats and anomalies, they were completely unable to predict future behavior or real-time threats. With a platform like MixMode which utilizes unsupervised AI and self-learning, these things would become possible.

MixMode identified active attacks and probes being missed by this piecemeal system, without relying on historic or aggregate log data and examined their SIEM solution from two primary angles:

- How much data the entity was generating.
- How much incremental data storage was required because of vendor labeling.

Ultimately, MixMode found, the log-based SIEM approach resulted in five times the amount of data that needed to be stored, a cost that was passed along to the government entity. Essentially, the SIEM vendor, like all SIEM vendors, gathered data, labeled it (which expanded the size of the data stores), and sorted it so that their product would work, without communicating true anticipated storage costs from the start.

In order to continue using the multiple log storage data repositories, which were proprietary to the SIEM and UBA vendors thanks to the extensive labeling, the government entity would need to pay exorbitant licensing and additive storage fees.

MixMode™

MIXMODE CUSTOMER STORY
LARGE GOVERNMENT ENTITY

"Traditional log aggregation approaches from rule-based systems don't have any real insights. The predefined queries and dashboards lack the alerts that one would need to identify threats."

The Results

Within the first 24 hours after deployment, MixMode had enabled the government entity to regain control over the security environment and network data infrastructure. No longer limited to log data analysis, they were able to identify and address real-time threats as well as network and operational configuration challenges.

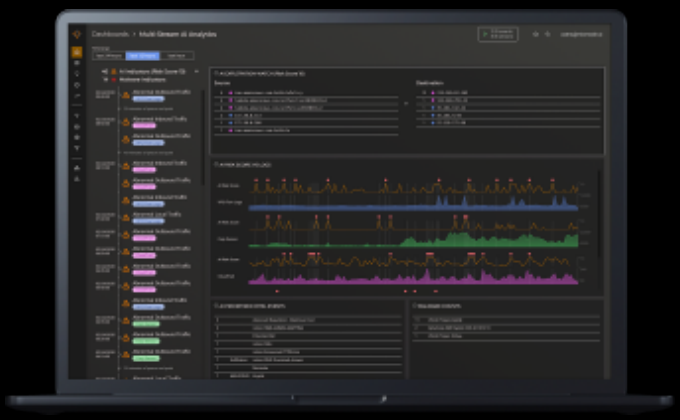
"We are able to shrink storage requirements by a wide amount," said a manager associated with the project. "Instead of the existing SIEM solution increasing data storage needs by 400 or 500 percent. With MixMode we can decrease it by 50 to 60 percent."

Similar MixMode clients have saved between 60 and 80 percent over their previous SIEM vendor contracts. The difference is in the approach. Instead of using warm storage where data is always standing by, MixMode:

- Ingests and compresses the raw data packet and sends it to cold storage.
- Eliminates the requirement for labeling and normalizing.

MixMode doesn't create a proprietary data labeling conflict like a traditional SIEM, and it doesn't require additional databases or time-consuming steps to monitor network behavior.

"Enterprise cybersecurity teams waste millions of dollars and man-hours every year storing, aggregating and managing data with traditional SIEM platforms. The solution is to instead leverage unsupervised AI-driven analysis and predictive anomaly detection across multiple streams of data in real-time, at scale with a platform like MixMode."
- Ritu Jyoti, AI Analyst, IDC



How Can MixMode Help You?

In some ways, the problems associated with log storage based SIEM solutions seem inevitable. Data is dynamic, ever-expanding and if it's not handled proactively, prone to overloading systems and system operators alike. MixMode customers know it doesn't have to be this way.

MixMode leads with innovation. Clients gain access to predictive alerting solutions that empower them to access robust, game-changing security features without being gouged by an unethical pricing structure.

"MixMode has proven to be a far more effective platform than traditional cybersecurity tools, at a fraction of the cost," explains Geoffrey Coulehan, Head of Sales and Alliances at MixMode. "Our customers achieve positive ROI with greater efficacy in identifying and addressing cyber threats by taking advantage of our Unsupervised AI and eliminating the need to store data in a redundant, proprietary format."