Blumira

CASE STUDY

Duraflame

Founded in 1972, Duraflame is the well-known U.S. firelog brand leader, manufacturing firelogs, fire starters and barbecue fire products for 50 years. They have two main manufacturing facilities located on the West and East coasts for log manufacturing, and several charcoal plants located in Texas and Kentucky.

The Challenge: Increased Cloud Security Risks and Lack of Visibility

Duraflame was undergoing a digital transformation focused on IT modernization to support employees working from home offices during the pandemic. As they moved from primarily on-premises technology to cloud-based services, they also realized they had a lack of visibility into cloud security risks.

Duraflame's Director of IT John Hwee runs IT and security services at the company with a small team of IT and external partners. As the company continues to grow and increase their security posture, they started investigating a comprehensive security solution that could quickly and accurately detect and respond to security threats. The solution also needed to be accurate, robust, scalable, cost effective, and easy to install and manage.

Complicated, Costly SIEM Options

When the Duraflame IT team started researching different SIEM (security information and event management) vendors and solutions, they faced similar challenges of high costs and complex implementation and management overheads while evaluating products like AT&T AlienVault and Splunk.

> "I didn't have the budget to spend on partnering with a managed SOC (security operations center) provider. All of the solutions we looked at required a long-term commitment with a high barrier of entry," John H. said.

With a small IT team, Duraflame needed a SIEM that could quickly and accurately aggregate and centralize all logs and, more importantly, provide comprehensive security visibility into their overall infrastructure.

> "I need to know what's happening in my environment – when a system is having a problem, under attack, or compromised," John H. stated.

Industry

Manufacturing

Driver

Cloud security risks, malware attacks

Company Size

201-500

Challenge

With limited IT budget and staff, Duraflame needed a secure, reliable, user-friendly, and cost-effective way to protect against internal and external security threats and malware, without the heavy cost of managing a SOC.

Solution

Duraflame deployed Blumira's cloud SIEM in less than four hours which provided actionable data to detect and respond to threats on its network. Blumira's platform can quickly scale and provide a predictable SaaS cost model.

Sign Up Free!
blumira.com/free

The Solution: Blumira's Easy-to-Use Cloud Security Platform

After attending a virtual CIO summit conference, Duraflame evaluated a handful of industry leading vendors, including Blumira. Duraflame needed a cloud-based solution that could be implemented quickly and provide complete and accurate security visibility. Duraflame's IT team and executive management were concerned with the high cost, complex and lengthy implementation time required by other solutions.

> *"I was looking for something new and different from the Splunks and AlienVaults of the world," John H said. "A solution that focused on the user experience and security relationship."*

As head of the decision-making process for determining what security technology and which vendors to acquire, John H. needed to sell the Duraflame IT team on what the solution was capable of, as well as show them how easy it was to implement.

He also had to sell executive management on the value of Blumira's solution – not only ease of deployment, but a good return on their investment by quickly detection, alert, and reporting all in one platform.

> "Knowing that I have something I can look at that can correlate everything is a real time-saver. I'm able to sleep at night knowing that all of our logs are centralized and I will know when there's a security event," John H. said. "The proactive nature of Blumira is something that pays for itself."

John H. was looking for a solution that was not only easy to use, but also provided a sense of predictability when it came to its pricing model. Blumira's easy-to-understand pricing model with a predictable monthly cost, along with flexible payment options allowed management to quickly approve the solution.

> "I like the predictable model," John H said. "I don't have to worry about how many endpoints I have or additional hardware required as Duraflame grows over the next few years."

Automate Detection & Response With Blumira

- Built-in integrations across hybrid cloud infrastructure, applications and services
- Simplified log collection, threat detection & response playbooks for remediation
- Scheduled, automated & customizable reports of security threats
- Access to Blumira's security experts for additional security advice

"Knowing that I have something I can look at that can correlate everything is a real time-saver. I'm able to sleep at night knowing that all of our logs are centralized. Blumira's dashboards provide accurate and high-fidelity actionable alerts."

- John Hwee, Director of IT

Sign Up Free!
blumira.com/free

He also liked the cloud-based nature of Blumira's solution that didn't require any dependencies on their current infrastructure, nor required his small team to support additional on-premises infrastructure. Patching and updates are taken care of remotely and automatically rolled out to Blumira's platform when available, making management easy for small to medium-sized companies.

5x Times Faster to Deploy With Real Security Value

Once Duraflame decided to start a trial of Blumira's platform, the Blumira team guided John through a quick proof of concept to start integrating with Duraflame's existing technology to collect logs, detect and analyze threats, and provide playbooks for easy response.

> *"Blumira's demo and free trial period gave us a lot of value and was pretty easy to do," John H. said. "The total implementation process took less than 4 hours to get fully functional."*

Blumira's team met and completed an hour-long working session to implement critical server sensors. Within 24 hours, Blumira's platform collected and correlated security events and provided recommendations. During the trial period, Duraflame's IT team completed deployment of all the sensors.

Now Duraflame has broad security coverage across their entire environment, including Windows, Office 365, Azure AD, Windows servers/workstations, Sophos Central, Meraki Firewall, Fortinet AP, Linux and Email.

> "It has given me a large level of relief to have a tool that gives me visibility into any major events on the network without having to dig for it," John H. said. "I do feel pretty comfortable now that we don't have unknown suspicious activity happening on my network and getting high-fidelity alerts from Blumira. We now have full visibility of our infrastructure."

In a comparison of 12 SIEM vendors on G2, **Blumira's solution was found to be five times as fast to fully implement and deploy**. The average time to security typically takes at least two months to get up and running, with additional time for ongoing operational management. While many other solutions require time to fine-tune and write detection rules, Blumira's platform comes with pre-written rules to both help reduce the noise of false-positives while increasing a customer's time to security significantly.

Start your free trial to easily detect and respond to threats in your environment, within hours.

Sign Up Free!
blumira.com/free