# TAS United Case Study

## How TAS United Replaced Splunk With Blumira for Fast Deployment & Greater Security Value

> "We don't have to go digging to uncover findings, alerts or reports. We're already getting a benefit out of Blumira without spending any time fine-tuning it - that's one thing in the SIEM space you can't say about other offerings."
>
> – **Tim Brewer**, Systems Analyst, TAS United

TAS United is a Texas-based telecommunication company, with a distributed office. They provide customized, secure call processing solutions for customers nationwide through their specialized technology platform. TAS United supports call processing operations for organizations of any size, including small to large enterprise, across healthcare/medical, construction, education, energy/natural resources, legal, real estate, government, hospitality, and e-commerce industries.

### The Challenge: Securing Remote Work & PCI DSS

The major shift to remote work meant all of TAS United's call center employees were now working from home and needed to use their personal devices to do their jobs. Securing BYOD (bring your own device), as well as properly managing and supporting IT for employees remotely became a priority and a challenge for the telecom company.

In addition to supporting and securing remote employees, TAS United needed to meet PCI DSS compliance.

**Industry**
Telecommunications

**Driver**
Remote workforce & PCI DSS

**Company Size**
51-200

**Challenge**
TAS United needed to secure and support a fully-remote workforce using their personal devices to do their jobs, while meeting PCI DSS compliance.

**Solution**
TAS United replaced their Splunk SIEM solution with a more user-friendly one built for lean IT teams with limited resources. They turned to Blumira for greater visibility, easier log search and investigation, and fast proof of concept to quickly meet PCI DSS.



The Payment Card Industry Data Security Standard requires organizations that process or collect cardholder data to meet certain event logging and reporting requirements that can help them detect and prevent cybersecurity attacks.

When Tim Brewer, systems analyst, security and compliance officer for TAS United first came onboard with the company, they were running Splunk as their internal SIEM (security incident and event management) solution. But to use it effectively, the platform required extensive time to manage and deep knowledge of the particular ins and outs of how to use the solution.

"With Splunk, you need to know specific ways to structure queries for what you're looking for," Brewer said. "You may as well have to learn a new form of SQL."

At the time of license renewal, they started to seek an alternative SIEM solution that was more user-friendly for lean IT teams with limited resources, and could help them easily pass their PCI DSS audit. The other solution they were using only collected a subset of logs, with more focus on alerting rather than visibility into their environment. To get to visibility, they would have to upgrade to a higher licensing tier at a more expensive cost.

### The Solution: "It's More the People Than the Product"

Brewer was looking for a SIEM solution that made it easier to investigate and search log events, as well as provide custom alerts that would help them pass penetration tests.

With their PCI audit fast approaching, they needed a security partner that could deliver on pace to meet their needs. That's when they turned to Blumira.

> "Our truncated time table was not a problem. Blumira was very fluent in helping move the process along, with a proof of concept up and running within a few days.

The proof of concept allowed Brewer to quickly demonstrate to his boss, the CTO, that they could see Blumira's platform in action on their network working without any issues; influencing his decision to sign the contract.

"The product is good and solid," Brewer said. "Differentiation in this space is hard to come by – while Blumira's product does stand out – it's more the people building the product than the product. You can have the best product in the world, but if it doesn't seem like the people involved are approachable or happy to help, then it just doesn't make me excited to use the product. It's that symbiotic relationship that many businesses have forgotten over the years."

### Security Automation, Powered by Real People

Before he joined the company, security operations were done manually and required knowing where to go to track information down. Building reports was a manual, slow and difficult process. With Blumira, TAS United gets more automated visibility into their overall environment.

"Visibility is a major thing for security, and it simplifies our processes," said Brewer.

TAS United gets the most value out of Blumira's findings that provide deeper threat analysis to help their team better understand detected threats and how to respond to them.

"It's not just about machine-learning, AI, or whatever the buzzword is – every single one of [Blumira's] triggers are purpose-built by people that have looked at how network disruptions are happening," said Brewer. "It's more about how all of this data gets read and processed through. It's still that human component that has created the picture of how to look through it and how to process it."

Blumira's automated threat detection and response platform is powered by the dedicated people behind the product. Engineers develop and maintain parsers on an ongoing basis to effectively normalize data and extract security value from raw logs (so customers don't have to). Blumira's security analyst team proactively hunts threats and writes detection rules to identify indicators of ransomware, lateral movement, password spraying and other attacks. Then they provide easy-to-understand playbooks to walk customers through next steps for threat response, remediation and containment, with options to automatically block known threats.

"You've got good people doing good work, and it accentuates the platform," said Brewer.

## Faster Time to Security Value With Ease of Deployment

When it came to deployment of Blumira's cloud SIEM, they had the entire technology stack up on it within a day or two.

The ease of deployment and automation built into the rollout allowed his small team to remotely stand up an office in Puerto Rico easily in under a day.

> "The roll-out was absolutely simple."

TAS United was able to easily integrate Blumira with their Fortinet Fortigate firewalls, Windows Defender, Active Directory servers, Microsoft Azure, Office 365 and Linux.

The business outcomes of partnering with Blumira have led to an increase in productivity for Brewer's lean team leading all security, IT and infrastructure needs for the organization.

"We don't have to go digging to uncover findings, alerts or reports," said Brewer. "We're already getting a benefit out of Blumira without spending any time fine-tuning it – that's one thing in the SIEM space you can't say about other offerings."

After Blumira helped TAS United achieve the logging and reporting they needed to meet PCI DSS compliance, they were able to complete their third-party assessment that helped earn the business of a customer that required vendor compliance. The value of Blumira allowed them to meet their business objectives, while automating and expediting the security operations process.



# Blumira

## Automated Detection & Response

Designed for small IT teams to deploy in hours

Blumira's modern cloud SIEM platform provides guided, actionable insights into cybersecurity risks to enable you to effectively detect and respond to threats.

### With Blumira, It's Easy to:

**Collect & Centralize Security Events**
Integrate with your existing tech stack for broad coverage across on-prem and cloud

**Automate Threat Response**
Implement blocking rules and stop active cybersecurity threats without manual intervention

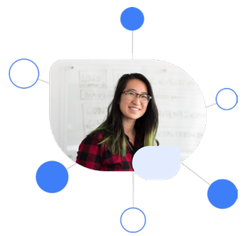
**Guided Security Playbooks**
Step-by-step incident response workflows are built into the platform to help guide IT teams without security expertise

**Rapidly Detect Cybersecurity Threats**
Backend automation and fine-tuned detections identify threats faster

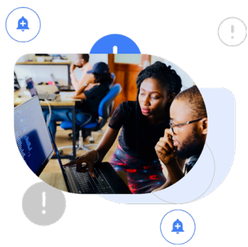
**Report on Security Findings**
Schedule and run reports for your executive team, auditing and compliance needs

**Deploy in Hours, Not Months**
Easily integrate Blumira with your network, firewalls, endpoint, identity, cloud infrastructure and more

### Streamline Security Operations



**Ease of Use -** Small teams can easily deploy and manage security with Blumira's cloud platform



**Save Time -** Reduce the noise with Blumira's prioritized alerts, enabled by pre-built rules and tuning

**Security Expertise -** Run lean while getting access to Blumira's security team for advice in investigations

Blumira was voted best ROI, fastest implementation, easiest-to-use, best relationship, best support, high performer, best results and more by real customers on G2.


**Get a Free Trial!**
**blumira.com/trial**