PathForward IT
BE CONFIDENT IN YOUR IT.

Blumira
CASE STUDY

Path Forward IT

Founded in 2002, Path Forward IT steadily expanded their reach to a national footprint spanning 30+ states. Originally designed to serve the healthcare industry, their services ensure high-caliber, tailored solutions, personalized service, rigorous security knowledge, and technical expertise that helps companies operate more efficiently, scale more effectively, and adapt to change more quickly.

As partners, Path Forward and Blumira ensure IT reliability is paired with an easy-to-use security operations platform that enables teams of all sizes to detect, prevent and respond to cybersecurity threats, such as ransomware.

The Challenge: Ransomware Concerns, Lack of Visibility

Path Forward was looking to increase their security posture and gain deeper visibility into network-related and Windows events, without having to put a ton of work into forwarding, monitoring and searching through logs, according to their Director of Cybersecurity, Adam Thomas.

> "Ransomware was high on our list of concerns when we were looking at Blumira and other products. We take our security seriously, and we wanted to update our security posture so our customers can keep operating normally," Thomas said.

They wanted to take proactive measures to prevent a potential ransomware incident that could lead to their clients getting compromised, similar to what happened with the Kaseya ransomware attack in July 2021. Attackers exploited a vulnerability in Kaseya's IT management and remote monitoring software, targeting 60 MSPs and affecting over 1,500 organizations, many of whom were downstream clients of those MSPs. Path Forward wasn't impacted by the Kaseya incident, but it served as solemn validation of their security focus.

Many of Path Forward's clients are in the healthcare industry and require HIPAA compliant security measures to protect sensitive information and reduce any impact on patient care — including disruptive ransomware attacks. Meanwhile, Path Forward's IT team was juggling multiple IT and security projects, so they needed a solution that could enable them to easily set up and manage a log aggregation and detection and response security platform for their clients that met industry data retention requirements.

Industry

Managed Service Provider (MSP) - IT

Driver

Increase security posture; prevent ransomware

Company Size

MSP With 40 Clients

Challenge

As a managed service provider (MSP), Path Forward IT needed deeper visibility into their network and Windows environment to protect both themselves and their clients against a potential ransomware attack.

Solution

With Blumira's easy-to-setup cloud SIEM backed by a security operations team to help with detection and response, Path Forward has gained greater insight into their environment, identified previously unknown issues and reduced the time it takes to find and remediate problems to help prevent events like a ransomware breach for their customers.

Blumira

CASE STUDY

The Solution: Fast Rollout, Easy to Manage

Path Forward's chief technology officer, Dale Montgomery recommended the solution to Thomas and their team for internal use after working with Blumira for several months.

They were able to easily deploy and integrate Blumira's cloud SIEM platform with Carbon Black, Windows, SonicWall and Palo Alto firewalls, while also leveraging Blumira's honeypots to detect attacker attempts to log into systems remotely.

The ease and speed of implementation of Blumira is a major advantage when they roll it out for their customers, especially with a small team.

> "Rolling out Blumira for a new customer takes just about four hours," Thomas said. "I would love to get Blumira deployed to all of our customers to help them become more security aware. With Blumira, we're able to see what happens, stop it quickly and keep our customers secure and happy."

Path Forward's busy IT team can efficiently manage their many different customer accounts with the help of Blumira's multi-tenancy built into the platform, simplifying their workflows by providing one login to access all customer accounts.

Shining a Spotlight: Simplified Detection & Security Reports

Many of their healthcare clients benefit from Blumira's automated detection capabilities that help Path Forward uncover previously unknown security and operational issues with log collection and management.

> "Blumira shines a spotlight on issues we didn't know about before, such as unexpected SSH connections from the internet and originating from international locations," Thomas said.

After Path Forward deployed Blumira and Sysmon (System Monitor), they were also alerted to a number of customer files that may have contained passwords, a practice that can increase a customer's risk profile if an attacker was able to gain access to and steal a list of passwords stored in plaintext.

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

"I would recommend Blumira** — it makes our daily job so much easier and **it's simple to set up security for our customers."

- Adam Thomas
Director of Cybersecurity
Path Forward IT

Sign Up Free!
blumira.com/free

> "I would recommend Blumira — it makes our daily job so much easier and it's simple to set up security for our customers. We only receive alerts that we need to act upon, and if it gets noisy, we can work with [Blumira's security operations team] support to tune alerts," Thomas said.

Blumira's SIEM platform is designed to automate detection and response for the Path Forward team, with new security rules, tuning, parsing and management completed by the Blumira team. Once Path Forward set up integrations to stream logs into Blumira's platform, there was nothing else required of their team for security expertise.

Every finding sent from Blumira's platform comes with security analysis, playbooks and workflows to help Adam and his team quickly respond. If they need additional help, the Blumira security operations (SecOps) team is available to answer questions or assist with response 24/7 for urgent issues.

Path Forward leverages Blumira's reporting capabilities to understand trends in their environment, including failed user account logins and account lockouts. Thomas and his team are able to drill down further to find the source of the lockout, relying on Blumira's reporting and log history.

> "Blumira's dashboards are really helpful for new clients – we can immediately see the most active devices and top alerts without having to do anything," Thomas said.

Automation Backed by Live Security Experts

Paired with the platform are the people behind it — the incident detection engineers that keep up with the latest exploits, writing new rules and releasing updates to previous ones automatically to ensure our customers are protected. Meanwhile, the development team consistently creates new parsers and integrations to keep expanding security coverage for new third-party applications and services.

> "The Blumira team has been fantastic; everyone has been very helpful with quick responses — I couldn't ask for more," Thomas said.

Blumira's security operations and technical account manager team work closely with partners and customers to provide their security expertise through onboarding, incident investigation, guided response and ongoing consultations that work to continuously improve their security maturity.

Become a Partner!
blumira.com/partners