flare

Web Hosting Company Increases Security Team Bandwidth with up to 80% Decrease in Threat Research Times

The Customer

20 years of web hosting experience

Provides domain registration, web hosting, and cloud services to 1.5 million sites, blogs, and applications

Supports over 400,000 web designers, developers, content creators, small businesses, and entrepreneurs

Industry Targeted By Attackers and Regulators

The internet is more than an information highway; it creates human connections, drives business operations, and drives innovation. When a hosting provider experiences a security incident, the harm trickles down to everyone using the company's infrastructure.

For threat actors, the vast amount of sensitive data that web hosting providers store and transmit is a digital goldmine. In 2020, sophisticated cyber attackers compromised the login details for a well-known web host's employees and 28,000 of its customers. Slightly over a year later, attackers gained unauthorized access to the hosting platform, impacting 1.2 million customers.

> "Everyone in the organization was blown away by the information we were able to get from Flare during the trial period. Within a month, we knew we wanted the real-time information and alerts that being a customer offered."
>
> **SVP Infrastructure, Web Hosting Company**

In response to this, the Federal Trade Commission (FTC) commenced an investigation that culminated with a complaint and, eventually, a settlement order. The final settlement focused on ensuring that the provider's data security promises were backed by action.

As cybercriminals and regulatory agencies focus on the industry, the web hosting provider sought a solution that would enable its security team to centralize and operationalize threat intelligence.

Challenges: Disconnected, Open-Source Intelligence

Understanding the importance of monitoring cybercriminal activity, the web hosting company's security team worked with open-source threat intelligence resources to gather information about leaked or stolen credentials. They relied on various sources from publicly available clear web resources to third-party security researchers for insights into potentially risky accounts.

While the web hosting provider engaged in manual dark web searches, the process was time-consuming, especially with ransomware leaks that could be hundreds to thousands of gigabytes or even multiple terabytes in size. When searching for a small number of specific files, the process became onerous. As sophisticated threat actors began targeting the industry, the security team learned that some contractors' compromised credentials were circulating on illicit Telegram channels.

In response to these challenges, the web hosting company sought a solution that would allow them to gain coverage for leaked information about or cybercriminal discussions of the company.

Implementation: Easy Onboarding with Near Immediate ROI

The web hosting provider began a wide search for dark web monitoring solutions, finding that Flare's platform included information gathered from illicit Telegram channels. Since compromised user data sold on Telegram was the catalyst for the process, the security team moved forward with Flare's free trial.

Within a matter of a few minutes, the security team gained insights from the depth of information available through Flare's platform. During the trial period, the team shared the insights internally and quickly began envisioning different ways to leverage Flare's functionalities.

As a web hosting provider, the company has hundreds of thousands of domains and hosts to monitor. Despite being concerned about a potential flood of information, the security team was able to fine-tune identifiers within a few weeks so it could focus on the 100 that would provide the most relevant information. With a wealth of information at their fingertips, the security team was able to inspire the legal department and other internal stakeholders to move forward.

Despite considering other tools, they determined that Flare was the best fit for their needs and moved to a paid subscription within a month of its initial valuation because the platform offered a depth and breadth of data while remaining cost effective.

> "Flare saves us tremendous time by centralizing the information that we need to see across dark web markets and hacker forums. It has saved us countless hours in remediation time because we now know immediately when data is being passed around and can be proactive... My advice to anyone who's evaluating Flare? Just get it."
>
> — Head of Security, Web Hosting Company

Benefits: “A More Complete Vision of the Past to Help Guide the Future”

Our customer gained immediate value by using Flare as a central source of intelligence for attacker conduct. By integrating Flare alerts into Slack, they now have access to real-time notifications within their existing workflows and are able to take immediate action.

Flare’s automation reduced search times from 20-30 minutes down to 5 minutes, which is an 80% decrease. The security team sees tangible improvements in their ability to identify and act on leaked credentials, dark web conversations about the company, and engage in searches related to vendors and executives.

With Flare’s easy-to-understand reporting capabilities, the web hosting provider’s security team can reach a wider audience. Internally, leadership has an additional layer of confidence and insight as Flare’s platform transforms hypothetical scenarios into real threats based on data.

Researching vendors has provided additional benefits beyond just third-party risk management. Today, the organization can go vendor-supplied security questionnaires and point-in-time audits to gain insight into security posture based on data available across the cybercriminal ecosystem. This visibility enables the organization to make informed decisions about security and be more judicious in their negotiations with certain partners, offering a business-level benefit beyond securing their own systems.

As the web hosting company looks to its future with Flare, it plans to incorporate more automation specifically around identifying and managing compromised customer logins to improve everyone’s security across internal and external users.