sumologic

Sumo Logic Solidifies Trust in Threat Intelligence Insights with Accurate IP Geolocation Data from Neustar

> "As we continue to scale our business, having accurate geolocation data is crucial for helping Sumo Logic's existing and future customers maintain continued confidence in their threat intelligence insights."
>
> – **Brian Bozzello,**
> Senior Product Manager
> at Sumo Logic

The Challenge

As a leading cloud-native multi-tenant machine data analytics platform, a critical function of Sumo Logic's core business includes ingesting, searching and analyzing nearly 100 petabytes of log and event data per day and 10s of millions of needles of insight in a global haystack of ever-changing data. The ability to provide accurate real-time threat intelligence is a prime use case of Sumo's cloud-native service.

In today's digitally connected, online world, all of this data comes from different networks, individual users and machines, and eventually all of these elements begin to talk to one another in the form of IP addresses to create a seamless user experience. IP addresses are similar to complicated cellphone numbers, meaning they can be registered in one place, used in another and then re-assigned to someone else without much notice. Keeping track of this is an enormous task. And over time, malicious actors figured out they could take advantage of this to not only mask their true location, but also create false security alerts to distract security teams from identifying and prioritizing legitimate high-risk threats.

While a multitude of weighted indicators can trigger a threat alert, one of the most useful inputs for Sumo Logic's machine data analytics platform is IP geolocation data. This data identifies the physical location of an object linked to the internet. For Sumo Logic, geolocation is a primary tool for detecting suspicious logins, maintaining regulatory compliance and analyzing end-user behavior.

If the reliability of that geolocation data is questionable, all Sumo Logic customers will be faced with a higher level of risk. Accuracy is also important for purposes of compliance, such as the new mandates in the General Data Protection Regulation (GDPR) for personal data of people in the EU. For instance, organizations need to know if they are interacting with and collecting data from a user in the EU because under EU law, that data needs to be treated differently than non-EU individuals, or else the organization could face potential fines.

"Accuracy of geolocation data is crucial for our business," says Brian Bozzello, Senior Product Manager at Sumo Logic. "It affects the integrity of our service and quality of our platform." Accuracy is also important for gathering analytics on trends and market performance as well as for ensuring security across the full application stack. "Our enterprise customers depend on Sumo Logic for mission-critical security and operational insights, and quality IP geolocation is a key part of the platform to help deliver that intelligence."

The Neustar Solution

Sumo Logic evaluated three vendor alternatives before choosing Neustar UltraGeoPoint, the authoritative source of IP geolocation decisioning data. After passing a proof-of-concept phase, Bozzello says his team did some accuracy testing and dug into the methodologies used by each vendor.

"We submitted tens of thousands of IP addresses to each vendor for the evaluation," says Bozzello. "It's hard to have a `truth set' of data, so we compared results from all three vendors and analyzed the discrepancies." For example, if logins from two countries resolved to one IP address, the vendor was asked to respond with more detail.

"Neustar's responses were long, well thought out explanations of the results," says Bozzello. "The other two vendors provided short, incomplete comments, such as, `You won't get that very often because it's an odd case.'" Responses like that were not what the team wanted to hear. "We needed confidence to know the locations were accurate," he says, noting that of all the results, there were just a few percentage points of discrepancies reflecting differences between the vendors. "But it's those outliers where we need to have confidence that the location data is accurate," Bozzello says. "Confidence is critical."

Country-level geolocation accuracy was the primary focus of Sumo Logic. UltraGeoPoint includes more granular location options such as region, state, city, and postal code. Network characteristics with UltraGeoPoint may include connection type, line speed, IP routing type, ownership and others.

In addition to accuracy, Bozzello says Neustar's company size, its internal resources and industry reputation helped cement the decision to go with UltraGeoPoint.

Learn More Today

www.security.neustar

PHONE

France: 0800-909-776
Germany: 0800-182-8063
UAE: 800-0357-03762
UK: +44-(0)-1784-448-444
US: +1-855-898-0036
Australia: +61-3-9866-3710

EMAIL

APAC: APACSec@neustar.biz
EMEA: Euroinfo@neustar.biz
North America/other:
NASec@neustar.biz

The Outcome

After implementing Neustar UltraGeoPoint's decisioning data, Bozzello says there were significantly fewer customer inquiries related to IP geolocation data. "The technology worked as intended, which is great because wasting time on false-positive alerts is something customers hate," Bozzello says. "It makes them feel blind to security issues – especially not knowing what they don't know."

With Neustar UltraGeoPoint, Sumo Logic's customers now have confidence that if a California-based user logs in with correct credentials, but the IP is physically located in Egypt, they can have higher confidence that the alert is valid. "Neustar lets us identify obvious anomalies like that and have high confidence in the results," Bozzello says.

Using Neustar UltraGeoPoint data is a solid investment in Sumo Logic's platform and contributes to great customer experience as the company grows. "As we continue to scale our business, having accurate geolocation data is crucial for Sumo Logic's existing and future customers to maintain continued confidence in their threat intelligence insights. Neustar's accurate IP geolocation data also helps us gain an edge over the competition." Bozzello says.

Moving forward, Sumo Logic plans to incorporate Neustar decisioning data in additional offerings. "We're making big investments in our security analytics services," Bozzello says. "Neustar's data will help us continue to enhance our products by offering new features and services that remain focused on delivering accurate, secure, and fast continuous intelligence needed to help our customers meet their operational and security needs."