MICRO FOCUS | VERTICA

Customer Success Story

Big Data & Analytics

HPE & Lancope

HPE improves network security with Vertica and Lancope solution.

Overview

Lancope StealthWatch, a network monitoring tool that leverages the Vertica Analytics Platform, provides Hewlett Packard Enterprise's network security team with a cost-effective, yet powerful, way to monitor and analyze HPE's network traffic.

Challenge

One of the challenges of securing an IT infrastructure is the sheer volume of the data generated by its subsystems.

Take HPE's global network, for example. The network comprises around 16,000 switches and 10,000 routers, and connects some 300,000 users working from 600 sites—plus uncountable remote connections—worldwide. And the network is constantly humming with activity—which means HPE's network is constantly generating data. In aggregate, the network generates some 150,000 data flows per second, each of which represents another discrete subset of data: records of IP packets and the time intervals associated with those packets.

The vast majority of that data, of course, represents benevolent network traffic. But not all of it is benign: a network security expert would certainly find, entwined within those flows, evidence of unwanted activity—malware, perhaps, or malicious behavior, or unsanctioned uses of network resources.

The question is: how to detect evidence of malicious traffic, given that it is buried within an around-the-clock tsunami of mostly innocuous data?

And to make the issue even more challenging, the evidence has to be uncovered quickly. "Consider a scenario in which a worm penetrates the network," explains Gaddiel Torres, network security architect, HPE. "We have to move fast if we want to contain it before it impacts too many network resources."

"The Vertica Analytics Platform is an integral component of Lancope StealthWatch because it enables the tool to handle the enormous volume of data it collects. Vertica's analytical capabilities and fast query speeds help ensure we detect network security issues as quickly as possible."

GADDIEL TORRES
Network Security Architect
Hewlett Packard Enterprise

Hewlett Packard Enterprise

Lancope
Network Performance + Security Monitoring™

At a Glance

- **Industry**
  Software & Technology
- **Location**
  United States
- **Challenge**
  Improve ability to detect anomalous activity within enormously complex, global network.
- **Products and Services**
  Vertica
- **Results**
  + Minimized potential damage by allowing security teams to act more quickly
  + Introduced the use of already-installed network devices to perform data collection, minimizing monitoring costs

It's a task that requires highly powerful analytics capabilities—which is why HPE has implemented Lancope StealthWatch, a network traffic analyzer that in turn leverages the Vertica Analytics Platform, a big data solution from HPE's own software portfolio.

Solution

HPE's three-pronged approach to online security—prevention, detection, and response—relies on a range of tactics. To address prevention, the company continually reinforces its systems against security vulnerabilities. To support detection and response, it uses intrusion protection technology, including HPE Tipping Point and HPE ArcSight HPE, the company's Security Incident Event Management (SIEM) solution.

Lancope StealthWatch complements these other elements of HPE's cyber security framework by providing network-based anomaly detection.

Lancope's first task is to collect network data, including NetFlow, sFlow, JFlow, IPFix, and netStream flows. The tool uses already installed network devices to perform data collection; this minimizes the cost of network monitoring because additional instruments don't need to be added to the network. "With some of the other network monitoring tools we've tried, we had to deploy excessive amounts of specialized hardware," Torres says. "With Lancope we don't need extra hardware to get a comprehensive, scalable view of network activity."

As the data is collected, it's sent to the tool's analytics engine, which is built on an embedded version of the Vertica Analytics Platform software. There, the flows are analyzed for indications of malicious or anomalous behavior, including attempted malware intrusions, misuse of network resources, or distributed denial-of-service (DDOS) attacks.

Vertica's powerful analytics capabilities are crucial to the tool's effectiveness. Lancope's monitoring of network flows is constant; the volume of data it gathers is enormous. The Vertica Analytics Platform software, however, is designed to manage large, fast-growing volumes of data. Lancope chose the Vertica Analytics Platform software because it can easily handle the data Lancope collects.

In addition, Vertica supports very fast query performance. HPE's network security team, therefore, doesn't experience long lags when they use the Lancope dashboard to load and query data. "We can easily view the last 5 to 10 minutes of flow data, because it's constantly being refreshed and because queries run so quickly," O'Shea notes.

Data can be viewed in detailed or summarized form, or in graphical format.

The Vertica Analytics Platform also provides built-in capabilities such as automated deduplication. This is critical for monitoring network flows, because the same data often passes through multiple routers. Deduplication reduces the total amount of data stored, and thereby simplifies its management and—over time—associated data storage costs.

If the Lancope system detects events that appear anomalous or malicious, it sends alerts to the other technologies HPE has deployed to help respond to computer threats, including HPE ArcSight and HPE Tipping Point. Within these solutions, data gathered by Lancope is correlated with other infrastructure data to provide additional insight into infrastructure events, and to provide HPE's Global Security Operations Center with the actionable information they need to respond to events.

"With an infrastructure as big and complex as ours, we need a broader approach than can be achieved with individual tools," Torres notes. "Integrating Lancope with HPE security solutions such as HPE ArcSight and HPE Tipping Point is consistent with the kind of comprehensive cyber coverage that modern global enterprises require. It helps ensure we have a complete picture of our infrastructure, and reduces the risk that we'll miss critical events."

The combination of continual network flow monitoring and analytics—provided by Lancope and the Vertica Analytics Platform—and the monitoring and intrusion protection capabilities offered by HPE ArcSight and HPE Tipping Point, help ensure that the HPE Cyber Security team can respond to events quickly and effectively. "The goal is to catch any potential threat early, so that we can respond appropriately," says Torres. "HPE Lancope provides functionality critical to meeting that goal."

Results

While the main reason HPE implemented Lancope was to provide detection of events as they occur, over time the solution will strengthen the company's cyber security capabilities in other ways.

For example, the Vertica Analytics Platform's capabilities can also be used to help HPE tell if its IT resources are being used in ways that are not authorized or permitted. Unusual network activity or connections might indicate that corporate resources are being used to host unauthorized websites, for example.

HPE can use the solution to help it with forensics. Because the tool's data analytics engine both stores and analyzes enormous amounts of data, HPE's network security team can use it to parse historic network activity. Over time, this will help HPE better understand what constitutes "normal" network behavior—which will in turn sharpen its ability to detect abnormal events. "The more history we have, the more we understand how our infrastructure components 'naturally' behave," says Torres.

> **"At the time when the platform was being chosen, it was impossible to predict the number of data sources, the volume of data, the rate at which information would be received, the tasks to be solved or the approaches to solving them."**
>
> **NIKOLAY GOLOV**
> Corporate Data Storage Architect
> Avito

Contact us at:
www.vertica.com

Analyzing historic data can also help HPE gain new insight into malware and the techniques hackers use when they try to breach corporate defenses.

Another benefit of the technology is that it helps HPE's network security team better understand how application eco-systems and networks interact and communicate. In the past, it was sometimes challenging for the company's network experts to collaborate with applications developers. "Developers might not understand the protocols of the network ecosystem, or how to share relevant information with the network team," Torres explains.

But by using the data amassed by the Vertica Analytics Platform, plus the analytics capabilities the solution provides, the network team can gain direct insight into how its protocols affect applications. "It's helping guide us as we design network protocols," says Torres. "We're more confident that we can build firewalls that won't break the applications they're supposed to protect."

And finally, HPE can potentially leverage the solution to help other HPE IT professionals with tasks that aren't necessarily security related. The data analytics provided by the Vertica Analytics Platform could, for example, be used to map how applications services are being consumed on an enterprise basis. This could help HPE more effectively allocate resources, which could in turn improve application performance and reduce costs.

"Network-based anomaly detection is a critical component of any enterprise cyber security framework," Torres concludes. "Lancope fits our needs. It is cost-efficient and it supports powerful analytics, thanks to the Vertica Analytics Platform. Plus, it supports integration with our other intrusion detection platforms. Lancope has proven to be a very effective addition to our cyber security arsenal."

VERTICA | MICRO FOCUS®