Case study

HP improves its network security with an HP Vertica and Lancope solution

Lancope StealthWatch combines round-the-clock network flow monitoring with the HP Vertica Analytics Platform

Industry
Information technology

Objective
Improve ability to detect anomalous activity within enormously complex, global network

Approach
Implement solution that quickly detects anomalies by continually monitoring network flows and performing fast, powerful analytics on flow data

IT matters
- Able to monitor and quickly analyze network's 600,000 flows/second, providing comprehensive actionable information on network activity

Business matters
- Fast detection of abnormal events helps minimize potential damage by allowing security teams to act more quickly
- Solution uses already-installed network devices to perform data collection, minimizing monitoring costs

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

Jim O'Shea, network security architect, HP

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

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

Take HP'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 HP's network is constantly generating data. In aggregate, the network generates some 600,000 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 Jim O'Shea, network security architect, HP. "We have to move fast if we want to contain it before it impacts too many network resources."

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

Network anomaly detection essential to HP's security approach

HP'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 HP Tipping Point and HP ArcSight HP, the company's Security Incident Event Management (SIEM) solution.

Lancope StealthWatch complements these other elements of HP'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," O'Shea 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 HP 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.

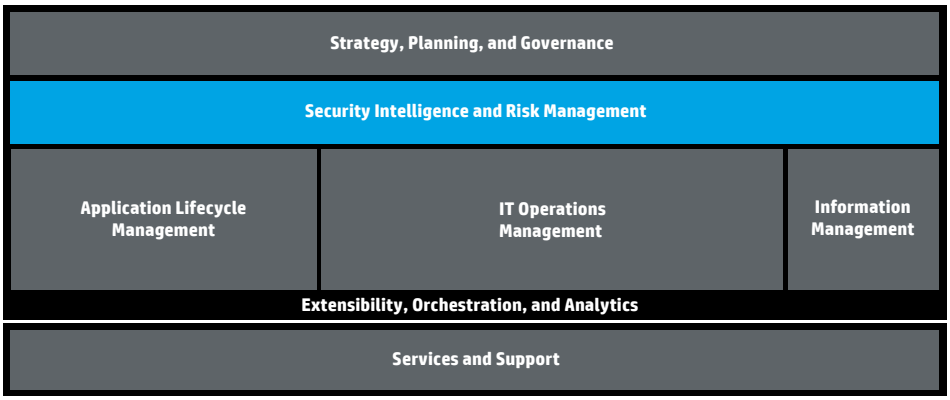
HP Vertica's powerful analytics capabilities are crucial to the tool's effectiveness. Lancope's monitoring of network flows is constant; the volume of data it gathers is enormous. The HP Vertica Analytics Platform software, however, is designed to manage large, fast-growing volumes of data. Lancope chose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

In addition, HP Vertica supports very fast query performance. HP'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 HP 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

HP IT Performance Suite solutions



Monitor HP network's 600,000 flows per second

of data stored, and thereby simplifies its management and—over time— associated data storage costs.

Integrated solutions support security framework

If the Lancope system detects events that appear anomalous or malicious, it sends alerts to the other technologies HP has deployed to help respond to computer threats, including HP ArcSight and HP 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 HP'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," O'Shea notes. "Integrating Lancope with HP security solutions such as HP ArcSight and HP 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 HP Vertica Analytics Platform—and the monitoring and intrusion protection capabilities offered by HP ArcSight and HP Tipping Point, help ensure that the HP 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 O'Shea. "HP Lancope provides functionality critical to meeting that goal."

Forensics, history support continual improvement

While the main reason HP 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 HP Vertica Analytics Platform's capabilities can also be used to help HP 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.

HP can use the solution to help it with forensics. Because the tool's data analytics engine both stores and analyzes enormous amounts of data, HP's network security team can use it to parse historic network activity. Over time, this will help HP 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 O'Shea.

Analyzing historic data can also help HP 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 HP'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," O'Shea explains.

But by using the data amassed by the HP 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 O'Shea. "We're more confident that we can build firewalls that won't break the applications they're supposed to protect."

And finally, HP can potentially leverage the solution to help other HP IT professionals with tasks that aren't necessarily security-related. The data analytics provided by the HP Vertica Analytics Platform could, for example, be used to map how applications services are being consumed on an enterprise basis. This could help HP 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," O'Shea concludes. "Lancope fits our needs. It is cost-efficient and it supports powerful analytics, thanks to the HP 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."

Customer at a glance

Application
Network security

Software
HP IT Performance Suite—Security Intelligence and Risk Management

- HP Vertica Analytics Platform software

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA3-8816ENW, November 2012