Cisco Stealthwatch and SIEM Optimization

Save time and money by integrating Stealthwatch with your SIEM deployment

Introduction: Stealthwatch & SIEMs

What is Stealthwatch?

Cisco Stealthwatch provides enterprise-wide visibility and can help you gain greater insight into the activities that occur on your network. Stealthwatch applies advanced security analytics to detect and respond to threats in real-time, and continuously analyzes network activity to create a baseline of normal network behavior. It can help you identify behaviors related to zero-day malware, insider threats, Advanced Persistent Threats (APTs), Distributed Denial of Service (DDoS) attempts, and other attack types before they have a chance to wreak havoc on your network. Unlike other security monitoring solutions, Stealthwatch not only monitors traffic going in and out of the network but also lateral, or east-west traffic inside the network to identify network abuse and potential insider threats.

Stealthwatch offers different deployment models - on-premises as a hardware appliance or a virtual machine called Stealthwatch Enterprise. Or cloud-delivered as a SaaS solution called Stealthwatch Cloud.

The core components that make up Stealthwatch Enterprise are the Flow Collector & Management Console; Flow Sensors and other components are optional depending on the topology and infrastructure monitored. Together, these components provide a unique view and analysis of network traffic and can improve real-time threat detection, incident response and network performance and capacity planning.

Table of Contents

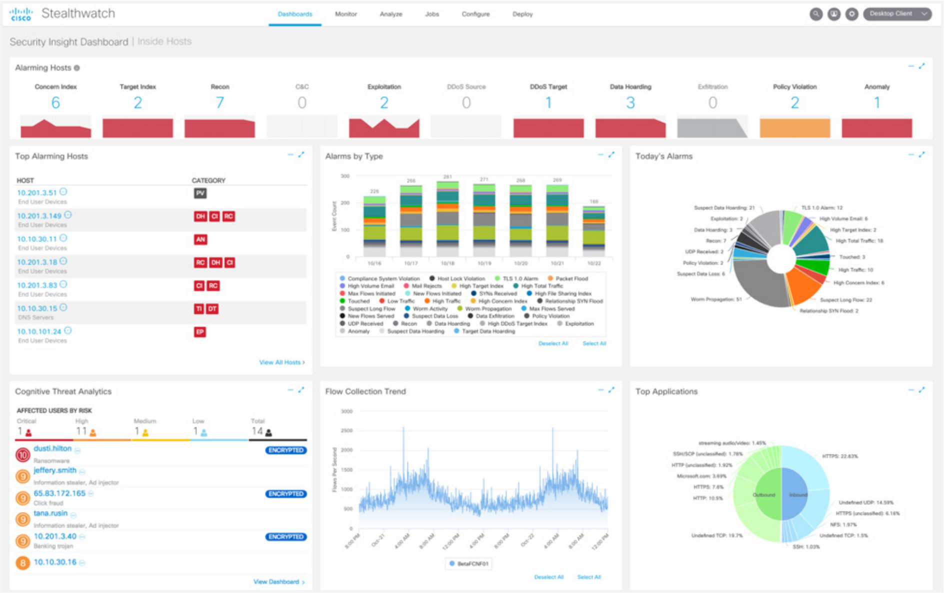

Figure 1: Stealthwatch Enterprise Dashboard

And what about SIEMs?

One might wonder about the value of a solution like Stealthwatch when a resident Security Information and Event Management (SIEM) is already deployed within the organization. The truth is that Stealthwatch complements your SIEM deployment. SIEM technology tracks syslog from network assets, and issues alerts and alarms from signature-based tools. Stealthwatch looks at traffic meta data such as NetFlow or IPFIX for the complete picture and is able to identify behavior-based anomalies. It applies analytics to reduce a large amount of security events to few critical alerts so that your security team doesn't have to manually sift through all that data. Stealthwatch can also be configured to integrate with a SIEM to send alerts and other information so that customers can choose the environment they would like to use for advanced threat detection and response.

In addition to reducing the time spent detecting and investigating a threat from months to hours, there's another benefit that customers with a Stealthwatch and SIEM integration have experienced. And it's related to the optimization of the data sent to the SIEM.

Let's say your network is generating telemetry at an average rate of 1TB per day with an annual license. Sending the data directly to a SIEM may cost you on average $600K per year with most of this data both unprocessed and duplicative. If you were to place Stealthwatch into this telemetry stream, you would see an approximate flow reduction of 80% – reducing the cost in this example from $600K to just $99K! While your results may vary, the mathematics still holds; the larger your flow production, the higher the value you stand to save.

Stealthwatch can save on data costs while also providing top tier visibility, security analytics and threat detection.

The Problem

SIEM systems have become increasingly vital to modern security architectures. As a vast and often literal wealth of data enters and leaves an organization, SIEMs help provide context and insight into how data is being accessed and shared. However, selecting a SIEM provider isn't always a simple task. As the sheer amount of data you must use for security monitoring continues to grow, so too can operating costs for SIEMs that charge by data volume. Furthermore, some data can traverse multiple points in your network in quick succession, leading to unnecessary duplicate data costs in the long term. If you are going to pay for data, you certainly don't want to pay for it multiple times unnecessarily.

The Solution

Stealthwatch's major advantage is its ability to reduce the data sets without any information loss. Stealthwatch knows which data is redundant and, at the time of collection, provides the de-duplication and stitching of data necessary to deliver all the information with the least amount of data. As the Stealthwatch Flow Collector receives and collects telemetry data from various proxy sources (routers, switches, firewalls, endpoints and other network infrastructure devices), it performs de-duplication so that any flows that might have traversed more than one of those sources is only counted once. It then stitches the flow data together for full visibility of a network transaction. This results in cost-effective telemetry monitoring and storage for even the largest, most complex enterprise networks.

Instead of paying a SIEM by data volume and running the risk of paying for duplicate data, Stealthwatch can save on data costs while also providing top tier visibility, security analytics and threat detection.

The Science

While NetFlow and IPFIX telemetry volumes will vary across an enterprise network, there are some characteristics and estimates we can use to model sizes and by extension, overall costs. The first thing we know is that depending on the hop-counts it takes to travel the network, telemetry is generated, which describes said communication. For example, an average client-to-server session will cross 5 to 6 hops – maybe more, maybe less. Each of the routers or switches crossed will export a record that summarizes all the observable metadata from the session and only in one direction (unidirectionally).

As multiple sessions are taking place across these routers, switches, firewalls, etc., telemetry related to these sessions is aggregated and exported every 60 seconds. If you were to send a TB/day of all this vital telemetry directly to a SIEM charging you a rate of $600K with an annual license, or $1.8m annually with a perpetual license, this level of visibility can quickly become expensive. Stealthwatch can sit between all of these telemetry exporters and your SIEM, providing cost savings without compromising visibility.

Stealthwatch is able to reduce the volume of flows being sent to a SIEM by as much as 80% for huge savings on SIEM data storage costs.

Scenario 1 - Stealthwatch data optimization

In this example, the SIEM (or homegrown data lake) still requires network telemetry for a ledger of activity used in its own analytics. Stealthwatch will take care of the stitching (synthesizing various telemetry sets) and de-duplication (discarding duplicate records upon collection) gaining you more fidelity at less data volumes. This is on average a 6:1 reduction, which is 83.5% less flows*!

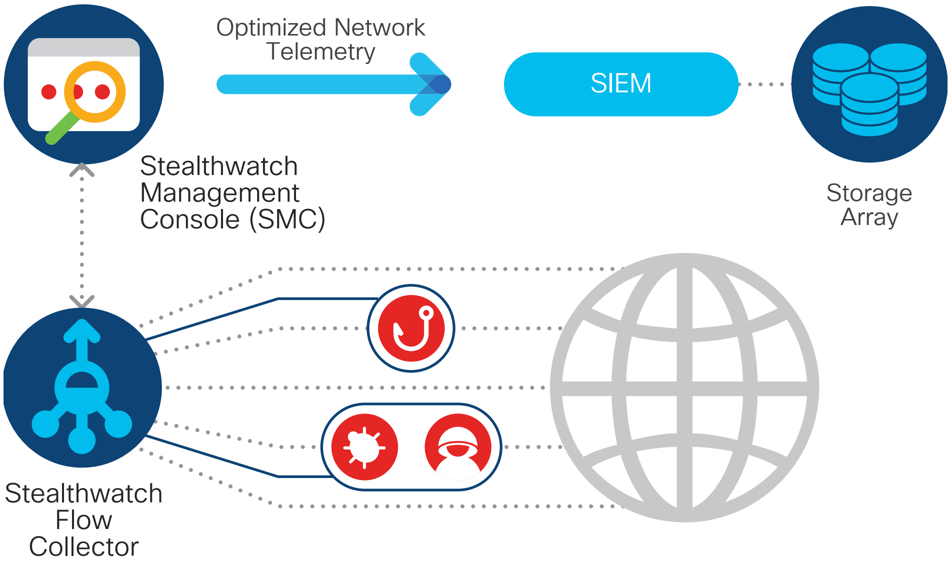
Optimized Network Telemetry
SIEM
Stealthwatch Management Console (SMC)
Storage Array
Stealthwatch Flow Collector

Figure 2: Stealthwatch Enterprise inline to reduce telemetry costs

Here, the user still wishes to get network flow telemetry into their SIEM but without the duplicity. As SIEM vendors generally charge for data storage, the reduction mentioned above would mean saving tens of thousands of dollars per year for data that was by its very nature, redundant.

* 83.5% reduction metric is based on measurements seen in an actual customer deployment. De-duplication and reduction of flows could vary between different environments based on the collection strategy that results in two separate telemetry exporters seeing the same traffic. This depends on the deployment, location and number of exporters, etc.

To learn more, visit https://www.cisco.com/go/stealthwatch or contact your local Cisco account representative.

If you are an existing Stealthwatch customer, check out the Stealthwatch Security Information Event Management (SIEM) Integration Service.

Scenario 2 – Stealthwatch security analytics alerts

There is also a scenario whereby Stealthwatch is the collector and retainer of all network activity, only alerting the SIEM with the analytical outcomes (threats detected), thus allowing the SIEM user to pivot back into Stealthwatch for deeper investigation. Here, the Stealthwatch APIs are used to turn Stealthwatch into a service fully integrated with the SIEM because Stealthwatch provides both the behavioral analytics and the general ledger to the network activities. Some of the largest enterprises choose this kind of deployment because of a huge volume of network telemetry that is difficult to analyze by security teams within a SIEM environment.

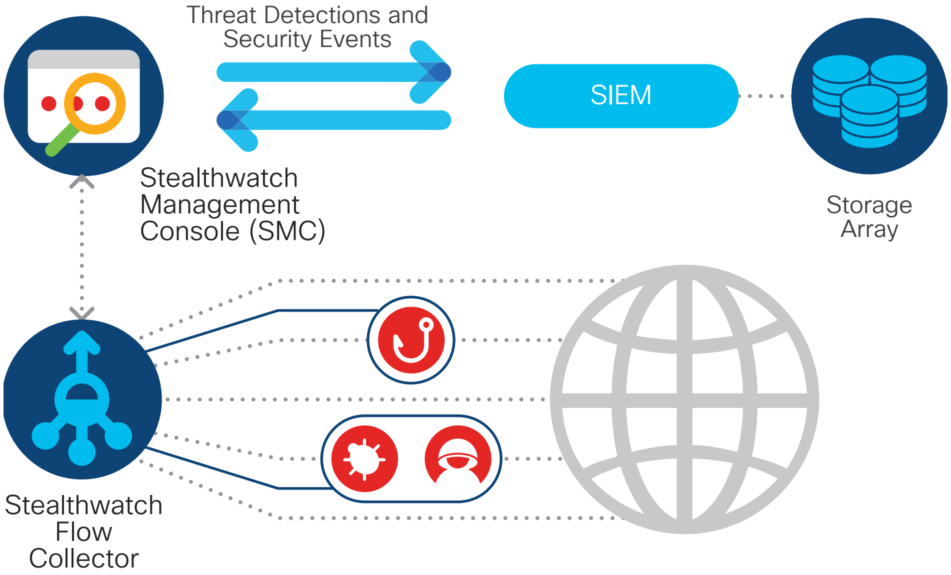
Threat Detections and Security Events
SIEM
Stealthwatch Management Console (SMC)
Storage Array
Stealthwatch Flow Collector

Figure 3: Stealthwatch Enterprise as a general ledger of network activity and tightly integrated with a SIEM

Conclusion

The mountain of data your organization now uses for security monitoring is only going to continue to grow in the years to come. Fortunately, you don’t have to pay a SIEM by data volume and thus risk paying for duplicate data. Cisco Stealthwatch has the ability to reduce your data sets without any information loss via de-duplication and stitching, providing you with all the information you need with the least amount of data. Not only can Stealthwatch help you reduce data flows by approximately 80%, it also provides you with top tier visibility, security analytics and threat detection.

References

Mathematics – based on major SIEM vendor tariffs:

100 GB / Day = $60,000 / GB Annually or $180,000 / GB Perpetual
1 TB / Day = $600,000 / TB Annually or $1,800,000 / TB Perpetual