At-a-Glance

Cisco Stealthwatch and the Cisco Secure Data Center

Increased Visibility of Data Center Threats for Accelerated Time to Remediation

Today the success of your organization may depend on effectively safeguarding the resources and information in your data center. Data center operators are challenged with continually adjusting traffic-flow volumes and infrastructure to meet the needs and expectations of the business while complying with all necessary security regulations. A major element in the most successful data center threat defense strategies is clear visibility into traffic flows. And that's exactly what you'll get with the Cisco Stealthwatch® and Cisco® Secure Data Center Solution.

Stealthwatch works with Secure Data Center Solution components–including Cisco NetFlow, Cisco Adaptive Security Appliances, the Cisco Identity Services Engine, and Cisco TrustSec® technology–to take advantage of network segmentation and user context. The result? Much better visibility into data center traffic for a much-improved threat defense posture.

The solution gathers NetFlow data from the Secure Data Center infrastructure along with flow sensors, if needed. All of the data is then sent to Cisco's Flow Collector platform, which analyzes the data for signs of threats propagating inside the network. The Stealthwatch console then displays the data along with any alerts about suspicious activity. Stealthwatch is also able to read Cisco TrustSec security group tags for better correlation of traffic segmentation data and to share its flow data with the Identity Services Engine to respond to a threat and to quarantine suspicious activity. This helps enable better planning and security policy, the detection of advanced threats, and the ability to investigate and perform postmortem activities when a breach has occurred.

Next Steps

Visit http://www.cisco.com/go/designzonesecuredc for more information, including the Cisco Validated Design for Cisco Stealthwatch and the Cisco Secure Data Center.

Benefits

- Gain visibility into system traffic flows from the network edge to the data center, including virtual machines, to expose potential attacks from all threat vectors
- Detect a wide range of data center issues, from malicious insiders attempting to exfiltrate sensitive data to malware spreading internally from host to host
- Improve incident response, forensics, and compliance with a comprehensive view of network activity

"With the Stealthwatch System, we have been able to find issues in our data centers that we would have otherwise missed, several of which were quite critical."

Henrik Strom
Head of IT security and the CERT at Telenor Norway

C45-736266-01 08/16