Network Security Management means fully understanding what your traffic is actually telling you

What is happening on the network? That’s exactly what the Continuous Diagnostics and Mitigation (CDM) Program seeks to answer. CISA highlights the importance of analyzing data in transit, including user behavior and activities, through its Network Security Management capability. After all, there’s little to mitigate unless you’ve diagnosed a serious problem. And network telemetry is a critical source of network behavioral insight.

Stealthwatch knows what’s happening. It delivers scalable network visibility and security analytics across your agency so that you can detect and diagnose advanced threats in real time. And it’s the only solution that does this consistently across your agency’s network, public clouds, and even through encrypted traffic. So read on.
CDM is about visibility and risk mitigation

The CDM Program automates controls and progress reporting through five key capabilities:

- Data Protection Management asks “How is data protected?”
- Network Security Management asks “What is happening on the network?”
- Identity and Access Management asks “Who is on the network?”
- Asset Management asks “What is on the network?”
- CDM Agency and Federal dashboards collect aggregate and convey critical information from CDM technologies at both the agency and federal levels.

CDM is much more than basic FISMA compliance
Getting your agency’s CDM approach aligned with Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) guidelines definitely helps you meet compliance. And, in general, CDM can help accelerate deployment times and streamline processes because it enables you to use advanced commercial off-the-shelf tools. Those by themselves are excellent benefits, so it’s easy to think that’s the extent of the CDM Program’s value. But the truth is, CDM is about more than compliance.

When it comes to selecting the right CDM approach for your agency, not all DHS approved solutions are equal. You can now add even more value by leveraging integrated, threat-driven security via a variety of simple, open, and automated solutions. And best of all, you may be able to do so using much of your existing infrastructure.

CDM demands integrated, threat-driven security
The Internet of Things (IoT) is here to stay, and with the ongoing federal move to the cloud, it is becoming the key method of connectivity for millions of end users and their devices. As a result, security can be complex.

Securing this flood of IoT data is probably the biggest challenge facing government today. To address this, the government needs integrated and secured networks that can scale with the explosion of data, devices and sensors. This means moving beyond prevention, detection, and response to deploy predictive, proactive capabilities. It requires continuous visibility and validation that’s fully integrated at every level. It’s about working continually to model behaviors that signal red flags on your network.

Continuous Monitoring applies to remote workers too
Even though more people are working outside the office, you still need to monitor and control their access. Stealthwatch continuously monitors remote user activity and spots policy violations even when network traffic is encrypted. It pinpoints suspicious behavior that often indicates a larger security incident. Learn more about Stealthwatch secures your remote user in our solution overview.

Stealthwatch is aligned to the kill chain
From reconnaissance through exfiltration -- to help you:

- Analyze network telemetry and detect anomalies
- Minimize time to detection of security incidents
- Build a complete ledger of your network by automatically stitching flow records together
- Create complete conversational records for every session across your network

That’s why Stealthwatch delivers complete visibility of your agency’s network environment

© 2020 Cisco and/or its affiliates. All rights reserved.
The challenges of encrypted traffic security

Many organizations today cannot detect malicious content in encrypted traffic. They lack the security tools and resources to implement a solution that can be deployed throughout their network infrastructure without slowing down the network.

Decrypting network traffic is often impractical.

Traditional threat inspection through bulk decryption, analysis, and re-encryption is difficult because it requires powerful, expensive resources. Plus it compromises privacy and data integrity.

On any given day, few know how much of their digital mission is in the clear versus encrypted.

If traffic is encrypted, the encryption is typically done to meet compliance requirements that mandate specific security policies.

How Stealthwatch detects advanced threats in real time

There are five main elements part of Stealthwatch Security Analytics that provide the ability to detect advanced threats in real time:

1. **Data collection.** Your network already generates rich telemetry about what’s happening on your network. But the volume is astronomical, making it extremely difficult to understand what your network is actually telling you. That’s why Stealthwatch gathers all network telemetry: to become the “general ledger” of your network for complete accounts of who, what, where, when, and how everything is behaving over time. It also collects metadata from Cisco Identity Services Engine, Cisco AnyConnect, and other solutions to apply user and application context to network behavioral analytics.

2. **Behavioral modeling.** Stealthwatch closely monitors the activity of every device on your network and develops baselines of normal behavior. It understands and spots bad behavior by applying nearly 100 different Security Events or heuristics that scrutinize many types of traffic behavior.

3. **Multilayered machine learning.** Stealthwatch also applies machine learning, both supervised and unsupervised, to discover advanced threats and malicious communications. It integrates with a cloud-based, multi-stage machine learning analytics pipeline to correlate threat behaviors observed in your environment with those seen globally.

4. **Global Threat Intelligence.** A global threat intelligence feed powered by the industry-leading threat intelligence group, Cisco Talos, provides an additional layer of protection against botnets and other sophisticated attacks. It correlates suspicious activity in the local network environment with data on thousands of known command-and-control servers and campaigns, to provide high fidelity detection and faster threat response.

5. **Encrypted Traffic Analytics.** Stealthwatch is the only solution that can analyze encrypted traffic without requiring decryption. It applies enhanced telemetry and advanced analytics to detect malware that would otherwise remain disguised in encrypted traffic. It also ensures that your encrypted traffic stays encrypted in compliance with your cryptography standards.
Network visibility is essential for CDM

Security is about efficiently and effectively managing risk, and applying security policy and controls based on it. You need an architectural approach to have that type of enforcement. And that’s why Stealthwatch provides essential visibility for the CDM Program and beyond.

As your agency adopts new practices and technologies, you need a way to know what’s normal on your network and what’s not. With multiple locations, roaming users, cloud and storage added to traditional networks and data centers, visibility into all parts of the business’s environment is paramount.

This visibility includes knowing every host: seeing who is accessing which information at any given point. It also requires recording conversations and the exchange of data between individual hosts. And from there, you must also know what’s considered normal behavior for a particular user or “host” and establish baselines. Then you need to know when behaviors change the instant it happens.

“Stealthwatch uniquely bridges the east-west requirements of CDM, with the north-south mission of Trusted Internet Connections 3.0 and the move to Zero Trust”

Doug Cowan,
Director of Federal Cisco Security Sales

Bottom line: Stealthwatch is total network visibility

Your agency needs visibility into your entire network infrastructure to be able to take action quickly in order to minimize the impact of a threat on critical information. You need a solution that enables your CDM program, provides continuous FISMA compliance, and improves your overall cybersecurity profile.

Cisco Stealthwatch delivers