Solving the Visibility Gap

Securing Your Network with the Cisco Stealthwatch Online Visibility Assessment
As networks grow larger and more complex, organizations struggle to protect themselves from increasingly sophisticated threat actors. Attacks often go undetected or unreported for months. To detect and mitigate security risks, you need to be able to see what is taking place on your networks.

To help you achieve that goal, we are offering the Cisco Stealthwatch™ Online Visibility Assessment. It is designed to evaluate your internal network visibility and overall security posture.

As networking continues to evolve with trends such as mobility, the Internet of Things, and the cloud, gaining visibility is crucial to protecting your assets from advanced threats. This insight into attackers’ behaviors and location within your environment can help you prevent a security event from becoming a full-blown data breach.

What You Will Learn

The Stealthwatch Online Visibility Assessment evaluates six primary criteria associated with malicious activities or security risks. This white paper covers:

- Six critical areas that you need visibility into
- How Cisco Stealthwatch can help you monitor these areas
- How NetFlow can provide end-to-end network visibility

Internal Monitored Network

Internal visibility is vital to understanding the state of your network. Cisco Stealthwatch technology continuously monitors and protects internal assets, observes data transferred between servers and the Internet, and processes traffic flows. These metrics and others help security and network personnel quantify the hosts, systems, and resources on your network so they can make sure there is nothing present that they don’t know about. This information can also be used to identify critical assets, validate policies, audit and demonstrate compliance, and help you make better decisions based on data.

The Stealthwatch Online Visibility Assessment determines the number of active hosts, the amount of traffic, and the maximum number of flows per second occurring on your network. In addition, it can estimate how much storage you will need to retain historical flow information.

Server Message Block Risk

Some threats use the Server Message Block (SMB) protocol to gain control of hosts. Because the protocol is used in many organizations, attackers can use it to mask signs of malicious activity.

Most notably, the ransomware WannaCry and Nyetya and the worm Conficker utilized SMB-based vulnerabilities to infect endpoints. We found suspicious SMB traffic in half the organizations we assessed.

Even though SMB is a common protocol, visibility and proper analytics can separate good SMB behaviors from the bad. For instance, abnormally large numbers of SMB sessions, especially between hosts inside the network and those on the Internet, can be a sign of malware propagation.

When the FBI Comes Knocking

A global oilfield services company was informed by the FBI that Chinese cybercriminals had compromised its network.

The company installed the Cisco Stealthwatch system and within one week identified the source of the breach. A local user appeared to be logging in from China and exfiltrating gigabytes of critical files at a time. The user’s access credentials had actually been stolen, giving the attacker privileged access to sensitive data.

With proper network visibility, this behavior could have been identified and remediated before the company lost its data.

Traffic to High-Risk Countries

Most organizations do business only in certain geographic areas. Identifying traffic coming from outside those regions is an effective way to detect threats. For example, a utility company that serves only residents in the central United States should not be experiencing significant traffic coming from Eastern Europe or Asia.

It is especially important to detect traffic coming from regions associated with a high volume of threat activity. In the organizations we have assessed, 50 percent were already compromised by attackers from high-risk countries.

Organizations that monitor for traffic from suspect countries can identify and stop attacks before their systems are breached.

DNS Risk

DNS servers are integral to network operations, especially for accessing the Internet, because they translate host names to the appropriate IP address. The use of an unsanctioned DNS server can be a sign of malicious activity or policy violation. More than 70 percent of the organizations we have assessed had instances of unauthorized DNS use present on their network.
Many organizations rely on their own DNS servers to enforce policies such as preventing access to forbidden websites. Some savvy users will use unauthorized DNS servers to circumvent such policies. This can place the organization at risk if the user visits an insecure website or violates company policies on web content.

Even more troubling, 91.3 percent of malware uses DNS in attacks, according to the Cisco 2016 Annual Security Report. The malware will often reconfigure infected computers to use malicious DNS servers. These malicious servers redirect users to websites that serve exploits or phish for access credentials, placing the organization at risk of compromise and data loss.

Remote Access Breaches
Remote network access is quickly becoming a standard business practice for most companies. The ability to access company resources at any time or place is critical for a mobile workforce, but these services are also popular among attackers. When compromised, remote access services provide attackers with the same privileges as legitimate users.

Roughly 38 percent of the organizations we’ve assessed experienced some kind of breach due to remote access. Gaining visibility of remote access traffic is vital for identifying suspicious activity.

Custom Malware
During a Cisco Stealthwatch evaluation, a large technology company discovered that almost half of its end-user workstations were infected with custom malware written specifically for its network.

The malware had been quietly stealing data for an unknown period of time. There is no signature for situations such as this, but behavioral analysis was able to detect the malware scanning, connecting, and propagating throughout the network.

Telnet Risks
Telnet is an old and insecure protocol, and its use can lead to compromised credentials and data loss. Telnet facilitates communication between machines, but most versions have no effective encryption capabilities, making it a prime target for packet sniffers. When data is transferred in plain text, attackers can intercept it to obtain passwords and other sensitive information.

Most organizations believe they do not use this protocol, but our assessments found that 67 percent of organizations have Telnet traffic present on their network.

Telnet is an old and insecure protocol, and its use can lead to compromised credentials and data loss. Telnet facilitates communication between machines, but most versions have no effective encryption capabilities, making it a prime target for packet sniffers. When data is transferred in plain text, attackers can intercept it to obtain passwords and other sensitive information.

Most organizations believe they do not use this protocol, but our assessments found that 67 percent of organizations have Telnet traffic present on their network.

Mainframes and other systems that store sensitive data, financial programs, and customer information often run Telnet, which leaves them open to attack. Since 1994, the CERT Division of the Software Engineering Institute has recommended using something other than plain text authentication such as Telnet’s.

To ensure Telnet is not placing their organization at risk, security operators must be able to detect and respond to Telnet activity anywhere on the enterprise network.

Illuminating the Dark Areas of Your Network
Gaining visibility into each of these areas is critical to effectively securing your network and data. Fortunately, most networks have monitoring capabilities built in and simply require a way to take advantage of them.

Network traffic metadata such as NetFlow is inherent in most network infrastructure devices, including routers, switches, and firewalls. Cisco Stealthwatch collects and analyzes this data to construct an audit trail of all network traffic, including IP addresses, ports, users, devices, and applications. Cisco Stealthwatch can store months or years of flow data without the need for a prohibitively large amount of storage space.

With Cisco Stealthwatch, security professionals can obtain the in-depth network insight they need to:

- Uncover suspicious attack behaviors in real time, whether it is on the network, in the cloud, or within encrypted traffic
- Investigate previous attack attempts in order to identify the root cause
- Trace attacks back to specific users, devices, locations, and timeframes
- Improve their organization’s security posture

The Stealthwatch Online Visibility Assessment turns the lights on in your network and evaluates your internal visibility and overall security posture. The visibility assessment consists of a virtual appliance that will collect, encrypt, and transmit your flow data to a cloud-based analytics platform. After 14 days of data collection, a visibility assessment report containing detailed information and an analysis of current security risks is provided to you.

To learn more, visit www.cisco.com/go/stealthwatch-free-assessment.