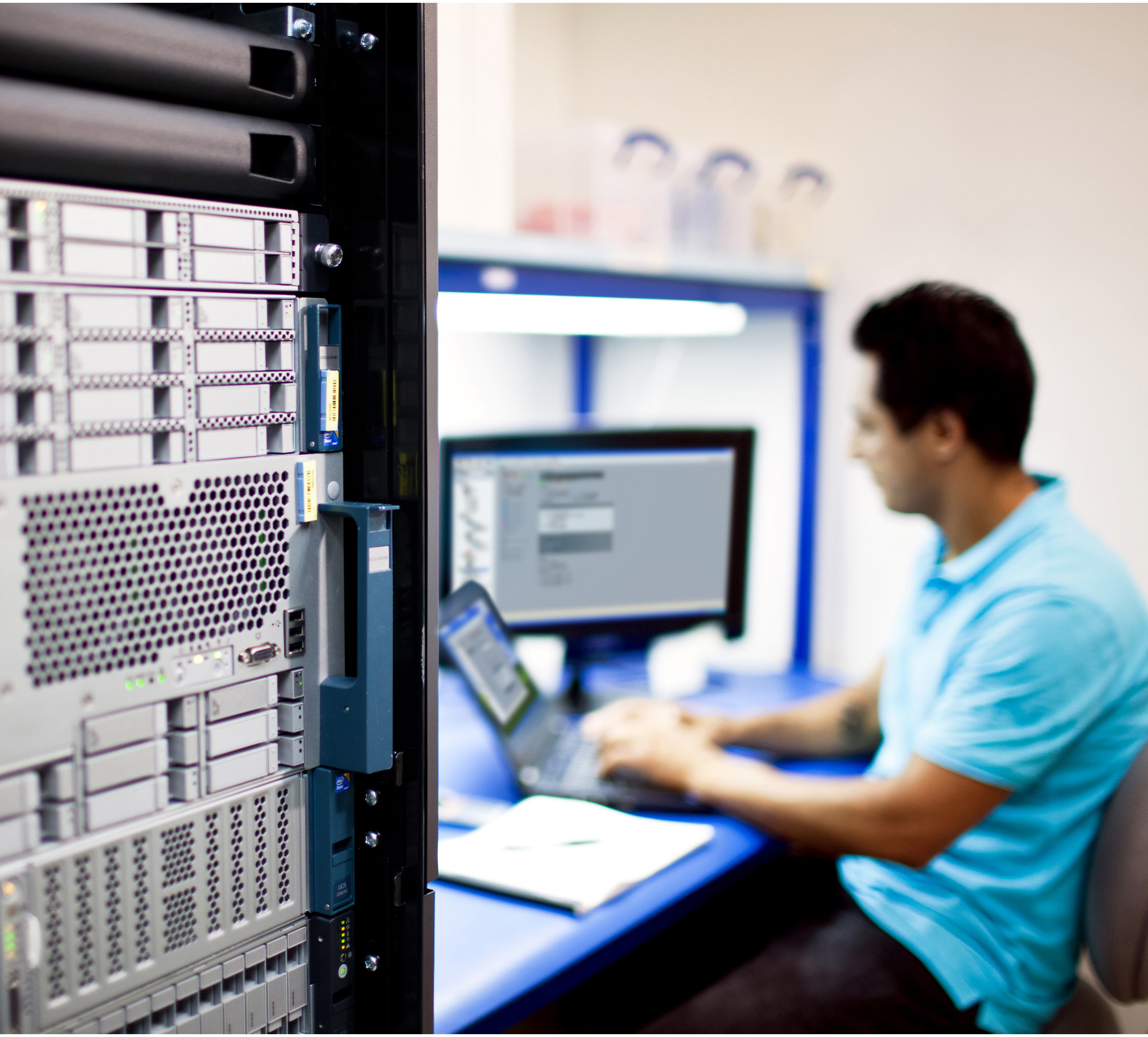
The Suspicious Seven: A Network Visibility Checklist



You know your network is already compromised. So what can you do?

The answer lies in network visibility. By providing you with insight into your attackers' behaviors and location within your environment, network visibility can help you prevent a security event from becoming a full-blown data breach.

Using our advanced visibility tools, we have assessed the networks of hundreds of organizations. We've found countless alarming issues, ranging from custom malware being used for data exfiltration to compromised servers used to attack government networks.

This checklist outlines seven of the most common types of network blind spots and suspicious activities that every security team needs to be able to see. If you can't detect these activities, you are giving threats a place to hide on your network.

Unauthorized DNS Use

Organizations use DNS to enforce policies and protect users from malicious websites. But use of unsanctioned DNS servers can be a sign of malicious activity or policy violations. Nearly 92 percent of malware uses DNS[1] in attacks, and more than 70 percent of organizations we have assessed had instances of unauthorized DNS use present on the network.

Rogue Server Activity

Rogue servers are servers that organization administrators have no control over, and they are a serious risk to security. Whether set up by a well-meaning employee or a threat actor, these servers allow threats to maintain a persistent presence on the network and exfiltrate sensitive data.

Server Message Block Risk

The Server Message Block (SMB) protocol is used in many organizations, and attackers use it to mask malicious activity. Targeted destructive malware such as Conficker use SMB to deploy proxy tools, install back doors, destroy data, and take servers offline.

Traffic Involving Suspect Countries

Most organizations do business only in certain geographic areas. Identifying traffic coming from outside those regions is an effective way to detect threats. If a utility provider in the western United States experiences significant traffic from Eastern Europe or Asia, it could be a sign of threat activity.

Remote Access Breach

Remote access is a common practice in most organizations, but it also gives attackers a means to gain privileged access to the enterprise network. Detecting anomalous or suspicious behavior among remote access users can identify cases of stolen access credentials or insider threats.

Telnet Activity

Telnet is an old, insecure protocol that transmits data unencrypted, which allows attackers to intercept it to obtain passwords and other sensitive information. Most organizations believe they do not use this protocol, but our assessments have found that 67 percent of organizations have Telnet activity on their network.

Other Anomalous Behaviors

Advanced threats are quick to innovate and adapt to avoid detection, and many rely on stealing legitimate credentials to circumvent defenses. Monitoring network activity for behavior that is known to be bad or is significantly out of the ordinary can help security operators detect even the most advanced threat activity.

For More Information

For more information on network visibility, read our whitepaper Solving the Visibility Gap.

[1] Cisco 2016 Annual Security Report