5 Vital Signs for Network Security Health

Just as healthcare providers monitor your vital signs on each visit, so too should you monitor your network vital signs.

The main vital signs routinely monitored by healthcare providers include body temperature, heart rate, respiration rate, and blood pressure. The first step in diagnosing an illness is to check for changes in your vital signs. What is most interesting about vital signs is often not their specific value, but the change in value over time for a given patient.

Here are five key network vital signs you should be monitoring to help keep your organization secure.

1: New Client and Servers

What to look for: There are lots of servers and clients on your network—and companies add new ones all the time as part of regular business operations. However, rogue servers on the network and unexpected clients communicating with those servers could be a sign that something is wrong.

Diagnosis: A new, unknown file server on your network could be a sign that someone is trying to exfiltrate information. A new SubSeven/Back Orifice/SVN server could indicate a backdoor used by a hacker. A new server could mean illegal file sharing.

2: Scans

What to look for: Unusual or increased scanning behavior on the network could indicate that your systems have been compromised and you need to find and stop the perpetrators fast.

Diagnosis: Scanning for open and available services is a common reconnaissance technique used by hackers who have found a way to infiltrate your network. Worms often resort to random scanning to find other systems to penetrate.

3: Blacklisted Communications

What to look for: Hosts that are known bad IP addresses such as botnet or malware distribution channels.

Diagnosis: A communication with a known bad host could mean that malware is being downloaded, or even that the attacker has already found a way into the network and the malware is establishing additional control and exploits.

4: Volume-based Activity

What to look for: Unusual increases in network traffic and connections on a continuous basis could represent an amplification, SYN flood, smurf/fraggle, slow loris, Christmas tree, LAND, IP/TCP NULL, or other attacks.

Diagnosis: These traffic patterns signal a potential in-progress DDoS attack that could take down your systems, so you need to be able to detect, classify, and mitigate them fast.

5: Data Exfiltration

What to look for: Data routinely moves in and out of your network. Unusually high volumes of data leaving the borders of the network—especially sensitive data—needs to be investigated immediately.

Diagnosis: Large data movement could be a sign that someone is stealing data. When organizations discover that they have been hemorrhaging sensitive data for weeks or months, the financial and reputational fallout can be devastating.

Key Takeaway

New clients and servers, scans, external communications, and data transfer are all routine events not necessarily a sign of a problem. However, when those activities change in volume or pattern, it's a sign that there could be something wrong. Your network's vital signs are also an early warning system. Monitoring them allows you to quickly identify and address changes so you can keep your network healthy.

For more information on how you can monitor your network vital signs with Riverbed, click here.