

The Signs of an Insecure Network

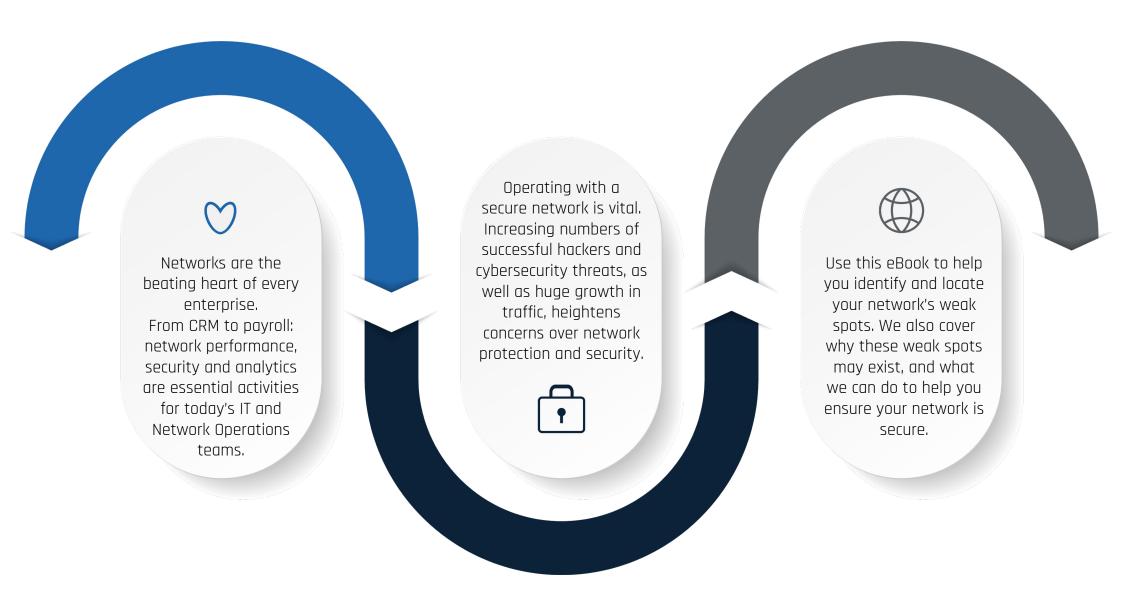
Identify and remedy your network's inefficiencies for ultimate network performance and success

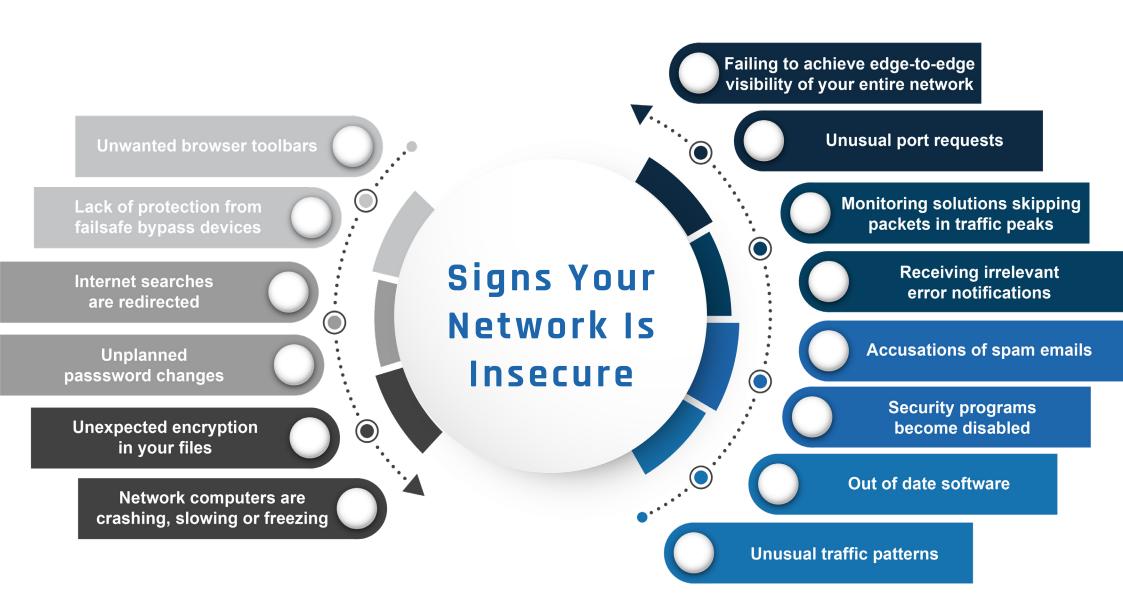


Contents

INTRODUCTION Signs Your Network Is Insecure Why Your Network Is Insecure	3 4 5		
		How We Can Help	6
		Contact Us	7

INTRODUCTION





NETWORK GROWTH

Networks can, and do, grow over time. The monitoring solutions installed last year may not be able to access all traffic in your network today. This is key as unmonitored areas of your network can result in weak spots which, in turn, compromises your network without detection. Make sure your visibility grow with your network.

WRONG TOOLS

Using the wrong tools for network security is unfortunately a common error that affects network performance. Without the right tools for your network, for example using SPAN Ports in cases where Network TAPs are better suited, results in a less secure network due to poor network visibility.

Why Your Network Is Insecure

03

01

SOFTWARE UPDATES

Delaying your software updates is another reason that your network may be insecure. Without timely software updates that introduce the latest security provisions, your software protection becomes outdated and therefore becomes a greater risk.

TRAFFIC FLOW

02

Monitoring tools may be seeing increasing traffic flows, either through organic growth or during peak periods. Being unable to successfully manage the traffic flow into monitoring tools will likely effect your efficiency and security coverage.

How We Can Help

Network Critical is the window to your network. We are the solution that provides 100% visibility into your network, thus ensuring network performance success. We achieve this for our customers through a variety of technology solutions that are best-in-class. See below how we can help:

1

2

3

4

Deploying our passive optical TAPs, which you can view here, to all areas of the network is an economical and robust method that we advocate to provide full visibility to network managers. This allows you to monitor all areas of your network for threats, including traffic that would not be visible when using SPAN ports. You can ask our experts where best to tap in your network, too.

Implementing our <u>specialised</u>

<u>Network Packet Brokers</u> can help because they:

- Report on traffic flow levels, providing 'first line' monitoring of the live traffic; raising alerts to unusual traffic behaviour.
- Aggregate multiple traffic paths into optimised feeds for the monitoring tool.
- Filter out unwanted traffic.
 Minimising the traffic being
 sent to the monitoring tools
 permits a smaller monitoring
 footprint with lower costs
- Provide load balancing, ensuring that traffic flows consitently to all tools thus allowing them to work at optimum efficiency.

Our Bypass TAPs with failsafe technology can be implemented alongside Inline monitoring tools, to add a layer of protection. If the monitoring tool suffers a problem, our Bypass TAP will reconnect the active network link ensuring that network traffic flow is maintained, minimising traffic loss and supporting SLA requirements. Find the diagrams on this page.

Sending the right data to your tools is key. Network Critical's PacketPro for packet manipulation is a highly complex and intelligent technology that allows you to prepare your packets for relevant tools. Whether you need to remove unwanted header layers, rewrite an address, or remove or redact the payload for security purposes, our PacketPro will be able to assist.

Contact Us

sales@networkcritical.com

Head Office, UK +44 (0) 118 954 3210 US Office, GA +1 (470) 554 7170