Fact sheet

Break the cyber attack chain with better information.

Network Threat Monitoring

verizon

As soon as you deploy new defenses, hackers are busy trying to work around them. So no matter how secure your network seems, you're probably still worried about it. Luckily, we can help you spot attacks before they get out of hand.

Know more about your traffic, identify potential threats and take steps to stifle breaches before they cause serious damage.

A single exploit may take an experienced attacker just seconds, but large-scale data breaches often develop over time. Attackers have to sift through your systems for the valuable data they want, then find a way to extract it. If you could see traces of these activities, you could stop attacks before they become critical problems.

Verizon Network Threat Monitoring gives you a chance to see an attack before it becomes a serious breach. We use NetFlow data from our IP backbone routers to discover if suspicious IP addresses are communicating with parts of your network.

When you see more, you can do more.

The service features basic traffic monitoring without requiring any additional hardware or software. You simply provide your IP addresses, and we look at a sample of the NetFlow data to identify traffic running over our routers to those IP addresses. Network Threat Monitoring automatically compares that data with our watchlists to identify potentially suspicious activity. We can analyze sample NetFlow records for many thousands, if not millions, of communications.

We've studied some of the world's largest and most notorious breaches and constantly gather intelligence data from public and private sources around the globe. As one of the world's largest internet service providers, we combine the visibility of our own IP network traffic with information about threats from many security disciplines.

Based on these watchlists, we can point out traffic going to suspicious locations on the internet or malicious hosts in your own network. By sampling traffic details and usage, you can decipher suspicious patterns and potential security gaps that may be early indicators of a compromise or network problems—including attack attempts and misconfigurations. You can then take action to stifle the attack before a serious breach occurs.

Identify threats before they become serious breaches.

You can see all the issues that Network Threat Monitoring identifies in the Security and Compliance Dashboard, which presents high-level information in an easy-to-read way. The dashboard also provides a detailed overview of the incidents. We'll automatically escalate all severe incidents so you don't miss them.

Cybercriminals aren't going to stop trying, but that doesn't mean they can't be stopped. By evaluating data from the Network Threat Monitoring service, your IT team can better detect malicious communications on your network and spot problems before they become serious issues.

Learn more.

To discover how Network Threat Monitoring can help you manage risk and avoid becoming the victim of a cyber attack, contact your account manager or visit:

verizonenterprise.com/products/security

© 2015 Verizon. All Rights Reserved. The Verizon name and logo and all other names, logos and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners. FS16469 12/15