

Cybersecurity monitoring

Devices that connect to a network – servers, workstations, routers, switches, IoT devices, firewalls and other security products – are continuously generating log data.



Managing the cybersecurity of a network is a challenge for any organization – large or small. Networks hold the hardware, systems, applications and data that companies rely on to conduct business and therefore must be secured so that the confidentiality, integrity and availability of all network components are assured.

However, networks today are “connected,” i.e., accessible from the internet. The challenge for companies is to monitor the devices on their networks to be certain that only authorized activity is taking place.

Most devices on a network produce logs—records of the activity taking place on that device. Access to log data can make it easier for administrators to understand what is happening on the network at any time and know when cybersecurity has been compromised. Most networks generate millions, or even billions, of log records each day, making manual review of log activity difficult. Any log-management function must be able to handle large amounts of data while also filtering out “noise” from those log records so that true “indicators of compromise” can be identified and presented in an alert to the network administrator.

Accessing cybersecurity monitoring capabilities

Organizations that continuously monitor their networks are much more likely to be cyber-resilient than those that do not. But until now, the cost of continuous monitoring has kept this capability out of reach for many small-to-midsize companies.

Zurich Cyber Insurance Policy customers can now opt in to a 24/7 cybersecurity monitoring and vulnerability management service to assist in identifying specific potential risks. These services also help you plan an effective path to remediation. Available through Zeneth Technology Partners, the ZenOpz™ service provides the following:

- Complimentary, one-time 360-degree threat assessment of your network and all visible devices
- Continuous, 24/7/365 monitoring of up to 50 connected devices on your network, such as servers, workstations, firewalls and other log-generating devices
- Full vulnerability scan of all devices in your agreement on a weekly basis, with full status reports and patch recommendations to mitigate revealed vulnerabilities
- Option to add devices for monitoring beyond the initial 50

Monitoring includes up to 50 connected devices on your network.

How ZenOpz works

ZenOpz managed security service provides log monitoring and reporting that is low-cost and does not require resources (human or computing) from the network owner after installation. When a customer opts in for the ZenOpz service, the following occurs:

- A simple, passive appliance provided by ZenOpz is sent to the customer with instructions for a simple 2-step (plug-and-play) installation.
- The appliance scans the endpoints and sends all generated vulnerability data to the ZenOpz cloud through a secure channel. The vulnerability report with recommendations is sent to the network administrator by email and is also available through a web-based customer portal.
- On each device to be monitored, a lightweight application is loaded which collects and packages the log data from that device and sends it to the ZenOpz cloud using a secure channel where it is aggregated and analyzed. Alerts resulting from the analysis are immediately presented to the network administrator via email.

ZenOpz access

Cybersecurity monitoring service is available by endorsement to the Zurich Cyber Insurance Policy. Access to ZenOpz is via a portal on the Zurich Cybersecurity webpage: www.zurichna.com/en/industries/technology/secpriv. You can opt in for the service by providing basic information, including your policy identifier. Once this information is submitted, you can access ZenOpz, where additional information on how to initiate your network-monitoring service will be provided.

For more information about Zurich Cybersecurity,
contact your broker or visit: www.zurichna.com/cyber.

Zurich

1299 Zurich Way, Schaumburg, IL 60196-1056
800 382 2150 www.zurichna.com

This is intended as a general description of certain types of insurance and services available to qualified customers through the companies of Zurich in North America, provided solely for informational purposes. Nothing herein should be construed as a solicitation, offer, advice, recommendation, or any other service with regard to any type of insurance product underwritten by individual member companies of Zurich in North America, including Zurich American Insurance Company, 1299 Zurich Way, Schaumburg, IL 60196. Your policy is the contract that specifically and fully describes your coverage, terms and conditions. The description of the policy provisions gives a broad overview of coverages and does not revise or amend the policy. Coverages and rates are subject to individual insured meeting our underwriting qualifications and product availability in applicable states. Some coverages may be written on a non-admitted basis through licensed surplus lines brokers. Risk Engineering services are provided by The Zurich Services Corporation.

ZenOpz is not a subsidiary or affiliate of Zurich and use of their products and services is independent from any Zurich products or services. Zurich expressly disclaims any and all damages and other costs that may arise related to the use of or reliance upon the products, services, representations or warranties made by or on behalf of ZenOpz. ZenOpz is a trademark of Zeneth Technology Partners.

©2019 Zurich American Insurance Company. All rights reserved.

A1-112012527-B (08/19) 112012527

