



# A CYBERSECURITY INCIDENT CAN OCCUR AT ANY MOMENT.

Implementation of a hybrid work model has created security gaps vulnerable to cyber threats. Add in the complexity of cloud and inadequately securing network-connected devices, and a cyber breach is inevitable. It's no longer a matter of if, but when. For the last 2+ years, IT organizations have grappled with this ever-changing work environment, and urgent deployments of inconsistent workflows and poorly implemented technology have led to a lapse in the management of users, data, and applications everywhere. Now what do you do? Let CyVig protect your attack surface from edge to endpoint.

By leveraging cyber threat data, hand-crafted algorithms, extended detection and response (XDR) with ML-Powered next-generation firewalls, our dedicated security analysts implement the Cyber Vigilance Trio (People, Process, Technology) to provide protection within minutes. Threats are isolated while our 24/7/365 U.S.-based Security Operations Center (SOC) team works hand in hand with your internal IT resources to mitigate risks and advance your security program.

## HERE'S HOW IT WORKS:



### 24/7/365 Network and Security Monitoring

Reduces response times and improves security outcomes. Dedicated experts monitor your environment and investigate threats as they occur.



### Automated Network Intrusion Prevention

Allows analysts to examine traffic flows from edge to endpoint detecting and automatically blocking traffic from malicious sources.



### SIEM/Centralized Threat Management

Centralizes the data collected across your entire environment to gain real-time visibility into activity that may introduce risk to the organization.



### XDR Endpoint Protection, Detection and Response

Unifies endpoint protection with detection and response across network, endpoint, and cloud assets.



### Next-Gen Machine Learning-Powered Firewall

Machine learning (ML) is embedded directly in the core of the firewall to provide real-time network-dependent device identification and inline, signatureless attack prevention.



### Alert, Event and Incident Management

Analysts investigate threats, define each attack's root cause, escalate to internal IT partners, and help facilitate targeted responses.

## THE IMPACTS OF A CYBER BREACH

**\$9.4 MILLION**

Average total cost of a data breach in the U.S. in 2021

**\$4.54 MILLION**

Average total cost of a ransomware breach in 2021

**\$167**

Cost per record of a data breach in 2021

**287 DAYS**

Average time to detect and contain a data breach

Breach data sourced from Ponemon Institute LLC.

Avoid business interruptions, reputational damage and a significant hit to your bottom line.

**Contact us today to begin fortifying your security program.**

**BE PROACTIVE. BE VIGILANT.**