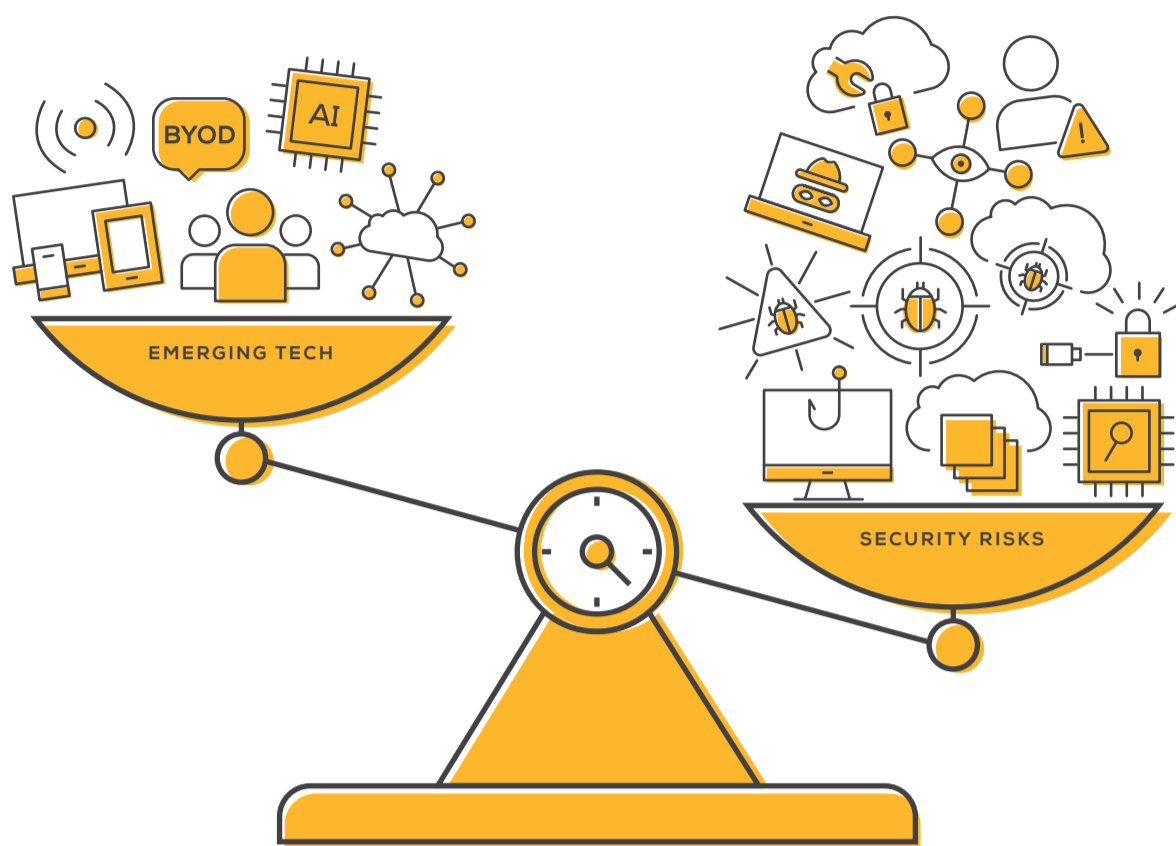




# Stay ahead of the cybercriminal heyday

As business becomes increasingly mobile, digital and cloud-based, networks become ever more vulnerable to cyberattacks. Add in the rapid rise of AI, IoT and the demands on in-house IT teams, and it's a perfect storm of opportunity for cybercriminals. To help defend your assets against today's fast-evolving threats, experts recommend a multi-layered approach to network security.

## The ultimate balancing act: Enabling emerging technologies. Ensuring security.

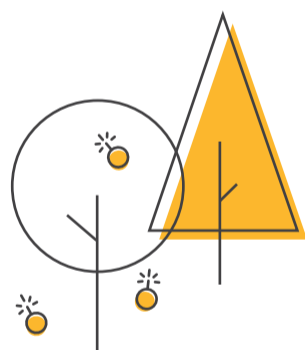


### Increasing ...

- Mobility
- Cloud computing
- IoT
- BYOD
- AI, ML and bots
- Demands on IT security teams

### ... exposes you to new and increased risks

- More exposure and endpoints
- Sophisticated phishing attacks
- Security alert fatigue
- Ransomware targeting the cloud
- New attacks leveraging old malware
- Human error configuring the cloud
- Personal apps on company network
- AI's ability to find and access data
- Deepfakes to ransomware targets
- RaaS spreading malware faster
- DIY cloud security



### Beware of low-hanging fruit for cybercriminals

- Old, unpatched vulnerabilities
- Existing, successful malware
- Overreliance on traditional tools
- Legacy infrastructures
- Fragile connectivity
- Misconfigured cloud environments
- Weak access controls
- Lack of real-time visibility
- Unmonitored network traffic

## More than \$3.5 billion was reported lost as the result of cyber crimes in 2019 alone.

FEDERAL BUREAU OF INVESTIGATION, 2019 INTERNET CRIME REPORT

### Defend against bad actors with an arsenal of security measures

- 24/7/365 monitoring
- SIEM
- IPsec VPN
- Stateful firewall
- Remote worker network access
- Application control
- Web content/URL filtering
- Antivirus/antimalware
- Intrusion prevention systems
- DNS filtering
- Cloud sandbox
- Botnet protection
- Content disarm and reconstruction
- Antispam
- Vulnerability management



Much of the success of cyber adversaries has been due to the ability to take advantage of the expanding attack surface and the resulting security gaps due to digital transformation.