# HOME WORKFORCE CYBER PROTECTION

COVID has changed our world. More office-based staff than ever are working from home. Most people do not need convincing of the advantages of remote working. Employer and employee alike. But there is a downside to remote working that often gets overlooked - employee cyber safety.

Anti-virus and VPN are standard-issue cyber protection for remote workers. Cyberattacks on home networks have risen by over 400%[1] during the pandemic. These suggest that this approach is not up to business-level security. Yet, home workers access the same data as they were in the office.

There are many challenges in protecting home workers. One challenge is that they share a network. Not only with other family members but with a multitude of internet-connected devices. Webcams, personal assistants, smart home-heating, gaming consoles, smart home-entertainment, WiFi-enabled children's toys. The list goes on.

**Botprobe** provides a robust, fully-managed cyber protection service for home workers.

## Home Workforce Protection

Attackers know that IT departments find it hard protecting non-company devices. So they search for weaknesses in these devices that will provide them with a door onto a home network.

Today's remote workforce and satellite office staff need two extra security elements:

### 1) Intruder Compromise Detection

- often the malicious act itself first alerts to the presence of an intruder. By this time, it is too late - a nefarious activity has taken place. It could be data theft, user or service compromise, or access to the corporate network. Yet, there are many indicators of an unwelcome guest.

### 2) Data Loss Prevention

- data leakage comes in many forms. This risk increases the longer the intruder has access to a network. For a home worker, the primary risk is theft of data. It could be direct theft via an attacker or malicious software. Or redirection of data to an intermediate endpoint on the way to the corporate network or cloud. A VPN cannot provide complete protection against all types of data leakage.

1 https://pages.checkpoint.com/cyber-attack-2020-trends.html

# HOME WORKFORCE CYBER PROTECTION

botprobe

## Home Worker Security Triad

Remote workforce protection requires three core elements:

1) anti-virus – **device** protection against malware
2) browser security – **user** protection against spam, ransomware and phishing attacks
3) network security - **home network** protection from intruders and data loss

Botprobe integrates with existing security tools, completing the home security triad.

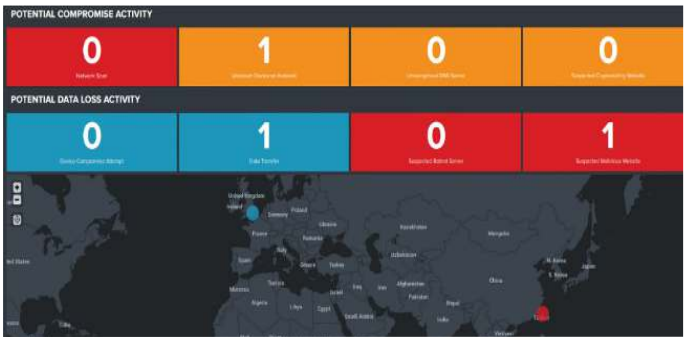
## The Implications of Weak Security

The repercussions from the theft of business-critical data can be huge. Not only financial or reputational consequences. The loss of personal identifiable information could lead to regulatory impact.

Botprobe's homeworker and satellite office cyber protection portfolio can help an organisation meet ISO and GDPR compliance.

## Botprobe Services Portfolio

| | | Homeworker Protect | Homeworker Advanced Protect | Homeworker Professional |
|---|---|---|---|---|
| INTRUDER DETECTION | Unknown device on network | ✓ | ✓ | ✓ |
| | Port scans | ✓ | ✓ | ✓ |
| | Web drive-by attack | | ✓ | ✓ |
| | Unusual network traffic profiles | | ✓ | ✓ |
| | Device vulnerability exploit attempt | | | ✓ |
| | Service password forcing | | | ✓ |
| | IT Policy violation | | | ✓ |
| | Safelist customisation | | | ✓ |
| DATA LOSS PREVENTION | Unusual data transfer activity | ✓ | ✓ | ✓ |
| | Request to unknown DNS server | ✓ | ✓ | ✓ |
| | Data transfer with known botnet servers | ✓ | ✓ | ✓ |
| | Data transfer with known malicious websites | | ✓ | ✓ |
| | Data transfer via TOR network | | ✓ | ✓ |
| | Data transfer with known cryptominer websites | | ✓ | ✓ |
| | Data transfer with known bruteforcer servers | | ✓ | ✓ |
| | Data transfer with unknown business-endpoint | | | ✓ |
| | VPN bypass | | | ✓ |
| | Safelist customisation | | | ✓ |
| | | Alert only | Alert + Dashboard | Alert + Dashboard |




Botprobe's cloud-based user-dashboard provides impact rating of compromise or data loss risks, geolocation mapping of suspicious data transfer or malicious web endpoints.

For a live, demo session as a guest user visit:
**www.botprobe.co.uk/demo**