Protection Beyond Antivirus and Firewalls

Most small businesses today are protected with **antivirus** and **firewalls** only. Defendify adds **multiple layers** of holistic protection to existing baseline defenses.

### Antivirus

**Protects devices against known infections**
- **Virus dictionary** identifies known malware (e.g. viruses, worms, etc.).
- **File and directory scanning** primarily detects, blocks and quarantines known malware.

### Firewalls

**Protects networks against unauthorized access**
- **Network controls** allow traffic in/out of the network, network segmentation, and/or VPN access.
- **Network monitoring** blocks traffic that doesn’t meet programmed security criteria.
- **Auxiliary features** may provide WiFi access, intrusion detection, and/or spam controls.

### Foundation

- **Cybersecurity health checkups** provide an assessment, score, and recommendations.
- **Technology & data use policies** establish workplace rules and expectations.
- **Incident response plans** identify steps to take in the case of an incident.
- **Ethical hacking** uses penetration testing to simulate an attack and provide results.

### Culture

- **Threat alerts** keep everyone up to speed with emerging attacks, stories, and patches.
- **Phishing simulations** test and train good habits through email attack scenarios.
- **Awareness videos** present bite size, engaging content to continuously train.
- **Awareness posters** serve as fun visual reminders in the physical workspace.
- **Classroom training** provides webinar-based education on key topics, threats, and tips.

### Technology

- **Stolen password scanning** identifies compromised credentials found on the Dark Web.
- **Vulnerability scanning** checks networks for weaknesses and reports on gaps.
- **Website scanning** checks websites for weaknesses and reports on gaps.

---

888.508.9221 • [hello@defendify.io](mailto:hello@defendify.io) • 1 Marginal Way, 2nd Floor, Portland, ME 04101
All-In-One Cybersecurity Platform

1. Threat Alerts Notification System provides visibility into relevant stories, incidents, and patches.
2. Cybersecurity Health Checkup Assessment Tool clarifies current cybersecurity posture and areas for improvement.
3. Stolen Password Scanner identifies compromised employee credentials so they can be reviewed and reset.
4. Incident Response Plan Builder establishes a simplified document with steps to take in the case of a breach or incident, including who is responsible.
5. Technology & Data Use Policy Builder establishes a simplified document setting workplace expectations and rules to train to.
6. Ethical Hacking uses human penetration testing and attack simulation to identify weaknesses for review and remediation.
7. Network Vulnerability Scanner identifies issues and exploits with networks for review and remediation.
8. Awareness Videos Learning System ensures ongoing employee training and engaging education.
9. Awareness Posters Library downloadable visual assets remind employees of key tips and topics in print and the physical workspace.
10. Phishing Simulation Tool keeps employees on alert with realistic email attacks and point-of-failure training.
11. Awareness Training Webinars are engaging web-based sessions for educating individuals and groups.
12. Website Scanner identifies issues and exploits found on public facing websites for review and remediation.