paloalto NETWORKS | **STRATA** BY PALO ALTO NETWORKS

How Can SMBs Stay Ahead of Cybersecurity Threats?

Struggling to stay on top of your security? You're not alone. **23% of small businesses describe cybersecurity as one of the top 5 biggest threats they currently face.**[1]

With tighter funds and fewer IT resources, small- and mid-sized businesses are increasingly vulnerable to successful attacks. **43%** experienced at least one cyberattack in the last year.[2]

Top offenders:[3]

Ransomware

Median intruder dwell time
28 days

Average ransom paid in 2021
$541,009.56

Increase over 2020
↑144%

Business email compromise

Median intruder dwell time
38 days

Average stolen
$286,000

Top access vectors in 77% of intrusions:[4]

- **Phishing**
- **Software vulnerabilities**
- **Brute-force credential attacks** (focused primarily on remote desktop protocol)

7 most targeted industries:[5]

- Finance
- Professional & Legal Services
- Manufacturing
- Healthcare
- High Technology
- Wholesale & Retail
- Education
- Hospitality

So, what's the solution for achieving big-time security as a small business?

ONE PART TECHNOLOGY

95% of common file and web threats can be prevented with machine learning-powered next-generation firewalls.[6]

What to Look for in a NGFW

- Prevents malicious activity concealed in encrypted traffic.
- Offers centralized management and visibility.
- Automates policy recommendations that save time and reduce the chance of human error.
- Enables consistent performance when security subscriptions are enabled.

TIP: Maximize ROI and prevent firewall disruption with AIOps.

ONE PART PEOPLE

95% of cybersecurity issues can be traced to human error.[7]

How to Build a Human Firewall

- Educate employees and customers on the latest attack trends.
- Do regular phishing tests.
- Incentivize employees using gamification.
- Establish a framework for effective patch management.

ONE PART STRATEGY

72% of cybersecurity professionals have already adopted—or plan to adopt—a Zero Trust security model to reduce the attack surface and prevent threats.[8]

Why Zero Trust

- Better security outcomes.
- Simplified infrastructure.
- Lower operational costs.