Cyber Security
Defending your Midmarket Digital Business

Your business relies on technology but lurking around the corner are intruders who can disrupt or devalue your operations.

A Techaisle midmarket global survey reveals:

- 97% agree that technology is important to the success of their business.
- 43% say that they have become more dependent on technology in the last 12 months.

But, midmarket firms have relatively small IT staffs. An average of 6.4 employees, who are tasked with:

- Delivering IT-enabled services
- Maintaining corporate IT environments
- Cloud-based & on-premise, Corporate-owned & employee-owned devices
- Managing IT budget, procuring, configuring & deploying physical assets
- Supporting users, patch management
- Researching, acquiring, aligning & continuously updating security technologies

Increased dependency on technology with stretched finite resources leave midmarket businesses vulnerable to cyber threats.

IT Security threats: Mobility & Cloud

- Midmarket businesses with mobility security breaches: 21%
- 79% of Midmarket Businesses had one or more mobility security breaches

Data breach is a matter of "when", not "if". Every midmarket business is a potential victim of cyber intrusion. Midmarket firms must deploy technologies & develop strategies to protect against intruders.

Midmarket businesses are investing in security solutions. Are you?

- 60% of midmarket firms are planning increased allocations to IT security.
- 8% of overall security spending annual increase by midmarket firms

Midmarket perception of most effective security technologies to protect data in the cloud:

1. Data encryption: 63%
2. Network encryption: 52%
3. Create data boundaries: 51%
4. Intrusion detection & prevention: 49%
5. Access control via broker or other means: 41%
6. Setting & enforcing security policies: 21%
7. Data categorization & segregation: 19%

Source: Techaisle global survey of 2015 midmarket (100-499 employees) businesses.