CoAction

CoActionTech.com
Sales@CoActionTech.com

SMB Fraud Defense

Each year cyber attacks become more sophisticated and widespread.

Small- to mid-sized businesses need robust security solutions to mitigate cyber threats and prevent fraud in the cloud.

33%

of all cyber attacks are targeted at small- to medium-sized businesses.

91%

of security breaches originate from phishing or spear-phishing attacks.

300M

fraudulent sign-in attempts are made to Microsoft cloud services every day.

Security Concerns for SMBs

As cyber security breaches make bigger headlines, more SMBs are starting to recognize their vulnerabilities.

43% of SMBs don't have a cyber security strategy in place.

61% of all small- to mid-sized businesses have reported at least one cyber attack in the past year.

75% of small businesses say they don't have the personnel to address IT security.

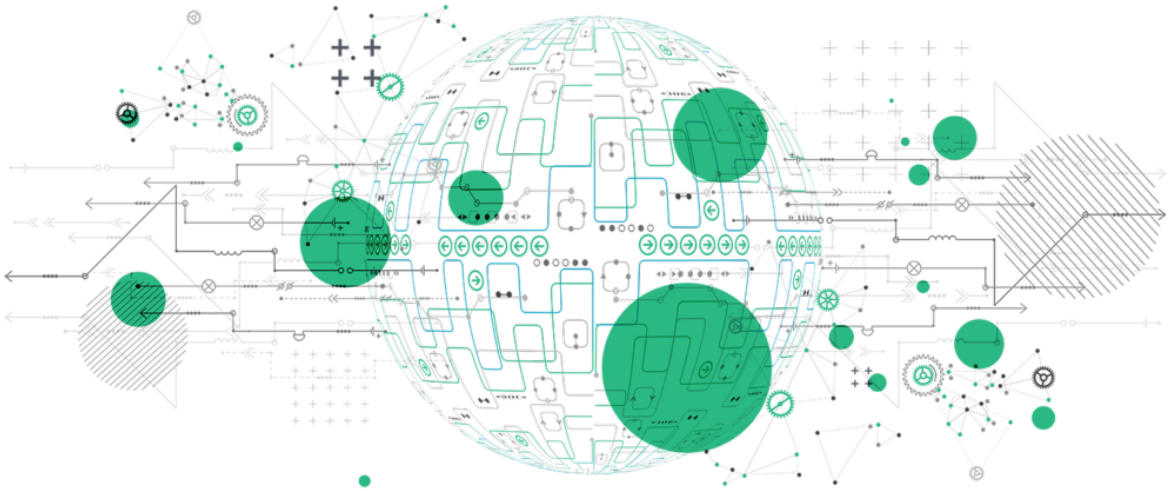
$955K on average is spent by small businesses per attack to restore normal operations; also 60% of victims go out of business within 6 months of an attack.

CoAction

CoActionTech.com
Sales@CoActionTech.com

Our Solution

With Microsoft Click-to-Run™ Solutions you can elevate your customers' security posture and reduce potential risks in day-to-day cloud operations.



Key Benefits:

- Proactively **detects** and **prevents** potential malicious cyber attacks.
- Sets up **alert mechanisms** and proactive **security policies** to **shield against** fraudulent activity in Azure environments.
- Helps to position you as a valued, trusted advisor.
- Partners also benefit from reduced costs, time and risks while **delivering industry best practices** for multi-level security standards when deploying the new solution for their clients.

With SMB Fraud Defense you can:

- **Enforce identity** and **Multi-Factor Authentication (MFA)** via Security Defaults or Conditional Access.
- **Provide a range of Conditional Access** pre-configured policies that are fully customizable and granular.
- **Enforce policies** across the Azure environment based on their needs.
- **Set thresholds** for Azure cost management and **send automatic alerts** if unusual activity is detected.

40%

of small businesses that faced a severe cyber attack experienced 8+ hours of downtime.

83%

of all small and mid-sized businesses are not financially prepared to recover from a cyber attack.

99.9%

of cyber attacks could have been prevented with multi-factor authentication.