WFH Security Bundle

AI Powered Remote Worker Protection

At VTECH, we are committed to make cybersecurity accessible to all by enabling MSPs to deliver cybersecurity-as-a-service. COVID-19 (Coronavirus) is driving many organizations around the world to rapidly adopt a work-from-home policy.

Business Email Compromise (BEC) and ransomware are the top two threats that MSPs and SMBs are facing in today's cyber-landscape. To enable MSPs to rapidly respond to the changing landscape, VTECH has designed a package specifically for companies with remote employees. Each product is backed by our 24/7/365 Security Operations Center and extensive technical and go-to-market support.

KEY FEATURES

- Prevents and Detects Business Email Compromise
- Blocks Ransomware
- Powered by AI and Machine Learning
- User-friendly
- Rapid, Remote Deployment
- SIEM Analysis
- AI Analytics Engine
- Multi-Tenancy Dashboard
- Self-Service Reporting
- Satisfies Industry and Regulatory Compliance

VTECH ENDPOINT PROTECTION

VTECH Endpoint Protection is an integrated threat prevention solution that utilizes our own streaming-data analytics platform. The product combines the power of AI to block malware infections with additional security controls that safeguard against script-based, fileless, memory, and external device-based attacks and is backed by our Security Operations Center.

VTECH EMAIL PROTECTION

VTECH Email Protection is a cloud-based email security product that blocks spam and phishing attacks. Our solution catches malicious emails by utilizing computer vision, AI and machine learning. Driven, curious, mobile, and growing smarter by the subject line, VTECH Email Protection adds an important layer of protection to your inbox.

VTECH O365 LOG MONITORING

SKOUT Office 365 Monitoring is a managed VTECHty product that collects, aggregates, and normalizes log data from Office 365 tenants using VTECH's analytics platform, SIEM, threat intelligence, and 24/7/365 Security Operations Center. Identify threat-like behavior in O365 like unauthorized access to cloud mailboxes, admin changes in the environment, impossible logins, mass file downloads, and brute force attacks.