WHITE DOG

Advanced Phishing Protection (APP)

Email Detection & Response

Gain real-time protection for the most vulnerable and targeted business tool in your organization.

The vast majority of breaches are the result of stolen passwords, not high-tech hacking tools. Business email compromise (BEC), spear phishing, and account takeover are today's top email threats. Adversaries continually evolve tactics to target and trick employees into making costly mistakes, so you cannot rely on your users be your first line of defense.

Advanced Phishing Protection (APP) empowers IT Operations teams and email admins with a more efficient way to protect users and their mailboxes against sophisticated threats. APP combines artificial intelligence, deep API integration with Microsoft Office 365, and brand protection to deliver a seamless cloud-based solution.

APP works alongside any email security solution as an indispensable component of a complete, multi-layered email security strategy. Our AI identifies and neutralizes known threats and adapts to new ones as they emerge, offering a dynamic defense mechanism that evolves in lockstep with an evolving threat landscape.

APP Editions

Starter
MAILBOX

Security beyond the gateway solutions. API integration into M365 &GWS.

Essentials
CLOUD STORAGE

Extend protection for your users beyond the mailbox, protect cloud storage that is included with M365 & GWS.

Premium
USER

Your users should not be your first line of defense, but they should be trained on how to respond via security awareness and simulated phishing.

KEY BENEFITS

- AI for real-time protection (Office 365 & Gmail)
- Identifies and neutralizes threats in real-time
- Defense against business email compromise (BEC)
- Account takeover protection
- Brand protection and domain fraud visibility (DMARC authentication and analysis)
- Limit damage and accelerate remediation (real-time notification, messages automatically quarantined)
- High risk employee analysis
- Visibility into inbox rule changes
- 100% cloud delivered
- API-based integration (15-minute set-up)
- Works in tandem with any email security solution

CONTACT US

Real-Time Protection

Defend Against Business Email Compromise

APP offers unique API-based architecture that enables its AI engine to study historical email and learn users' unique communication patterns. It can then identify anomalies in message metadata and content, to find and block socially engineered attacks in real time.

This approach based on historical patterns is far more accurate than traditional policy-based strategies for detecting socially engineered and account-takeover attacks.

Protect Against Account Takeover & Insider Risk

Account takeover lets hackers secretly study their target and plan their attack. Gateway defenses never see the internal attacks that are launched from these compromised accounts, so they can't detect them.

APP stops phishing attacks used to harvest credentials for account takeover. It detects anomalous email behavior and alerts IT, then finds and removes all fraud emails sent from compromised accounts.

Brand Protection & Domain Fraud Visibility

Domain spoofing is a common type of social engineering attack that targets your employees, customers, and partners. APP helps prevent email domain fraud with Domain-based Message Authentication Reporting and Conformance (DMARC) reporting and analysis.

APP helps set up DMARC authentication. Granular visibility and analysis of DMARC reports helps you minimize false positives, protect legitimate email, and prevent spoofing.

AI for Real-Time Protection

- Stops spear phishing attacks in real time
- Uses AI to learn each organization's unique communications patterns
    - Maps social networks inside the company to understand typical patterns
    - Identifies anomalies in metadata and content
- Real-time notification
    - Quarantines messages automatically
    - Alerts administrators and users
    - Visibility into historical and internal communications
- Comprehensive protection against personalized attacks (spear phishing, BEC, whaling, impersonation attempts, and/or CEO fraud)
- Blackmail and extortion email protection

Account Takeover Protection

- Real-time defense and remediation
- Detects and alerts account takeover activity/compromised email
- Notifies external users and deletes compromised email
- Blocks attackers' access to compromised account
- Provides visibility into inbox rule changes
- Alert on suspicious sign-ins

Domain Fraud Protection

- DMARC authentication and analysis to prevent:
    - Brand hijacking
    - Domain spoofing
- Intuitive wizard to help set up DMARC authentication
- Analysis of DMARC reports to understand who is sending mail from each domain
- Ensure deliverability of legitimate messages
- Actionable step-by-step insights to comply with DMARC

Advanced Phishing Protection (APP)

	Starter	Essentials	Premium	
Co-Managed Global SaaS Platform				
Secure Access, High Availability	✅	✅	✅	
Complete Management & Monitoring	✅	✅	✅	
24 x 7 x 365 Security Operations Center	✅	✅	✅	
Real time identification and response to threats by SOC	✅	✅	✅	
Email Security				
Mailbox Protection (GWS or M365); 10 unit minimum	✅	✅	✅	
AI-based Threat Detection & Protection	✅	✅	✅	
Phishing & Spear Phishing Protection	✅	✅	✅	
Account Takeover/Impersonation Detection	✅	✅	✅	
Zero Day Phishing Protection	✅	✅	✅	
BEC & CEO Fraud prevention	✅	✅	✅	
Cloud Storage Security				
Real-time Scanning of All Files		✅	✅	
Commodity malware detection		✅	✅	
User Security				
Security Awareness Training			✅	
Advanced Threat Simulation			✅	
Program Gamification			✅	

Read data via API
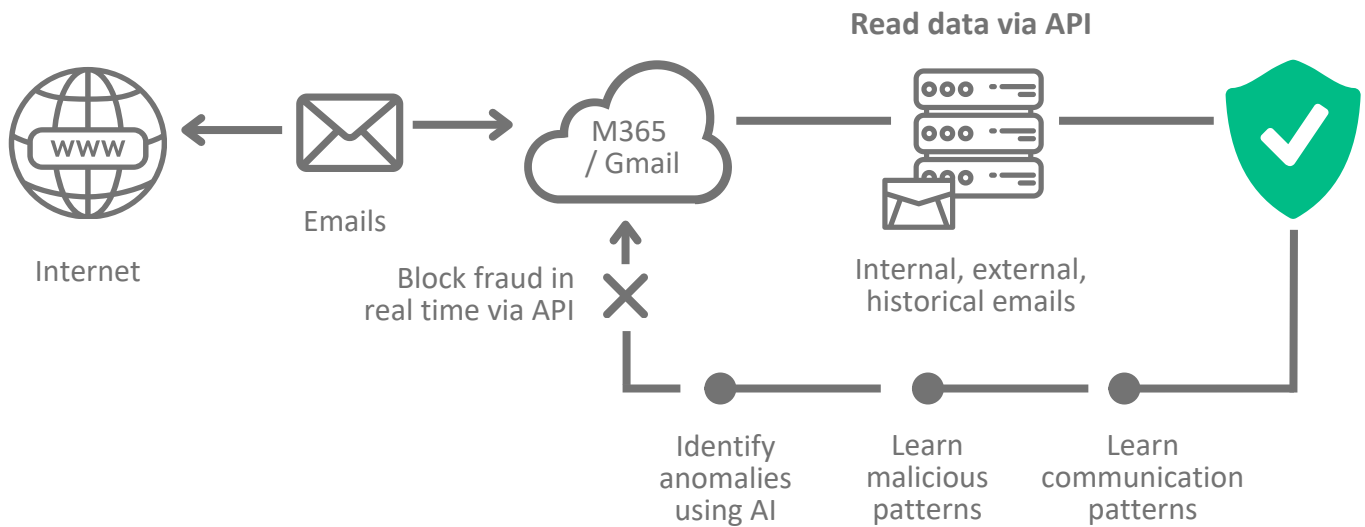
Microsoft
Microsoft Exchange
Exchange Online
Office 365

Google
Google Gmail

Powered by WHITE DOG