Barracuda **Sentinel**

Artificial Intelligence for Real-Time Email Protection

Business email compromise (BEC), spear phishing, and account takeover are rapidly becoming the most significant security threats facing organisations. These hyper-targeted attacks use socially engineered tactics designed to deceive employees and can be devastating to your business and brand.

Barracuda Sentinel combines artificial intelligence, deep integration with Microsoft Office 365, and brand protection into a comprehensive cloud-based solution that guards against business email compromise, account takeover, spear phishing and other cyber fraud.

The Barracuda Advantage

- AI that learns your business's unique communication patterns to detect personalised fraud in real-time
- The only solution on the market with API-based architecture to stop threats emanating from within your organisation that traditional gateways cannot
- Comprehensive solution for detecting and stopping email account takeover

Product Spotlight

- API-based architecture provides direct connectivity to Office 365
- AI solution for real-time protection against targeted attacks
- Brand protection using DMARC reporting and enforcement
- Works alongside any other email security solution including Barracuda Essentials and Microsoft Office 365
- Fast, cloud-based setup that does not require re-routing email traffic

AI

Real-Time Defence Against Business Email Compromise

At the heart of Barracuda Sentinel is the AI engine that detects and blocks socially engineered attacks in real-time and identifies the employees who are at highest risk.

Unique API-based architecture gives Sentinel's AI engine access to historical email data to learn each user's unique communications patterns. The engine leverages multiple classifiers to map the social networks of every individual inside the organisation and identifies anomalous signals in message metadata and content.

Sentinel's unique approach does not rely on static rules to detect targeted attacks—it relies on historical statistics of each organisation to determine with a higher degree of accuracy whether a certain email is part of a socially engineered attack or account takeover.

Protection Against Account Takeover and Insider Risk

Every day, legitimate business accounts get compromised due to stolen credentials. The account takeover can remain dormant in your environment for months, with hackers watching and learning before launching their attacks. Any internal attacks launched from a compromised account often don't pass through the gateway and therefore go undetected.

Barracuda Sentinel's comprehensive solution to account takeover includes three components: prevention, detection, and remediation. Barracuda Sentinel prevents targeted phishing attacks that bypass traditional email gateways and can lead to harvesting credentials. If an account has been compromised, Barracuda Sentinel detects the anomalous behavior and alerts IT. Finally, Barracuda Sentinel can remediate the attack by removing all of the malicious emails sent by the compromised account from within employee mailboxes with one click.

Brand Protection and Domain Fraud Visibility

Domain spoofing and brand hijacking are a common technique used by hackers in social engineering attacks. Domain spoofing can be used to target organisation's employees, customers, external partners, and other third parties that would trust its brand. Barracuda Sentinel provides complete protection from email domain fraud through DMARC (Domain-based Message Authentication Reporting and Conformance) reporting, analysis, and visibility.

Barracuda Sentinel offers an intuitive wizard to help companies easily set up DMARC authentication. Once DMARC is properly configured, it provides granular visibility and analysis of DMARC reports to help customers properly set-up DMARC enforcement and reduce the potential of false-positives enforcements.

Well-configured DMARC enforcement ensures deliverability of legitimate email traffic and prevents unauthorised spoofing emails.

Key Features

AI for Real-Time Protection

- Stops spear phishing attacks in real time
- Uses artificial intelligence to learn each organisation's unique communications patterns
  - Maps social networks inside the company to understand typical communications 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 personalised attacks, commonly known as spear phishing, business email compromise (BEC), whaling, impersonation attempts, and/or CEO Fraud

Account Takeover Protection

- Real-time defence and remediation

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

High Risk Employee Analysis

- Identify high-risk individuals inside the company using artificial intelligence

Deployment & Availability

Available to Microsoft Office 365 Users Worldwide

100% Cloud Delivered

- No hardware or software required to install or maintain

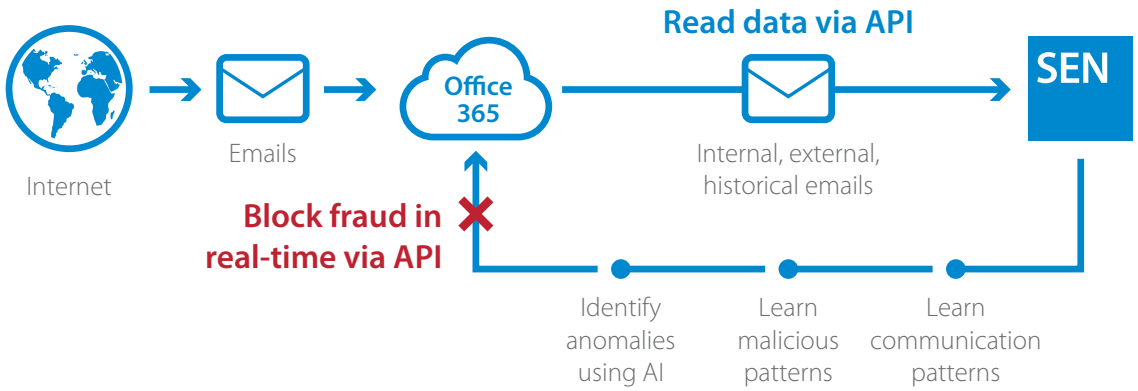
Works Alongside any Email Security Solution

- Barracuda Essentials – email security, archiving, and backup for Office 365
- Barracuda Email Security Gateway
- Microsoft Exchange Online Protection (EOP)
- All others

API-based Architecture

- Direct connectivity to Office 365
- Zero impact on network performance or user experience
- Fast, easy set-up (less than 5 minutes)

Sentinel – How it works



List pricing is based on per user, per year. Discounts are available to Barracuda Essentials and Barracuda Email Security Gateway customers. Volume discounts apply. International pricing may vary.