Barracuda **Sentinel**

Artificial Intelligence for Real-Time Spear Phishing and Cyber Fraud Defense

Spear phishing attacks are rapidly becoming the most significant security threat today. These attacks are highly personalized and the results can be devastating to individuals, businesses, and brands—$5 billion in losses so far, according to the FBI. Barracuda Sentinel combines three powerful layers of artificial intelligence, domain fraud visibility, and simulated fraud training into a comprehensive cloud-based solution that guards against spear phishing, impersonation attempts, business email compromise (BEC), and cyber fraud. **Barracuda Sentinel is the leading AI solution for real-time spear phishing and cyber fraud defense. It integrates directly with Microsoft Office 365 to protect people, businesses, and brands from these personalized attacks in real time, with zero impact on network performance.**

The Barracuda Advantage

- The security platform for today's IT Professionals
- Powerful, yet easy-to-deploy and manage security and data protection solutions
- Global threat intelligence framework across multiple threat vectors, including email, network, application, and web
- Flexible deployment across public and private cloud, on-premises, and hybrid environments
- Trusted by more than 150,000 organizations worldwide to protect their networks, applications, and data

Product Spotlight

- AI solution for real-time spear phishing and cyber fraud defense
- Domain fraud protection using DMARC authentication
- Fraud simulation training for high-risk individuals
- Works alongside any email security solution, including Barracuda Essentials, Exchange Online Protection, and others
- API architecture – easy set-up, zero impact on network performance

AI

Real-Time Spear Phishing and Cyber Fraud Defense

At the heart of Barracuda Sentinel is the AI engine that detects and blocks spear phishing attacks in real time, and identifies the employees inside an organization who are at highest risk of spear phishing.

Barracuda Sentinel utilizes artificial intelligence to learn each customer's unique communications patterns. The engine analyzes multiple classifiers to map the social networks of every individual inside the company and identifies anomalous signals in message metadata and content.

Barracuda Sentinel combines this messaging intelligence to determine with a high degree of accuracy whether a certain email is part of a spear phishing attack. If so, Barracuda Sentinel quarantines the attacks in real time, and alerts both the user and the administrator.

Domain Fraud Visibility and Protection

Barracuda Sentinel helps protect customers from domain spoofing and brand hijacking.

Barracuda Sentinel offers an intuitive wizard to help companies easily set up DMARC (Domain-based Message Authentication Reporting & Conformance) authentication. DMARC is a protocol that allows companies to monitor emails sent from their domain.

Once DMARC is properly configured, Barracuda Sentinel offers granular visibility and analysis of DMARC reports to help customers ensure deliverability of legitimate email traffic and prevent unauthorized activity such as spoofed emails.

Simulated Fraud Training for High-Risk Individuals

The personal nature of spear phishing attacks means that everyone is a target. Not just the large enterprise; not just the C-suite. Attackers are more frequently targeting lower-level employees who might have access to sensitive information or who might have the ability to authorize or send payments.

Barracuda Sentinel utilizes artificial intelligence to identify high-risk individuals within an organization. Administrators receive access to a set of tools to then periodically conduct simulated spear phishing attacks to test the security awareness of those individuals.

Key Features

AI for Real-Time Protection

- Stops spear phishing attacks in real time
- Uses artificial intelligence to learn each organization'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
- Comprehensive protection against personalized attacks, commonly known as spear phishing, business email compromise (BEC), whaling, impersonation attempts, and/or CEO Fraud

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

Fraud Simulation Training

- Identify high-risk individuals inside the company using artificial intelligence
- Test and improve security awareness using simulated spear phishing attacks

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

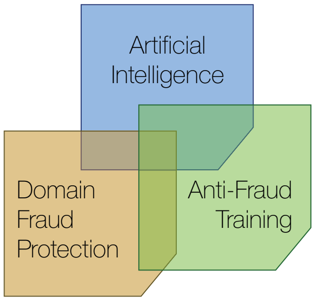
- Barracuda Essentials – email security, archiving, and backup for Office 365
- Barracuda Email Security Gateway
- Microsoft Exchange Online Protection (EOP)
- Others

API-based Architecture

- Direct connectivity to Office 365
- Zero impact on network performance or user experience
- Fast, easy set-up (less than 5 minutes)
- Cross communications platform defense
  - Easily extend beyond email to other communications platforms like G-Suite, Slack, Skype, or others

Barracuda **Sentinel**

AI for Real-Time Spear Phishing
and Cyber Fraud Defense



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. Additional information is available at **www.barracudasentinel.com.**