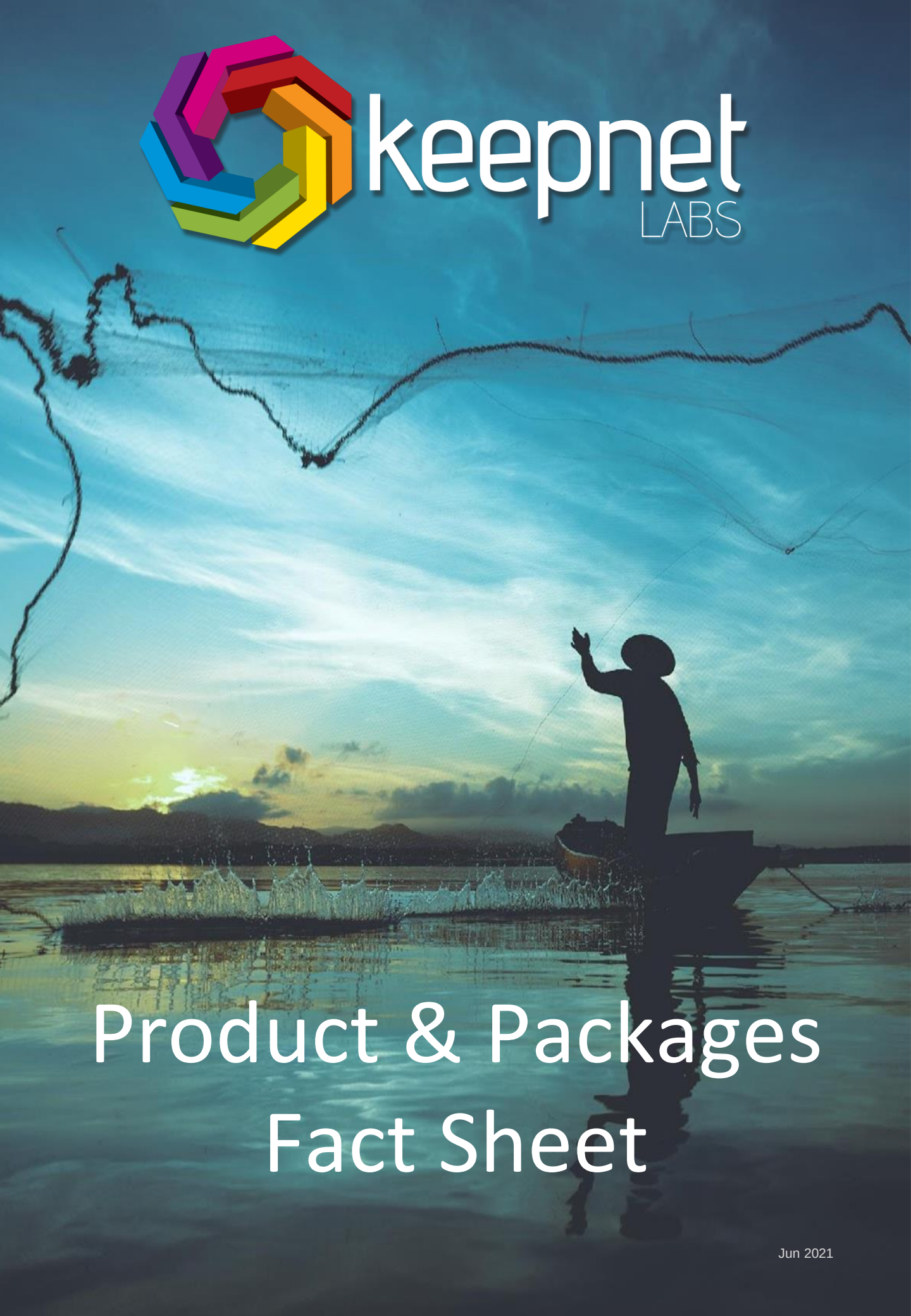
keepnet LABS



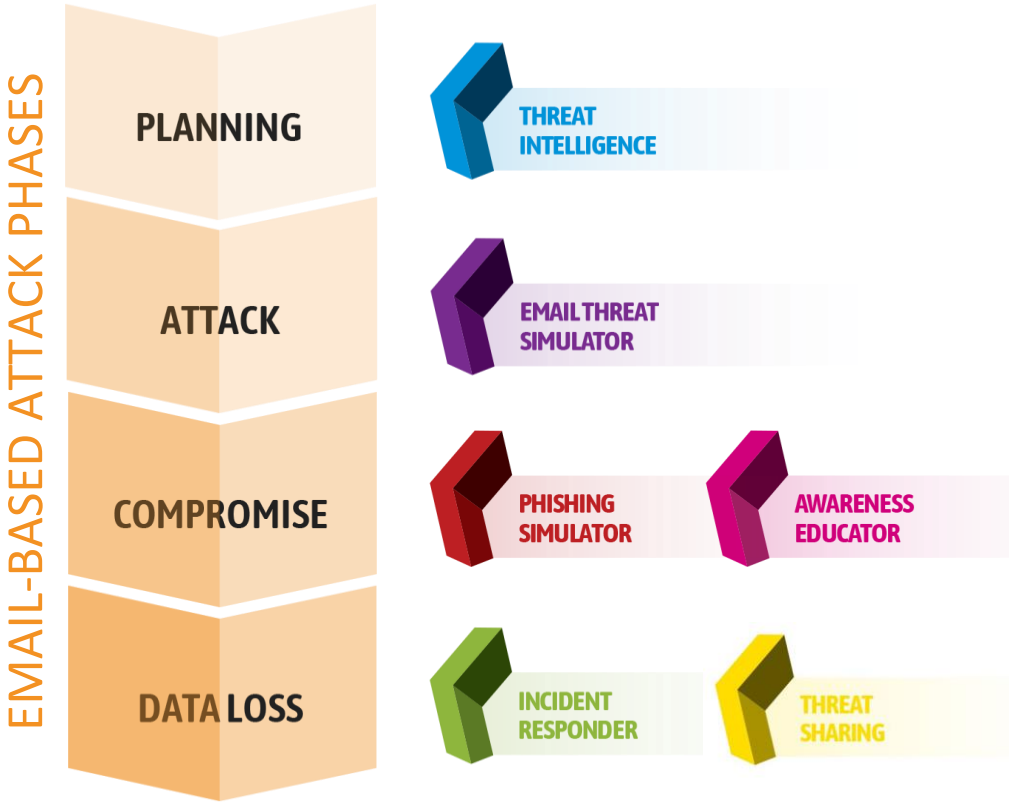
Product & Packages Fact Sheet

Jun 2021

keepnet LABS

Phishing, Awareness & Defense Platform

"protecting businesses through the life cycle of email-based attacks"



Packages Available:

Defender
- THREAT INTELLIGENCE
- EMAIL THREAT SIMULATOR

Awareness
- PHISHING SIMULATOR
- AWARENESS EDUCATOR

SOC
- INCIDENT RESPONDER
- THREAT SHARING

Enterprise
- THREAT INTELLIGENCE
- EMAIL THREAT SIMULATOR
- PHISHING SIMULATOR
- AWARENESS EDUCATOR
- INCIDENT RESPONDER
- THREAT SHARING

keepnet LABS

Defender

Product/ Market Position

Threat Intelligence provides compromised credentials from known breaches - without remediation, a breach is considered inevitable.

Email Threat Simulator tests the company's email defense technology against a wide range of email attack vectors, malware and misconfigurations.

Complimentary Vendors/ Solutions

SIEM and SOAR products, such as IBM Resilient, Splunk Phantom, Palo Alto Demisto, etc.

Microsoft ATP
Email Gateways (e.g. Barracuda, Mimecast etc.)
Firewalls and Spam Filters

Threat Intelligence
Data Leakage Monitoring
Deep Web & Dark Web Digging
Threat Feeds
3rd Party Threat Intelligence Service Integrations

"94% of malware is delivered by email"
Verizon

"91% of all cyber attacks begin with a phishing email to an unexpected victim"
PhishMe

Email Threat Simulator
Phishing
Spear-Phishing
Domain Squatting
Client-side Attacks
Malicious Attachments
Ransomware Samples
Misconfiguration Tests
Browser Exploits
File Format Exploits
No Installation, Conf or Special Permission Needed
Remediation Checklist
Testing of DLP & Similar Security Solutions
Email Threat Simulator add-in
Generating Threat Simulator Policy/Procedure
Assessment and Remediation Report
API Automated Scanning

Primary Use Case

Malicious emails bypass company's email security. Company wants to regularly test current products/ controls, then mitigate vulnerabilities found.

Why buy? USP?

Implement in minutes, easy to schedule, more effective that using emulators. Can simulate insider attacks and tests for misconfigurations in addition to malware samples.

keepnet LABS

Awareness

PHISHING SIMULATOR

AWARENESS EDUCATOR

Product/ Market Position

Complete phishing simulation and integrated LMS platform, for end customers (or resellers/MSSPs) to have complete control over phishing and awareness training. Purpose – human factor – build cyber awareness culture so that users engender active defense behaviours.

Fully functional LMS with added third party content available as bundle upgrades. Suitable to track compliance with IT and corporate policies. One click engagement for end users and gamification.

Complimentary Vendors/ Solutions

Awareness Vendors, MSSPs, Consultancies, VAR, cloud platform services, InsureTech + OEM

Bespoke Content (training, policies, assessments) NINJIO, Bobs Business, Cybermaniacs, etc.

Phishing Simulator
1,000+ Phishing Scenarios in the Library
One Click Launch
URL Site Cloning
Trusted SSL Support for Phishing URL's
Playbooks for Phishing Campaigns
Password Complexity Checker
Clone Scenarios
Annual Security Awareness Plan
Customisable Attachment Attacks
File-Upload Templates
Sending Prioritisation
On-the-Fly Custom Subdomain Creation
Cloudflare Integration
Phishing Campaign "Mark As Test"
APIs for Phishing
DLP Activation String
Custom Domains

Awareness Educator
Fully Functional LMS
Rich Content Library, Incl. Third Party: NINJIO, Bobs Business, Cybermaniacs, GetZem Secure, Mavi Interactive
One Click Launch for End Users
Integration with Phishing Simulator & Other API
3rd Party eLearning Integrations (iSpring)
HTML5 Compatible
Upload Custom Content (incl. Policies)
Serious Games
Customisable Certificates
Scheduled Reports
Leader Boards for Gamification
Automated Training Assignment
Posters and Infographics
Weekly Newsletters
Screensavers & Tip Sheets

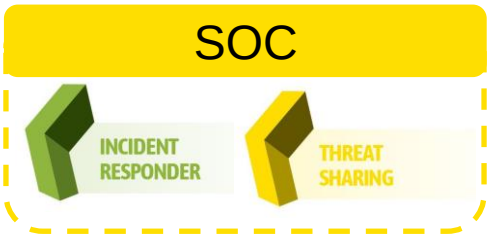
Primary Use Case

"Human factor" - Company concerned about vulnerability of employees clicking links/attachments, or compliance driven (e.g. ISO27001). Companies observing record numbers of phishing attempts.

Why buy? USP?

Simple to use, complete and mature solution with many USP features for highly demanding customers. Variety of content providers available, offering wide choice. Partners offer full Awareness managed services.

keepnet LABS



Product/ Market Position

Automated (email) incident analysis, investigation and response – mitigate threats that bypass email defense technology with one click.

Threat Sharing: Share email threat intelligence anonymously, within trusted communities, in near real time. When combined with IR, very powerful solution, leveraging the eyes in the community, to beat attackers at a community-wide level.

Complimentary Vendors/ Solutions

SIEM and SOAR products, such as IBM Resilient, Splunk Phantom, Palo Alto Demisto, etc.

Most threat analysis tools, such as Antivirus, Sandboxes, Email Gateways. Integrates for investigation with Outlook, Exchange, O365 and G-Suite.

Threat Sharing is a big opportunity for all companies to gain access to intelligence sharing communities with actionable alerts and full integration with Incident Responder. Unlimited integration possibilities on next gen platform.

Incident Responder & Threat Sharing	
Customisable Phishing Reporting Add-in for O365/OWA/Outlook/Gmail clients	Built-in Integrations with Analysis Services
Automation Playbooks	IOC Feeds
Generating Custom Rules	Incident Response Capabilities
Cross-Organization Threat Sharing	Create and Manage Communities
Real-Time, Human Verified Threat Intelligence Sharing	Share Threats Anonymously within Communities
Orchestrated Suspicious Email Analysis	Fast Launch Investigations from Intelligence Received
Advanced Polymorphic Email Detection	Investigation Emails Stored as .PST Files
Affected Inboxes Real-Time Report	Investigation on Archiving Systems (like Enterprise Vault)
1-Click Smart Investigation on the Inbox	ROI Calculator
Auto Investigation by Playbooks	Audit Logs
Automated Workflow Triggering	Encryption of Phishing Reporter Users Details
Investigation on the Client Inbox via Add-in	SIEM Integrations
Investigation on O365 & Exchange and GSuite	Configurable API requests/responses logging.
	SAML Integration

Primary Use Case

When our user(s) receive a malicious email that has bypassed the perimeter, we cannot analyse and investigate fast enough, so response is not adequate. We don't have the technical skills available to respond in time. We need better, actionable alerts for email threats.

Why buy? USP?

Implement within an hour, easy to automate and can add API integrations to other security products. E.g., sandboxes, analysis services, etc. – therefore can leverage other investments and centralise processes. Respond to attacks in minutes.

keepnet LABS

Phishing, Awareness & Defense Platform

Enterprise

Why buy Enterprise?

Keepnet Labs is the only vendor to provide features that protect against each stage of the email-attack lifecycle. The platform addresses people, processes and technology, and offers affordable pricing.

Threat Sharing is a game changing, next generation solution that is reinventing how businesses identify and stop active email-based attacks.

"New types of cyber attacks are emerging every day; that is why our security technologies can be insufficient against such attacks, no matter how good they are. Email Threat Simulator enables us to see if the technologies we use are effective against the most recent cyber attacks."
Head of IT Security, Telecoms

"In addition to educating users with Keepnet Labs Awareness Educator modules, we have successfully applied the gamified learning method to our company and another 7 subsidiaries, which teaches users how to behave against risks by building skills for behavioural change. Conclusion: We have hundreds of cybersecurity agents."
Head of InfoSec, eCommerce

"In cases where a malicious email targeted our bank and its affiliates, we had to coordinate the different teams for incident intervention and compound the output of many products and thus analyse this email. With Keepnet IR module and the Phishing Reporter add-in, we solved this problem in the most efficient manner by executing incident investigations and responses within users' inboxes in minutes with one click."
CISO, Investment Bank

keepnet LABS

Phishing, Awareness & Defense Platform

System Management, Integrations, Security & Compliance

Deployment
Cloud (SaaS)
On Premise
Hybrid

Management Roles
Multi Tenancy Model for SOC Team and MSSPs
Company Admin
Company User
Reseller Mode
Role Based Access
Custom roles

Advanced Settings
Seamless Integrations for Active Directory
Seamless SIEM Integrations
Static and Dynamic User Group Management
White-Labelling
Seamless Integrations for Azure AD SCIM
Seamless Integrations for Octa AD SCIM

Integrations
Cloudflare
Virustotal
IBM X-Force
IBM Q-Radar
AlienVault OTX
Exchange EWS
haveibeenpwned.com
Office 365
Google Gsuite & Gmail
POP3 / IMAP
Veritas Enterprise Vault
Bluecoat Antispam
Cisco IronPort
Symantec Antispam
Splunk
ArcSight SIEM
Jira Integration
Fortinet Sandbox
VMray Sandbox

APIs
API for Phishing Simulator
API for Incident Responder
API for Email Threat Simulator
API for Awareness Educator
Custom API Development
Rest API
API for Dashboards and Reporting

Security, Compliance and Certificates
Regular Internal/External Code Validation
Regular Penetration Testing
Source Code Escrow
GDPR Compliant
Security
Full Disk Encryption
2 Factor Authentication
Ldap Authentication
Audit
Zero Trust Audit Mechanism
Data Anonymization (for GDPR)
IP Encryption
User-Agent Encryption
Browser Information Encryption
E-mail Address Encryption
Captured Data Encryption
Certifications
ISO 27001 Certification

For technical documentation and user guides: https://doc.keepnetlabs.com

www.keepnetlabs.com

Turning Vulnerability into Strength