SPEED TO DETECT
SCORECARD

PROOF THAT MAILGUARD IS UP TO 48 HOURS FASTER TO STOP EMAIL THREATS.

Microsoft Partner

GCC
Global Compliance Certification
ISO 27001 Certified

JAS-ANZ
WWW.JAS-ANZ.ORG/REGISTER

mailguard

HOW LONG IS TOO LONG FOR A THREAT TO SIT IN YOUR EMPLOYEES M365 INBOXES?

Every second matters when a malicious threat is sitting in a business's employee inboxes.

The important question to ask a vendor is not if they stopped a threat, but when, because sometimes that window of vulnerability can be hours or even days. Its why experts recommend a cybersecurity 'mesh' approach to protect your business.

And, it's why we developed the 'Speed to Detect Scorecard', to demonstrate how much faster MailGuard identifies and blocks advanced, malicious, zero-day threats.

Because MailGuard is proven to stop threats up to 48 hours faster.*

*Every email is different and speed to detect will vary for each individual threat. In this report we demonstrate one example where MailGuard was > 20 hours faster, and another which was not identified 9+ days after initial detection. These examples are not isolated incidents, rather they are representative examples of threats that MailGuard intercepts every day. MailGuard advertises up to '48 hours faster' as an indicative maximum, although some examples may be even longer.

MailGuard, defending the Microsoft 365 ecosystem.

"It's the type of innovation that we want to see."
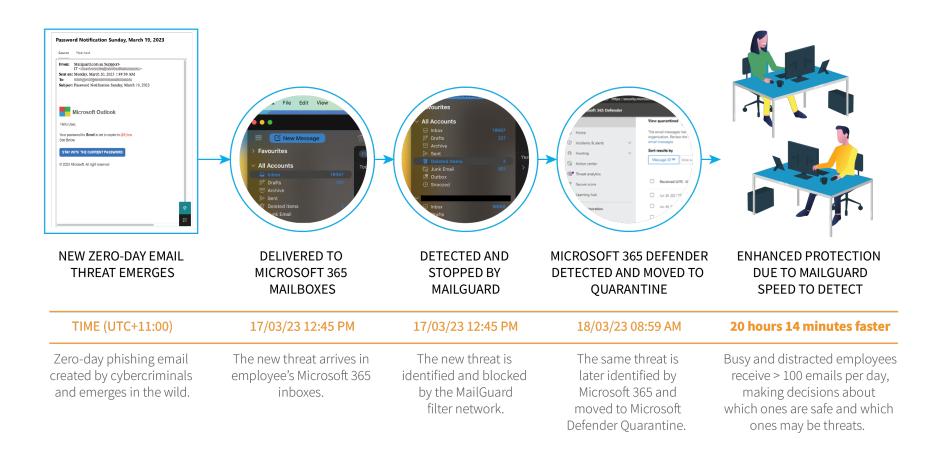
Satya Nadella
Executive Chairman & CEO

Microsoft

mailguard

DEMONSTRATED 'SPEED TO DETECT' ADVANTAGE FOR A MICROSOFT 365/ E5 CUSTOMER

Real world example:

Zero-day threat intercepted 12:45 PM 17/03 by MailGuard, and 08:59 AM 18/03 by Microsoft 365 Defender/ E5.

20 hours 14 minutes faster

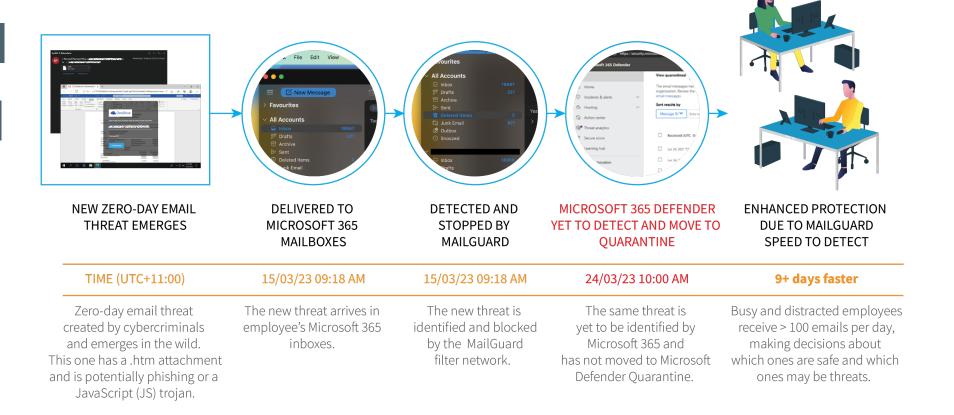|	NEW ZERO-DAY EMAIL THREAT EMERGES	DELIVERED TO MICROSOFT 365 MAILBOXES	DETECTED AND STOPPED BY MAILGUARD	MICROSOFT 365 DEFENDER DETECTED AND MOVED TO QUARANTINE	ENHANCED PROTECTION DUE TO MAILGUARD SPEED TO DETECT
TIME (UTC+11:00)		17/03/23 12:45 PM	17/03/23 12:45 PM	18/03/23 08:59 AM	**20 hours 14 minutes faster**
	Zero-day phishing email created by cybercriminals and emerges in the wild.	The new threat arrives in employee's Microsoft 365 inboxes.	The new threat is identified and blocked by the MailGuard filter network.	The same threat is later identified by Microsoft 365 and moved to Microsoft Defender Quarantine.	Busy and distracted employees receive > 100 emails per day, making decisions about which ones are safe and which ones may be threats.

mailguard

DEMONSTRATED 'SPEED TO DETECT' ADVANTAGE FOR A MICROSOFT 365/ E5 CUSTOMER

Real world example:

Zero-day threat intercepted 09:18 AM 15/03 by MailGuard, and at 10:00 AM 24/03 Microsoft 365 Defender/ E5 had yet to identify the email.

	NEW ZERO-DAY EMAIL THREAT EMERGES	DELIVERED TO MICROSOFT 365 MAILBOXES	DETECTED AND STOPPED BY MAILGUARD	MICROSOFT 365 DEFENDER YET TO DETECT AND MOVE TO QUARANTINE	ENHANCED PROTECTION DUE TO MAILGUARD SPEED TO DETECT
TIME (UTC+11:00)		15/03/23 09:18 AM	15/03/23 09:18 AM	24/03/23 10:00 AM	**9+ days faster**
	Zero-day email threat created by cybercriminals and emerges in the wild. This one has a .htm attachment and is potentially phishing or a JavaScript (JS) trojan.	The new threat arrives in employee's Microsoft 365 inboxes.	The new threat is identified and blocked by the MailGuard filter network.	The same threat is yet to be identified by Microsoft 365 and has not moved to Microsoft Defender Quarantine.	Busy and distracted employees receive > 100 emails per day, making decisions about which ones are safe and which ones may be threats.

© MailGuard Pty Ltd.

mailguard

START YOUR **FREE TRIAL** TODAY AND SEE THE RESULTS FOR YOUR BUSINESS.

EXPERT@MAILGUARD.COM.AU

mailguard