May 2023

Seller Guide:

MAILGUARD 365

mailguard365

© MailGuard 365 | Commercial in confidence. Not for distribution.

THE PROBLEM: CYBER RISK LANDSCAPE

#1 cybersecurity threat to your clients is EMAIL

- 91% of successful cyberattacks result from human error, cybercriminals go straight to the source through email.
- Phishing scams claimed four times more victims than any other cybercrime type in the U.S..
- Business Email Compromise (BEC) attacks were by far the most financially damaging, costing victims almost $2.4 billion.
- The industry is worth more than $1.2 trillion - a number expected to grow to $6 trillion by 2025.
- On average, we each receive more than 100 emails per day, so if your defenses are 99% effective, that's still a threat a day that's slipping through. And for large organisations with hundreds or thousands of employees, that's a lot of risk.
- Close to 300 billion emails are sent and received globally every day, so if 1% are threats that are slipping through the cracks, then that's 3 billion opportunities for a compromise.

Microsoft 365 (including Defender) can't stop all threats

- The spectre of a cyberattack continues to loom large for every business, and the problem is only getting worse.
- The digital threat landscape is constantly evolving, as is the scale, speed and sophistication of cyberattacks. With workforces more remote than ever, the attack surface has expanded, meaning more vectors to defend and greater vulnerability.
- Hackers are now even more relentless, thanks to ransomware-as-a-service and phishing kits, their attacks continue to be more advanced, quicker to execute, and harder to defend against.
- Plus, there are sophisticated organised crime groups, and transnational nation-state sponsored bad actors.

mailguard 365

© MailGuard 365 | Commercial in confidence. Not for distribution.

THE SOLUTION: SPECIALIST EMAIL SECURITY THAT'S UP TO 48 HOURS FASTER

MailGuard 365 – An essential email security add-on for M365

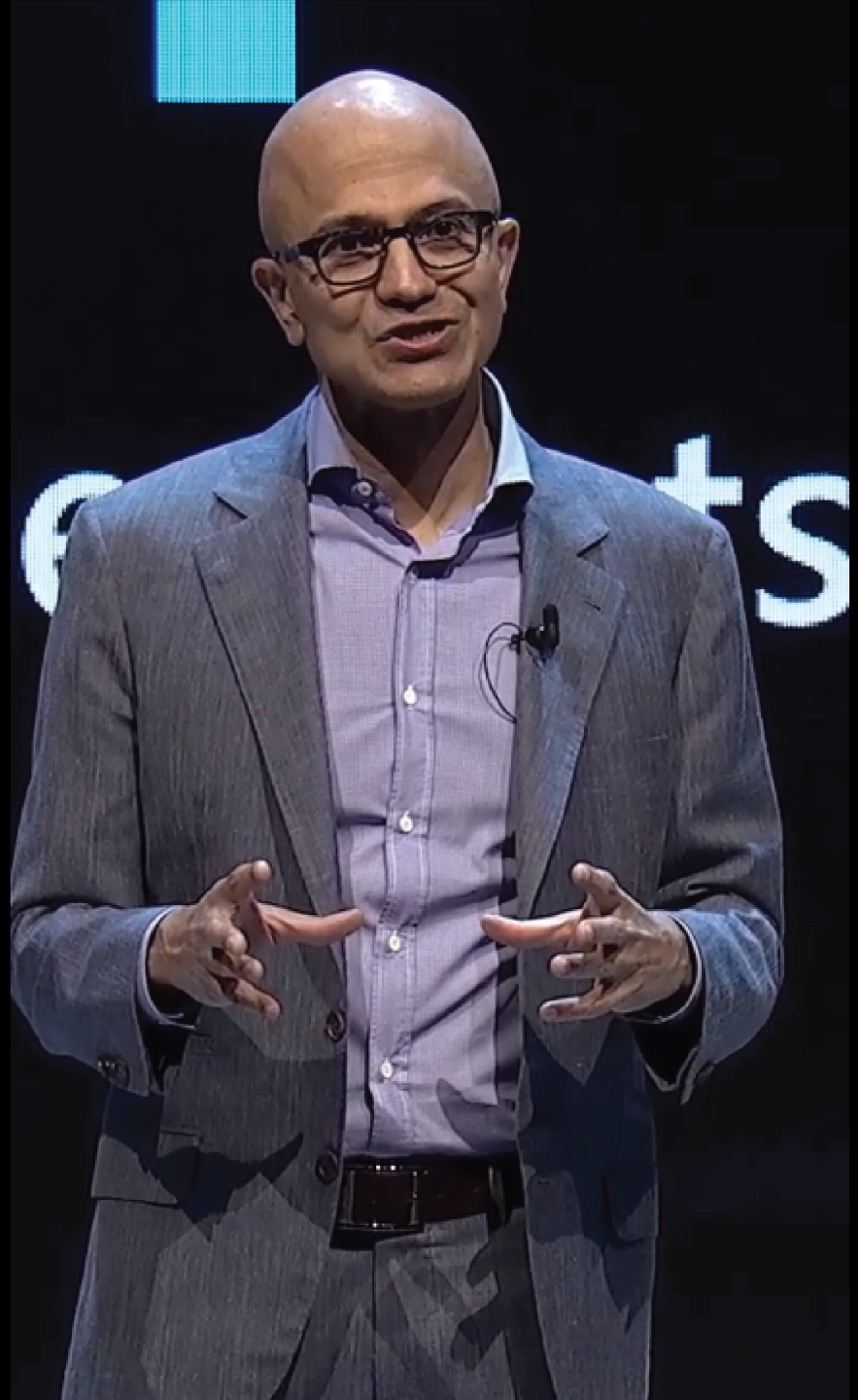
- Speed is the advantage of MailGuard 365, stopping zero-day threats up to 48 hours faster
- Stops advanced, never-before-seen email threats, like phishing, ransomware and sophisticated BEC (business email compromise) attacks
- Co-built with Microsoft engineers, adopts a 'Better Together' approach to defend 345+ million Microsoft 365 inboxes worldwide
- Combines 22+ years specialist email security expertise/ IP from MailGuard, with the best of Microsoft
- Works inside M365 to stop threats that the Microsoft security stack (including Defender) missed
- A Microsoft Marketplace 'Preferred Solution'

Frictionless, channel friendly, set up and admin

- Native M365 customer experience means threats are instantly moved to the users Junk and Deleted Items folders
- No training needed for end-users, admins or partners
- Evidence based reporting in the dashboards demonstrated the threats that are being stopped
- Set up and billing via the Microsoft tenant, in the Microsoft Partner Centre
- Transact ready in the TDS marketplace and Partner Centre
- Increase ARPU($) and reduce support overheads for partners
- MACC draw-down eligible for Microsoft Azure Customer Commitments

mailguard 365

© MailGuard 365 | Commercial in confidence. Not for distribution.



MailGuard 365, defending the Microsoft 365 ecosystem.

“It’s the type of innovation that we want to see.”

Satya Nadella
Executive Chairman & CEO

Microsoft

mailguard365

Five Common Seller Scenarios

mailguard365

© MailGuard 365 | Commercial in confidence. Not for distribution.

SCENARIO 1: MY CUSTOMER THINKS MICROSOFT EMAIL SECURITY IS ENOUGH

Every Office 365 subscription comes with security capabilities, depending on the level of the subscription, from Exchange Online Protection (EOP), through to Microsoft Defender for Office 365 Plan 1, and Plan 2.

- Employees continue to receive malicious emails in their inboxes, after M365
- 90% of businesses are impacted by phishing and malicious email attacks, despite having an email security solution like M365 in place
- MailGuard is a close partner of Microsoft, sharing threat intelligence, and partnering in engineering, sales, and marketing to protect businesses throughout the world
- Even **Microsoft, CEO, Satya Nadella** went as far as to refer to the importance of a defense-in-depth approach, acclaiming MailGuard 365 as the ***'type of Innovation that we want to see"***

Businesses are moving to the cloud and adopting Microsoft 365, but concerns remain about security, compliance, and control

- Experts agree that no one vendor solution can stop every malicious email threat, and call for a multi-vendor, defense-in-depth approach
- MailGuard 365 was co-built with Microsoft engineers to protect Microsoft 365 inboxes
- With **over 22 years accumulated specialist proprietary threat protection IP**, real-time blacklists, proprietary master rule sets, and sophisticated BEC threat detection engines, it enhances your email security
- It sits inside M365 and adopts a native approach, moving threats to Junk and Deleted Items just like Microsoft 365 does, and honours whitelists and blacklists
- **Take a 30-day free trial and see the threats that it's stopping** in the evidence-based dashboard, before making your decision

mailguard 365

© MailGuard 365 | Commercial in confidence. Not for distribution.

SCENARIO 2: MY CUSTOMER IS CONSIDERING A SEG (SECURE EMAIL GATEWAY)

Most businesses have native M365 security, and often also have a traditional secure email gateway (SEG) solution like Proofpoint or Mimecast in place.

- A traditional **SEG relies upon access to the business's mail exchange (MX) record** to operate
- It means by design they force the business to choose one solution over others, leaving the business at risk
- Microsoft allege that an upstream SEG can alter email records, **diminishing the effectiveness of the security that is native to the customer's M365** investment
- Many businesses also find the **administration of multiple vendor consoles and email quarantines burdensome, unsustainable and sub-optimal**

MailGuard 365 is collaborative by design, built with the team at Microsoft to enhance M365 email security

- Integrated Cloud Email Solutions (ICES) are the fastest growing category of email security solutions according to Gartner
- MailGuard 365 was the first ICES in the Microsoft marketplace
- **As an ICES, it is activated in the Microsoft marketplace using the business's Microsoft tenant**, and does not require access to the business's mail exchange (MX) record
- It can work seamlessly alongside other solutions in the email security stack, including Microsoft 365 and third-party SEGs
- It leverages 22+ years proprietary threat detection IP from MailGuard's SEG solution, in a modern ICES solution that works natively after M365 has done its threat analysis

mailguard 365

© MailGuard 365 | Commercial in confidence. Not for distribution.

SCENARIO 3: MY CUSTOMER IS COMPARING A BUNDLE OF VENDOR MSP SERVICES

Vendors bundle products for MSPs in an attempt to gain a greater share of wallet ($), offering the MSP convenience, but it does not always translate to the best customer outcome.

- As an example, take Acronis, best known for Backup services. It has partnered with Israeli firm, Perception Point, to include anti-malware and threat protection services in a bundle known as Cyber Protect Cloud.
- **As an MSP, you are partnered with Tech Data Synnex so that it can source and fulfil a suite of best fit solutions** at a competitive price for your customers.
- **Tech Data Synnex is recommending MailGuard 365 as the best fit solution to enhance Microsoft 365 email security**, and it is providing it to you with a generous margin.
- So, the question is, will you accept the recommendation of Acronis, who specialize in Backup, or will you take the recommendation of Tech Data Synnex?
- And, in the absence of Acronis or Tech Data Synnex, which solution would you recommend to enhance your customers Microsoft 365 email security, MailGuard 365 or Perception Point?

When comparing a bundle of services, consider what is best for the customer, and what the true costs are for you as an MSP.

- As an MSP, you must not only think about the up front margin that you will take on a sale, even though the margin offered by Tech Data Synnex for MailGuard 365 is hard to beat.
- You must also **consider the cost to serve, and the implications of a poor customer experience on your customer relationships across all services**, their trust in you, and indeed that of your entire install base.
- MailGuard 365 needs no training for customers, and no support from the partner or admins. Co-built with Microsoft, it's activated in their marketplace, with their tenant, and billed on their account. The partner has no added effort or risk.
- Plus, Microsoft themselves promote MailGuard 365 as a Microsoft Preferred Solution in their storefronts (marketplace).
- Compare that experience to Acronis and Perception Point. Who does the partner turn to if the customer is experiencing problems?
- Is the partner confident that their concerns will be resolved quickly, and who is recommending Perception Point for M365?

mailguard 365

© MailGuard 365 | Commercial in confidence. Not for distribution.

SCENARIO 4: MY CUSTOMER IS UNSURE ABOUT THE ADDED COST OVER M365?

Price will always be a factor, regardless of what service you're providing, but in cybersecurity the more important consideration is the cost of a breach or other serious cyber incident.

- The investment in Microsoft 365 is not insignificant for a business, with Business Basic starting at USD $6 user/mth, and Business Standard USD $12 user/mth. They both come with standard security built in, and for businesses that want Advanced Threat Protection (ATP) from Microsoft, the price is USD $22 user/mth for Business Premium.
- By comparison, for businesses that recognise email security as a priority, **MailGuard 365 delivers advanced threat protection for Microsoft 365 users from USD $1.60-3.00 user/mth**, depending on the number of users.

The cost of a data breach or cyber incident goes beyond the financial damages to the business, and there are also ramifications for the MSP.

- **The global average cost of a data breach is USD $4.35M**, according to IBMs 'The Cost of a Data Breach Report' 2022.
- But that's just a start. Depending on the incident, business operations may be disrupted, and there will be repercussions for customers and staff. The business will suffer reputational damage, and likely the humiliation of media coverage.
- **For the MSP, it will mean days, weeks or longer, attempting to remediate the incident**.
- The MSP will also suffer from reputational damage, with trust in their brand impacted, and there will be embarrassing questions from other customers, about their advice and services.

mailguard 365

© MailGuard 365 | Commercial in confidence. Not for distribution.

SCENARIO 5: MY CUSTOMER WANTS AN ADMIN CONSOLE AND EMAIL QUARANTINE

The traditional paradigm for specialist email filtering to protect against advanced threats, is the secure email gateway (SEG), which allows an admin and/or partner to configure a console and rule sets to improve performance.

- Many industry professionals now find the SEG model to have limitations.
- To implement a multi-layered, multi-vendor, defense-in-depth approach means **with an SEG the business, its partners and admins must monitor several systems and administer those email quarantine queues**.
- An SEG also **requires access to the mail exchange (MX) record creating physical limitations on the number of solutions in the security stack**.
- And **Microsoft suggest that upstream filtering (SEGs) sometimes amend the email record making their security/ protection less effective**.

The limitations of the traditional SEG are fuelling a trend towards Integrated Cloud Email Security Solutions (ICES), acknowledged by Gartner as the highest growth segment in email security.

- **MailGuard 365 is a first-mover in the ICES category**, as the first such solution in the Microsoft marketplace.
- Speed is still the advantage of MailGuard 365, stopping advanced threats up to 48 hours faster.
- It was co-built with Microsoft engineers to work inside Microsoft 365, after Microsoft has done its own analysis.
- It requires no additional effort from admins or partners to administer a console or quarantine, and no training for end-users.
- MailGuard 365 enhances Microsoft 365 email security, honouring blacklists and whitelists.
- And **evidence-based reporting in real-time MailGuard 365 dashboards enable businesses to see the threats that are being stopped, and targeted users**.

mailguard 365

© MailGuard 365 | Commercial in confidence. Not for distribution.

Solution/ Segment Comparison

mailguard365

© MailGuard 365 | Commercial in confidence. Not for distribution.

SOLUTION COMPARISON (1 OF 2)

Feature		Description	Other API Solutions	Microsoft Defender (E5)	MailGuard 365
Critical Features	Accumulated Specialist Proprietary Threat Protection IP (Since 2001)	MailGuard 365 leverages 22+ years of specialist cloud email security intellectual property (IP), incorporating incremental enhancements and historical datasets. This specialisation allows MailGuard 365 to proactive and real time threat detection, up to 48 hours ahead of rivals.	x	x	✓✓✓
	Proprietary Master Rule Set for Email Management	Specially developed, ingrained rule sets enable global customer protection.	x	x	✓✓✓
	Proprietary Real time Blacklists	MailGuard 365 utilises best of breed commercial data feeds, partnered with real time in house, advanced globally located data sources, to build superior real time blacklists.	x	x	✓✓✓
	Proprietary Sophisticated BEC Threat Detection Engines	Automated analysis of multiple meta's using predictive algorithms, are combined with human intelligence vectors based on 22+ years of R&D.	x	x	✓✓✓
Provisioning	Automated Deployment via Microsoft	1-Click Scalable, Immediate Activation via Microsoft AppSource, Azure Marketplace or Microsoft CSP Marketplace	x	✓✓✓	✓✓✓
	No DNS changes required	Hackers are unable to determine the email security service used by an organization	✓	✓✓✓	✓✓✓
	Ease of evaluation	Free 30 day trial, with evidence based reporting	x	✓✓✓	✓✓✓
	Ease of provisioning	No additional setup/configuration required	x	x	✓✓✓
	Enterprise Scalability	Built with scalability in mind to protect all current and future Office 365 mailboxes	✓	✓✓✓	✓✓✓
	Unified Billing via Microsoft/Partner	Billing is done through exiting agreements through Microsoft/Partner	x	✓✓✓	✓✓✓
Protection	True In-Depth Defence (Multiple Layers)	Integrates and enhances any existing security stack, without negating learning and reporting mechanisms that could miss emails	✓	✓✓✓	✓✓✓
	Detection Speed	Threats detected and stopped in milliseconds	✓✓	✓✓	✓✓✓
	Detection Accuracy	Best in class detection rate, with near zero missed detections	✓✓	✓✓	✓✓✓
	Zero Day Detection	Upto 48 hours ahead of competitors with zero day threats	✓✓	✓✓	✓✓✓
	Malicious URL Detection	Scans URLs in real-time to detect malicious links using best in class internal and external threat trackers	✓✓	✓✓	✓✓✓
	Malicious Document Detection	Scans attachments in real-time to detect malicious files using best in class internal and external threat trackers and anti-malware engines	✓✓	✓✓	✓✓✓
	Phishing Protection	Not as an add-on, MailGuard 365 is an all in, email security specialist that defends against the zero hour threats including sophisticated phishing attacks, including social engineering, domain spoofing and spear phishing.	✓✓	✓✓	✓✓✓
	Spam & Greymail	Defends against spam and greymail	✓✓	✓✓	✓✓✓

mailguard 365

© MailGuard 365 | Commercial in confidence. Not for distribution.

SOLUTION COMPARISON (2 OF 2)

	Feature	Description	Other API Solutions	Microsoft Defender (E5)	MailGuard 365
BEC & Social Engineering	Compromised Account Detection	Administrators can see which accounts are targetted and/or sending out threats internally or externally	✓✓	✓✓	✓✓✓
	Internal Attack Detection	Scans and detects threats transmitted in internal emails	✓✓	✓✓	✓✓✓
	Brand Impersonation Detection	Advanced engines with awareness around major brands, to detected spoofing or impersonation attempts	✓✓	✓✓	✓✓✓
	Vendor & Supply Chain Compromise	Real-Time detection of threats from compromised vendors with automated threat trackers	✓✓	✓✓	✓✓✓
	Context Aware Protection	Engines developed specifically to monitor mailbox attributes and detect suscicious activity	✓✓	✓✓	✓✓✓
	Wholistic Approach to BEC	Not as an add-on, MailGuard 365 is an all in, email security specialist that defends against the zero hour threats including sophisticated phishing attacks, including social engineering, domain spoofing and spear phishing.	x	x	✓✓✓
Simplified Administration	Easy of Use	MailGuard 365 is a pure set and forget service, specifically designed for low interaction with no complex portal to navigate	x	x	✓✓✓
	No training required for Admins	MailGuard 365 is a pure set and forget service, specifically designed for low interaction with no complex portal to navigate	x	x	✓✓✓
	No trainings required for End Users	MailGuard 365 is a pure set and forget service, specifically designed for low interaction with no complex portal to navigate	x	x	✓✓✓
	Real-Time Reporting & Analytics	MailGuard 365 provides real-time evidence based reporting illustrating threats which have bypassed an organisation's entire security stack	x	✓✓✓	✓✓✓
	Unified Interface for Threat Management	Single, easy to use interface for reporting, analytics and remediation	x	x	✓✓✓
	Honor Microsoft 365 Policies	MailGuard 365 integrated deeply into Microsoft 365 by honoring exiting rules and configurations done in Microsoft 365, to further simply administration	x	✓✓✓	✓✓✓
	Honor Microsoft 365 Blacklists and Whitelists	MailGuard 365 integrated deeply into Microsoft 365 by honoring exiting rules and configurations done in Microsoft 365, to further simply administration	x	✓✓✓	✓✓✓
	Automated treatment of False-Positives and False-Negatives	Automated learning of false positive and false negative through end user signals	x	✓✓✓	✓✓✓
Remediation	Auto-Remediation	Automated remediation of threats with no manual review required	x	✓✓✓	✓✓✓
	Post-Delivery Protection	Advanced post delivery detecting for highly sophisticated threats that evaded detection	x	✓✓✓	✓✓✓
	Deep-Dive	As an add-on, MailGuard 365 provides historical scanning and remediation	x	x	✓✓✓
	Investigations and Reports	Detailed investigation and search capabilities, including remediation actions via the administration console	x	✓✓✓	✓✓✓

mailguard 365

© MailGuard 365 | Commercial in confidence. Not for distribution.

Speed to Detect is the Difference

mailguard365

© MailGuard 365 | Commercial in confidence. Not for distribution.

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

MailGuard think every second matters.

That's why they co-built MailGuard 365 with Microsoft, designed to sit inside Microsoft 365 to stop threats that have evaded a business's upstream defenses. Because experts recommend a cybersecurity 'mesh' approach to protect your business.

And, it's why they developed the 'Speed to Detect Scorecard', to demonstrate how much faster MailGuard 365 identifies and blocks advanced, malicious, zero-day threats.

Because MailGuard 365 is proven to stop threats up to 48 hours faster.*



mailguard 365

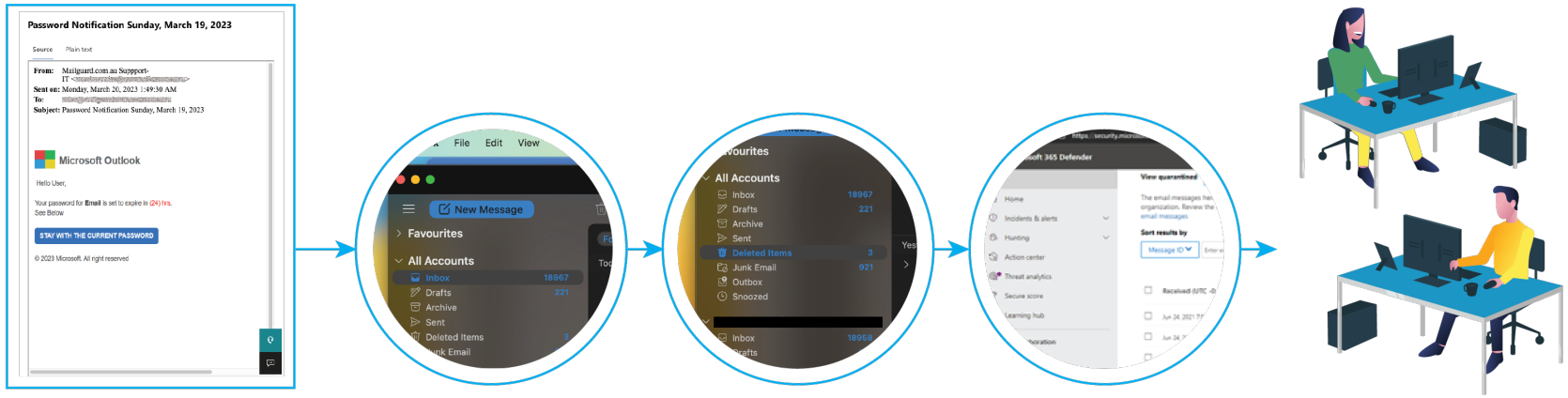
© MailGuard 365 | Commercial in confidence. Not for distribution.

DEMONSTRATED SPEED TO DETECT ADVANTAGE FOR M365/E5 CUSTOMERS

Real world example:

Zero-day threat intercepted 12:45 PM 17/03 by MailGuard 365, 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 365	MICROSOFT 365 DEFENDER DETECTED AND MOVED TO QUARANTINE	ENHANCED PROTECTION DUE TO MAILGUARD 365 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 by MailGuard 365 and moved to Deleted Items or Junk.	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.

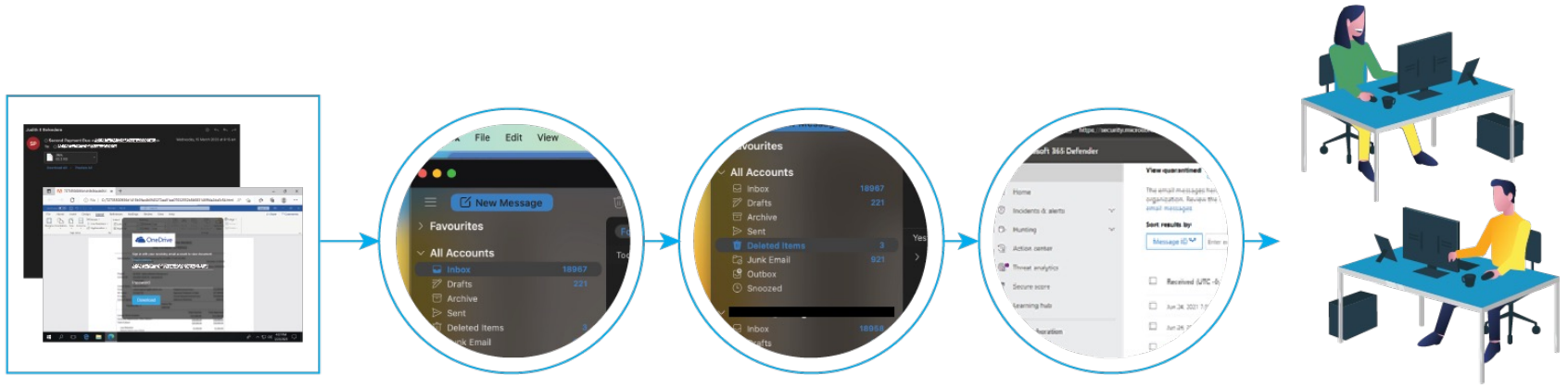
mailguard 365

© MailGuard Pty Ltd.

DEMONSTRATED SPEED TO DETECT ADVANTAGE FOR M365/E5 CUSTOMERS

Real world example:

Zero-day threat intercepted 09:18 AM 15/03 by MailGuard 365, 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 365	MICROSOFT 365 DEFENDER YET TO DETECT AND MOVE TO QUARANTINE	ENHANCED PROTECTION DUE TO MAILGUARD 365 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 by MailGuard 365 and moved to Deleted Items or Junk.	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 365

© MailGuard Pty Ltd.

mailguard365

© MailGuard 365 | Commercial in confidence. Not for distribution.