ACRONIS-POWERED. SOTERIA CLOUD DELIVERED.

How to respond to phishing and malicious email trends

Turn blocked threats, risky users, mailbox compromise concerns, and recovery actions into a repeatable buyer-facing response workflow.

Buyer-ready **Operational evidence** **Total Data Protection**

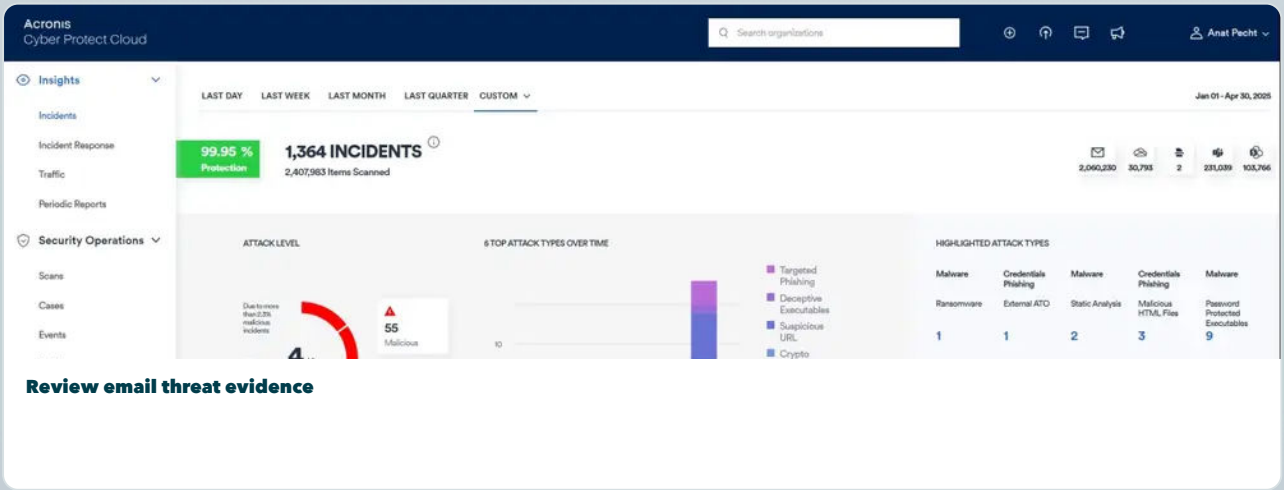
BEST FIT

MSPs, resellers, IT leaders, security teams, and Microsoft 365 customers managing email risk.

The buyer sees phishing activity or mailbox compromise risk and needs a practical response beyond a dashboard screenshot.

Acronis **Powered by Acronis**

Soteria Cloud delivered



Review email threat evidence

BUYER NEED

Make the commercial requirement operational.

Email remains a common entry point for cyber incidents, so buyers expect prevention, response, user risk visibility, and recovery alignment.

BUYER TRIGGER

The buyer sees phishing activity or mailbox compromise risk and needs a practical response beyond a dashboard screenshot.

PRODUCTS INVOLVED

Advanced Email Security, Microsoft 365 Protection, EDR, Security Awareness Training, MDR

CONSOLE SURFACES

Email Security, Reports, Audit log, Executive summary

01

Do not review email security in isolation; connect it to identity, endpoint, and SaaS recovery risk.

02

High-risk users need different review and coaching from the general user population.

03

Blocked threats still matter because they show targeting patterns and buyer exposure.

04

Mailbox restore expectations should be clear before a compromise or mass deletion event.

05

Use trend evidence to justify security awareness or stronger controls.

06

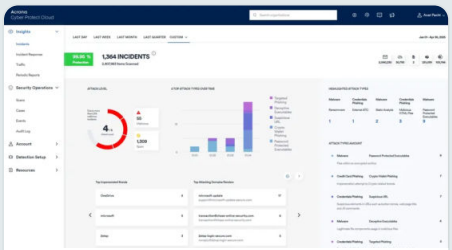
Escalate repeated targeting against finance, executive, or admin users.

PRACTICAL PATH

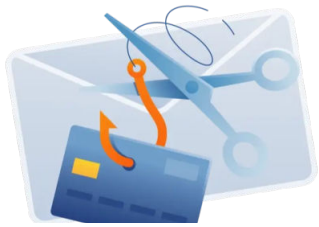
Turn the offer into a repeatable service motion.

Soteria Cloud positions Acronis technology around buyer outcomes, support ownership, recurring review, and evidence that can be explained without product jargon.

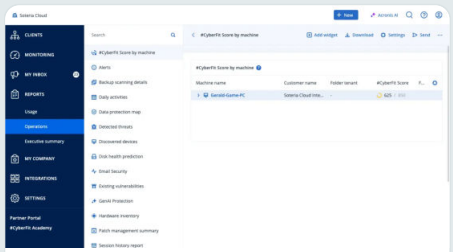
REVIEW THREAT PATTERNS	Check phishing, malicious URLs, malware, impersonation, and attachment trends by user group and customer.
IDENTIFY HIGH-RISK USERS	Focus on executives, finance, admin users, shared mailboxes, and users with repeated exposure or risky behavior.
ALIGN RESPONSE	Define when to quarantine, block, investigate, reset credentials, check endpoints, restore mailbox data, or escalate.
CONNECT RECOVERY	Confirm Microsoft 365 backup and mailbox restore options for malicious deletion, overwrite, or account compromise scenarios.
REPORT ACTIONS	Show blocked threats, risky users, controls changed, training needs, recovery readiness, and unresolved exposure.



Review email threat evidence



Explain phishing protection in buyer language



Turn threat activity into review evidence

BUYER OUTCOME

Turn blocked threats, risky users, mailbox compromise concerns, and recovery actions into a repeatable buyer-facing response workflow.

EVIDENCE

Show the proof buyers expect to see.

Soteria Cloud service reviews give buyers visible status, known exceptions, agreed actions, and a reviewable record of protection activity.

Evidence to keep

- Threat category trend
- High-risk user list
- Policy changes
- Mailbox recovery readiness
- Training or escalation actions

Measures to review

- Phishing attempts blocked
- Repeat-risk users reduced
- Policy exceptions closed
- Mailbox recovery scenario validated
- Executive risk trend reviewed

01 **Phishing attempts blocked**

02 **Repeat-risk users reduced**

03 **Policy exceptions closed**

04 **Threat category trend**

05 **High-risk user list**

06 **Policy changes**