

SOTERIA CLOUD ADVANCED EMAIL SECURITY

How to reduce phishing and business email compromise risk

Protect the inbox as the first line of everyday cyber risk for Microsoft 365 and Google Workspace users.

Email threat protection

Acronis Advanced Email Security

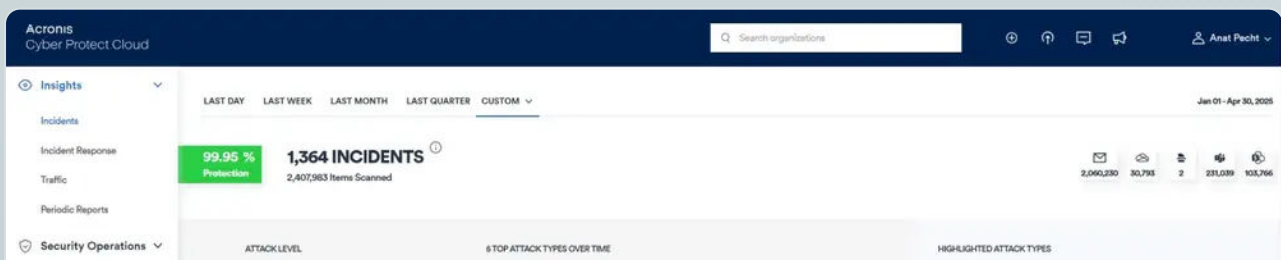
Total Data Protection

BEST FIT

Businesses, MSPs, and resellers protecting email users from phishing, malicious links, impersonation, and credential theft.

Email remains the easiest way for attackers to reach users, steal credentials, and trigger wider business disruption.

Acronis Powered by Acronis



DECIDE FIRST

Make the business choices clear before rollout.

Useful protection starts with the workloads, users, data, recovery targets, and risk decisions that shape the service.

01

Which users are most exposed to payment or credential attacks

02

How suspicious messages are reviewed and escalated

03

What controls apply to links and attachments

04

How impersonation and spoofing risk is handled

05

How mailbox protection connects to SaaS backup

06

Which trends leadership needs to see

Readiness checklist

- Identify finance, executives, HR, and privileged users
- Review Microsoft 365 or Google Workspace mail flow
- Set phishing, URL, attachment, and impersonation policies
- Confirm mailbox backup and recovery coverage
- Report blocked threats and repeated risk patterns

Gaps to close

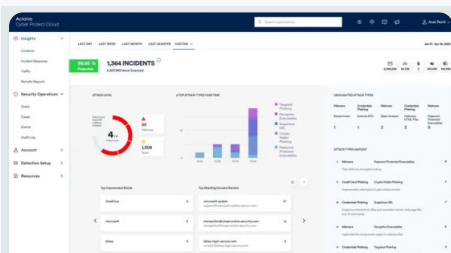
- Email security treated separately from data recovery
- High-risk users protected the same as everyone else
- No visibility into business email compromise trends
- Mailbox recovery excluded from security planning

PRACTICAL PATH

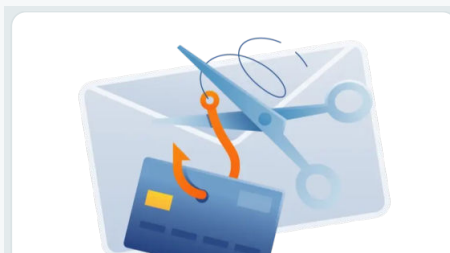
Turn the requirement into an operating model.

Soteria Cloud surrounds Acronis technology with assessment, policy design, onboarding, review, and support ownership.

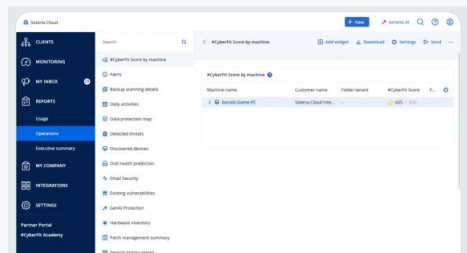
PROFILE RISKY USERS	Map departments and roles most likely to receive payment, credential, or impersonation attacks.
APPLY LAYERED CONTROLS	Protect against phishing, malicious links, attachments, spoofing, and account takeover signals.
CONNECT SAAS RECOVERY	Align email security with Microsoft 365 or Google Workspace backup coverage.
REVIEW INCIDENTS	Use blocked threats and suspicious messages to refine policies and target user awareness.
REPORT TRENDS	Show executives where email risk is falling, where it persists, and what actions remain open.



Review inbound threat evidence



Explain phishing protection to buyers



Track security reporting

SOTERIA CLOUD OFFER

Soteria Cloud Advanced Email Security

POWERED BY

Acronis Advanced Email Security

SERVICE FIT

Best for buyers that want email threat protection tied to SaaS data resilience and clear risk reporting.

OUTCOME

Reduce phishing and malicious email exposure. The plan is stronger when controls, recovery expectations, and reporting evidence are connected from the start.



EVIDENCE

Measure the things that prove protection is working.

Good cyber resilience is visible. Buyers need coverage, exceptions, recovery confidence, and service actions they can understand.

01

High-risk mailboxes protected

02

Phishing and malicious messages blocked

03

Impersonation attempts detected

04

Mailbox backup coverage

05

Repeated-risk users reviewed

Business outcomes

- Reduce phishing and malicious email exposure
- Improve protection for everyday collaboration
- Connect email security with backup and recovery planning

Strong fit scenarios

- Microsoft 365 email security uplift
- Google Workspace email protection
- Security bundle for backup customers

SOTERIA CLOUD

All your data. One strategy. Zero compromise.

Protect inboxes from phishing, malicious links, account takeover risk, and business email compromise. Delivered with Soteria Cloud onboarding, support, reporting, and recurring review.