HOW-TO

SOTERIA CLOUD ADVANCED EMAIL SECURITY

# How to reduce phishing and malicious email exposure

**Protect inboxes from phishing, malicious links, account takeover risk, and business email compromise.**

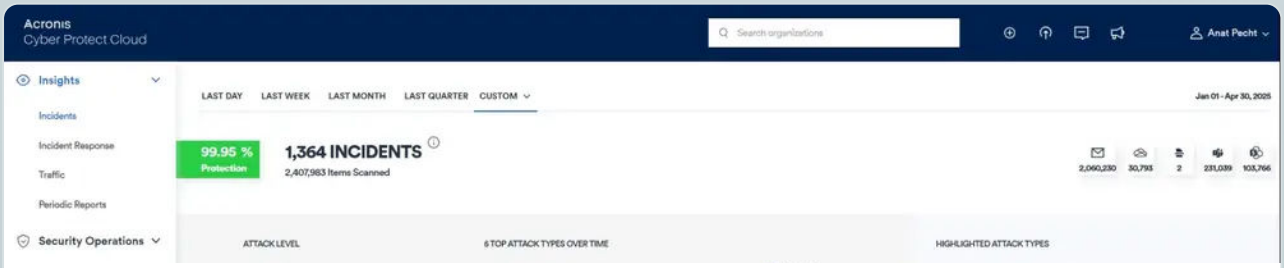
Email threat protection | Acronis Advanced Email Security

STARTING POINT

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

For Microsoft 365 and Google Workspace customers where email is still the most common attack path.

Acronis Powered by Acronis | Microsoft | Google Workspace




Email security dashboard and detection evidence

STEP-BY-STEP PATH

# Move from scope to validated service without losing the buyer's objective.

These are the decisions and checks Soteria Cloud uses to turn Acronis Advanced Email Security capability into a practical service outcome.

| | |
|---|---|
| **01 Confirm mail flow** | Identify Microsoft 365 or Google Workspace mail domains, user groups, and high-risk roles. |
| **02 Set policies** | Apply phishing, malicious URL, attachment, impersonation, and quarantine controls. |
| **03 Validate detection** | Review inbound incidents, false positives, and blocked-threat evidence. |
| **04 Align recovery** | Confirm SaaS backup and account recovery plans for mailbox compromise scenarios. |
| **05 Review trends** | Use reports to show threat patterns, policy exceptions, and actions for the next review. |

KEY OUTCOME

**Reduce phishing and malicious email exposure. The service is shaped around the workloads, users, data, and risk profile that matter most.**

TECHNOLOGY FOUNDATION

**Acronis Advanced Email Security**

PROTECTION FOCUS

**Email threat protection**

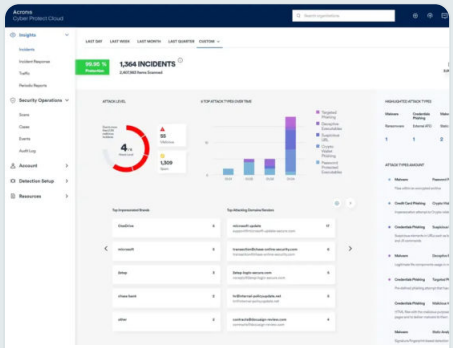
SERVICE OWNER

**Soteria Cloud**

SCREEN CUES

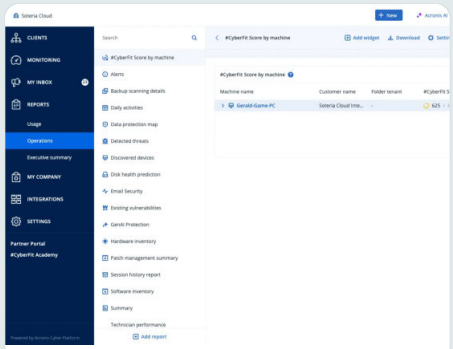
# Use the console views to confirm progress and explain the service clearly.

Protect inboxes from phishing, malicious links, account takeover risk, and business email compromise. The screens below help buyers understand where scope, controls, and reporting evidence come from.



**Review inbound threat evidence**

**Explain phishing protection to buyers**



**Track security reporting**

**Email threat protection scope has named owners and clear exclusions.**

**Required administrator access and customer approvals are confirmed.**

**Policies match the workload, user, data, and recovery risk profile.**

**Reports show coverage, exceptions, and action owners in plain language.**

**Soteria Cloud review rhythm is agreed for changes, incidents, and renewals.**

BUYER CHECKPOINT

**Before expanding the service, confirm that the buyer can see what is protected, what is excluded, what needs action, and how Soteria Cloud reports improvement.**

OPERATIONAL FIT

# Clear coverage, visible progress, and support when it matters.

The result is a protection approach customers can understand, fund, and measure through recurring Soteria Cloud reviews.

01

**Reduce phishing and malicious email exposure**

02

**Improve protection for everyday collaboration**

03

**Connect email security with backup and recovery planning**

### Controls to put in place

- Anti-phishing protection
- Malicious URL and attachment defense
- Business email compromise protection
- Account takeover risk reduction
- Email security policy controls
- User and admin reporting

### Strong fit scenarios

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

SOTERIA CLOUD

## Protection should be operational, not theoretical.

Soteria Cloud brings Acronis-powered capability together with onboarding, support, and recurring review.