eSENTIRE

ATLAS PLATFORM

Atlas Email Security

Email Detection & Response inside Atlas, powered by Sublime.

One Email Is Still All It Takes.

A convincing invoice. A fake IT ticket. A QR code that opens a fake login page. Attackers don't need an exploit when an inbox will do, and AI now takes minutes to write a fresh version of a lure that worked.

Most teams protect email in one tool and everything else in another. By the time a log reaches the SOC, the message has been opened and the link clicked. Atlas Email Security closes that gap. Email Detection & Response runs on the same platform, with the same experts, as the rest of your defense.

5x
increase in AI signals found in email attacks
Sublime Security, 2026 Email Threat Research Report

1,450%
year-over-year rise in email bombing and IT impersonation
eSentire, 2026 Threat Report

389%
year-over-year rise in account compromise
eSentire, 2026 Threat Report

What Atlas Email Security Delivers

Caught On Arrival

- Credential phishing, BEC, and malware
- Callback, QR-code, and calendar-invite phishing
- Email bombing

Evidence You Can Check

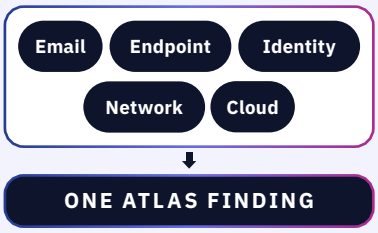
- An Attack Score on every flagged email
- The detection logic behind each verdict
- The same evidence our analysts see

Cleaned Up Everywhere

- A threat, or the whole campaign, pulled from every mailbox it reached
- User Reported Phishing investigated, answered and removed

The Whole Attack, in One Finding.

A phishing email is rarely the whole story. Atlas investigates every email alert alongside your endpoint, identity, network and cloud activity, so our analysts see the message, the click and the login that followed in one place. That's the difference between deleting an email and stopping an attack.



How It Works

1. **Connect**
   We connect to Microsoft 365 over API. No MX records, no rerouting, no gateway changes.
2. **Tune**
   Together, we set exclusions and which threats are removed automatically.
3. **Detect**
   Each message is read for intent, sender behavior, links, attachments and images as it lands.
4. **Investigate**
   Atlas AI and our analysts evaluate each alert with the rest of your telemetry.
5. **Respond**
   We pull the message, or the whole campaign, from every inbox, using the response rules you set. Every action is logged.

5
Sources in one Atlas Finding: email, endpoint, identity, network and cloud

2 weeks
Typical onboarding, from kickoff to protected

24/7
Expert SOC on every alert

Email Security Is Not Just a Log Source

	EMAIL AS A LOG SOURCE	ATLAS EMAIL SECURITY
Who catches it	Your email tool, on its own	Atlas, with our SOC watching
Why it was flagged	A verdict you have to trust blindly	The evidence behind each verdict
When one gets through	Your team hunts down every copy	We pull every copy, from every mailbox
The rest of the attack	Investigated somewhere else, if at all	Same Finding as endpoint, identity and cloud
Reported phishing	Piles up in an abuse mailbox	Investigated by our SOC, with an answer back



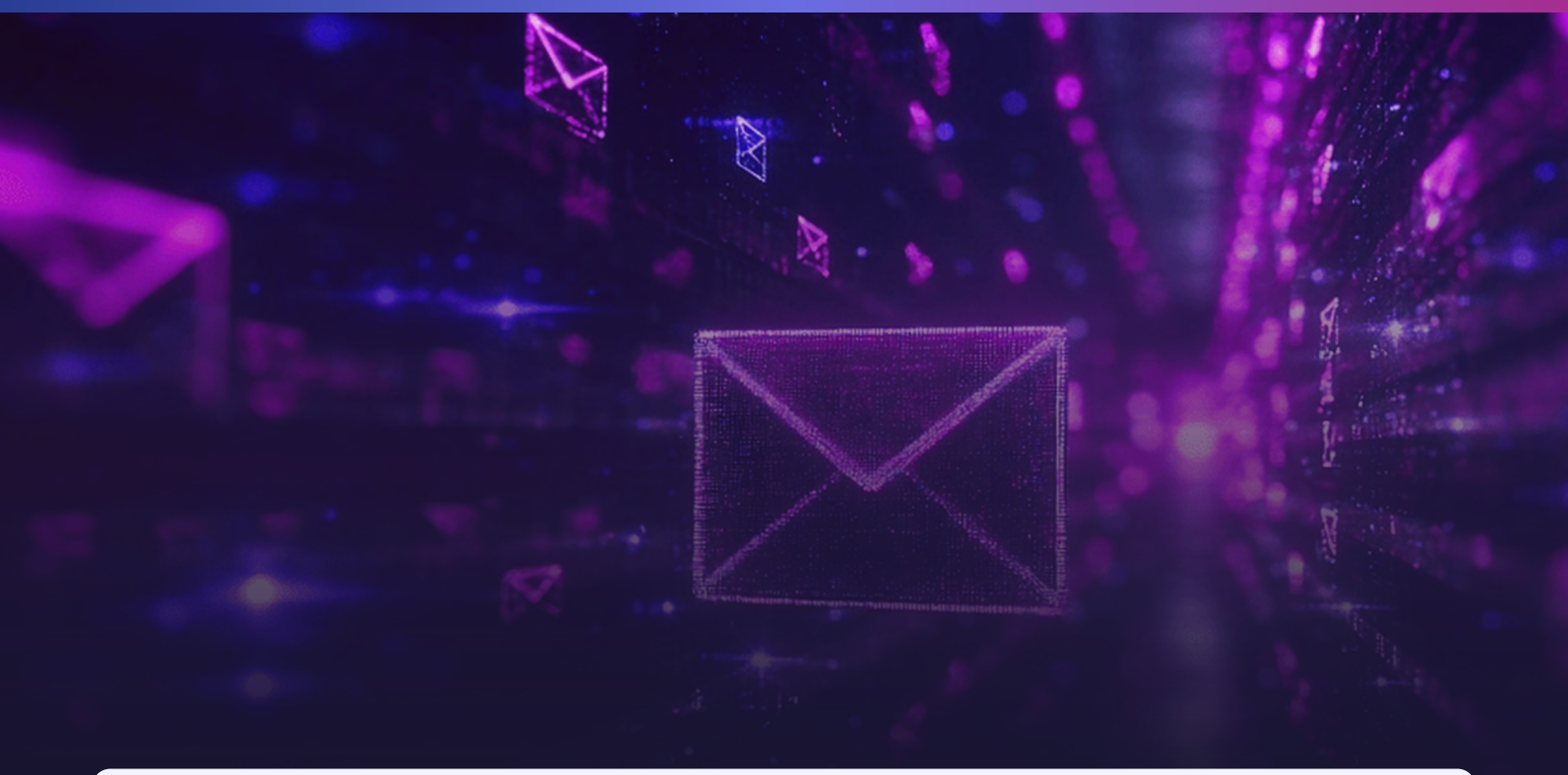
Built Around Your Email Stack.

- Connects to Microsoft 365 over API, with no mail-flow changes
- Can augment Microsoft Defender for Office 365, or run without it
- Runs alongside the email gateway you already own, or replaces it
- Google Workspace coming soon



You Stay in Control.

- Your admins keep allow lists, exclusions and quarantine release
- We own the integrations and watch the platform
- You call us for support, not the vendor
- Our analysts never log in to your mailboxes



See What's Getting Through.

Atlas Email Security is available as an add-on to any Atlas Package.

LET'S TALK SECURITY →

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US 1-866-579-2200

"We look at eSentire to be the experts. We trust them implicitly. They're with us through the thick and thin till the end."

CISO, Financial Services GARTNER PEER INSIGHTS

Thousands of organizations in **90+** countries | **25** years of SOC expertise | **2M+** endpoints protected | **Leader**, IDC Marketscape for MDR

eSentire is a leader in Controlled Autonomy SecOps, protecting thousands of organizations in 90+ countries across 35+ industries. Founded in 2001, the company's Controlled Autonomy SecOps operating model pairs agentic AI operatives with engineered human-judgment controls, delivering expert-depth security outcomes at machine speed without ceding accountability to opaque automation. Powered by the unified agentic AI Atlas Platform, eSentire's Atlas AI + 24/7 expert human SOC coverage delivers offensive capabilities that preempt exposures before attackers do, detect, and respond to stop threats in real time. For more information, visit **www.esentire.com** and follow **@eSentire**.