EMAIL SECURITY OVERVIEW

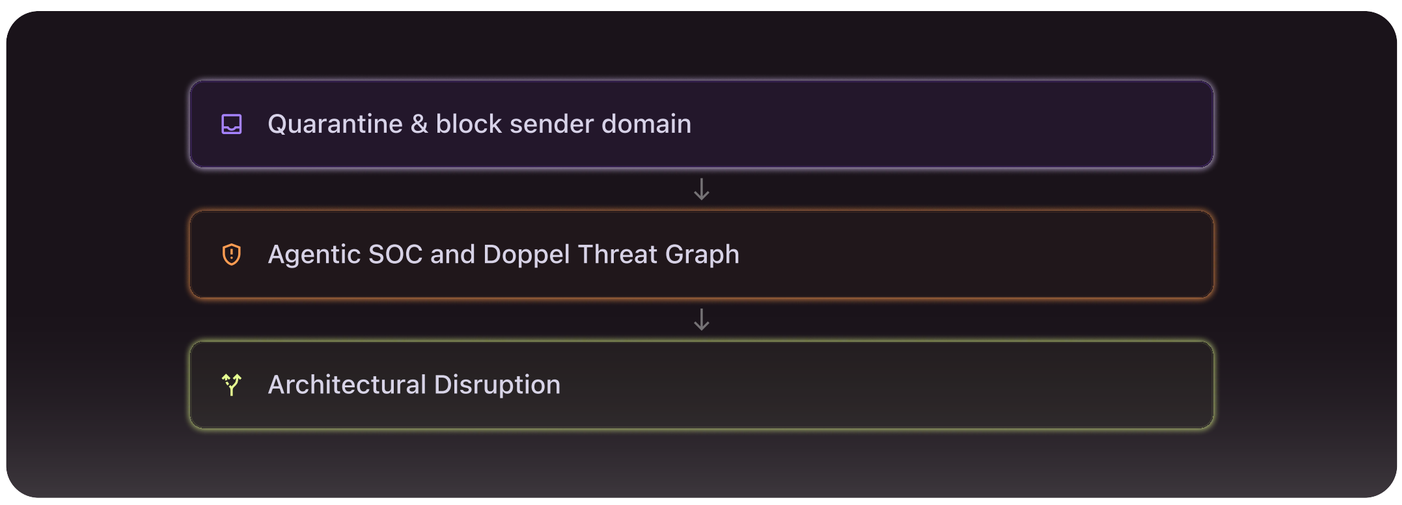
Doppel

Introducing Doppel Email Security

Agentic email security built on external attack infrastructure intelligence.

How Doppel Email Security Works

Doppel Email Security inspects every delivered message, evaluates it for malicious content or intent, links the threat to the external attacker infrastructure mapped by the Doppel Threat Graph, and takes that infrastructure down, so the campaign can't retarget your organization.



Intelligence Layer

Incorporates external infrastructure context (DNS registrations, certificates, multi-channel indicators), tracked in real time and surfaced through clear, human-readable detection logic.

Detection Stack

Deploys via API on Microsoft 365 and Google Workspace with zero mail-flow rewrites.

The Takedown Engine

Executes machine-speed takedowns of sending domains and malicious links.

Core Capabilities

External Infrastructure Sourcing

Brings real-time external attacker infrastructure intelligence directly into inbox analysis to catch novel attacker tactics and generative AI lures that lack behavioral baselines.

Disruption Through Targeted Takedowns

Moves beyond simple quarantine by executing machine-speed takedowns on the sending infrastructure and malicious domains behind every phish.

Capacity Scaled by the Agentic SOC

Replaces static blackbox models and YARA rule sprawl with natural-language detection policies and investigations, continuously tuned 24/7 by autonomous AI agents for a fully self-healing solution.

Closed-Loop Ecosystem

Integrates directly with Digital Risk Protection and Human Risk Management. External intelligence fuses with internal telemetry, and every phish immediately informs simulation and training.

Measurable Email Security Outcomes

Stop the Campaign, Not Just the Email

Eliminates repeat incidents and degrades attacker return on investment by dismantling the underlying infrastructure, not just individual messages.

Scale the SOC Without Headcount

Automates noisy triage queues and investigations across mailboxes, reducing in manual security operations workload and offering clear, human-readable detection logic and investigations.

Catch Novel and Polymorphic Attacks

Catches hyper-personalized social engineering tactics, polymorphic attacks, and unmapped threat pathways while maintaining business continuity with fewer false positives.

Cross-Channel Visibility

Connects the dots across multiple communication channels to uncover hidden threats. By analyzing the bigger picture, the system recognizes that when minor, seemingly harmless indicators appear across different surfaces simultaneously, the combined pattern reveals a highly coordinated campaign, even if the email itself looks clean.

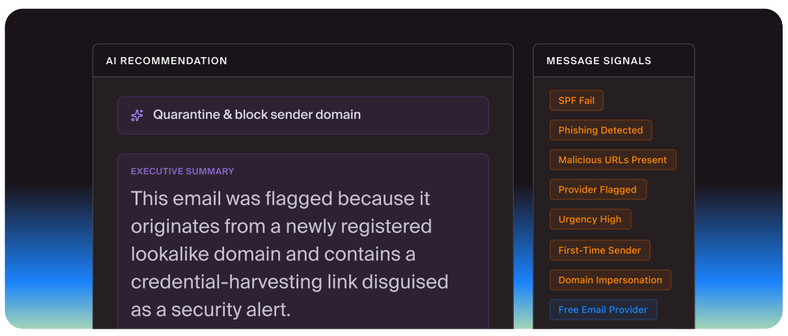
EMAIL SECURITY OVERVIEW

Doppel

The Email Security Architecture

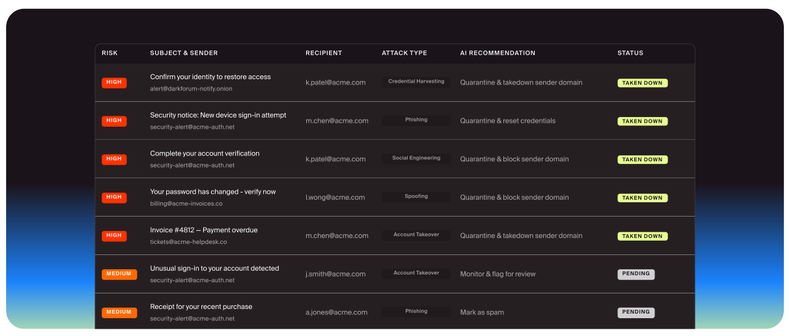
Doppel Email Security converges real-time external threat intelligence with active inbox defense, moving email security from a reactive filter to a continuous loop of campaign disruption.

Architectural Pillars of Disruption



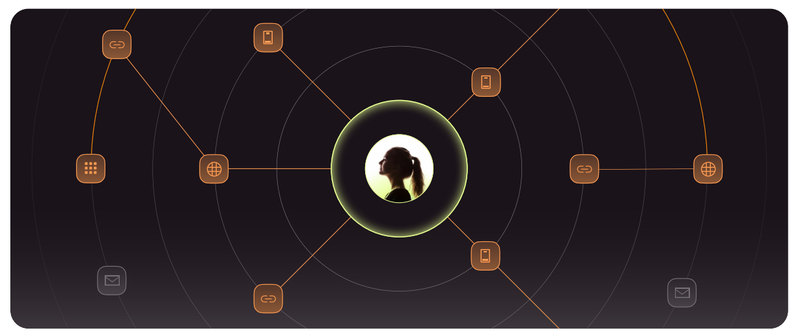
Threat Graph Correlation

The architectural backbone linking delivered emails directly to live domain registrations, hosting networks, and multi-channel indicators. Instead of evaluating phish in isolation, the system identifies the full threat footprint before an employee clicks.



Agentic Detection Stack

Driven by human-readable natural-language policies. AI agents dynamically inspect content and sender behavior, continuously updating defensive postures to eliminate rule sprawl and detection drift.



Multichannel Infrastructure Disruption

The remediation layer extends outside the perimeter. When a phish is verified and quarantined, automated workflows trigger takedowns against the registrars, hosting environments, and networks hosting the exploit infrastructure.

Technical Integration and Stack Alignment

API-Native Cloud Deployment

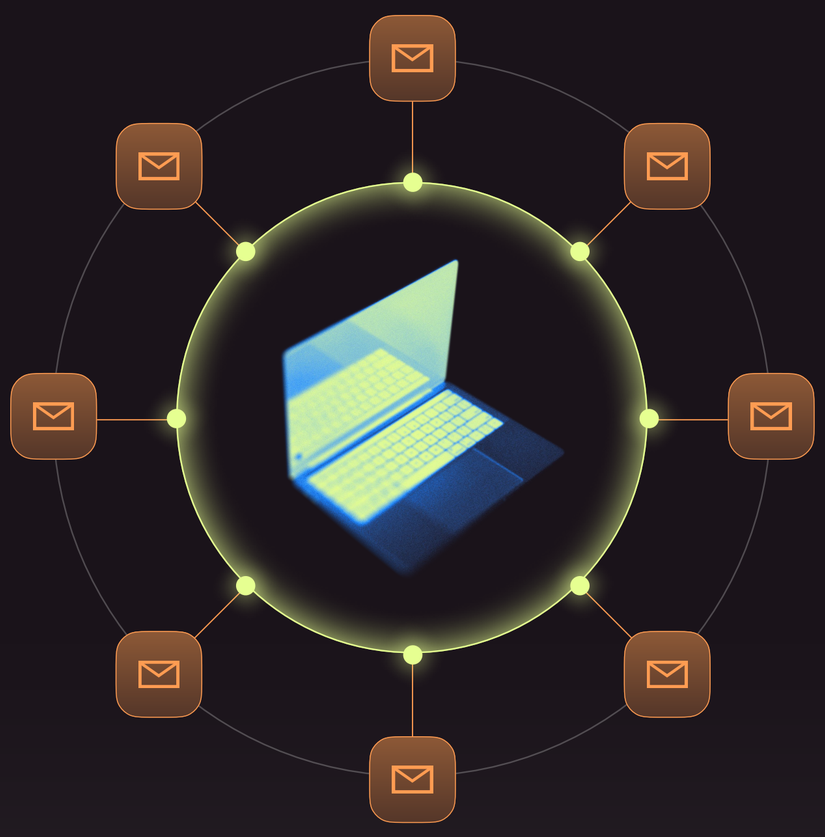
Connects directly to Microsoft 365 and Google Workspace through native cloud APIs. This design choice ensures operational stability, completely bypassing the need for disruptive MX record changes or mail-flow modifications. Doppel Email Security can sit alongside a SEG or native email security tool.

Threat-to-Simulation Feedback

Closes the loop between technical infrastructure defense and human risk. Live campaign data captured by the inbox layer is automatically translated into realistic, just-in-time employee simulations and training.

Shared Threat Graph Contribution

Every infrastructure takedown initiated by a single mailbox signal enriches the global database, immediately protecting all endpoints across the entire unified platform network.



Book your demo at doppel.com/request-a-demo-email-security