sublime | VALIMAIL a digicert company

# Preventing modern email attacks and impersonation

## with Sublime + Valimail

### Modern phishing is sophisticated

Attacks blend AI and impersonation techniques to bypass traditional, content-based email security. Campaigns spin up in minutes, frequently using techniques like lookalike domains, spoofed senders, and compromised infrastructure to impersonate brands and executives.

### Email threats need to be stopped inbound and outbound

Splitting inbound protection and outbound authentication into separate projects can leave gaps for attackers to exploit. It also creates more work for SOC teams that are already buried in abuse mailbox triage, false positives, and vendor tickets whenever something new gets through.

### Identity and content both matter

Modern threats exploit both **who** is sending and **what** they send. To stop these threats, security needs both:

- **Inbound protection** detects and stops malicious content before it impacts users.
- **Outbound authentication** ensures that only authorized senders can use your domains and brand.

Without both, identity-based attacks slip through, detection coverage lags, and brand and customer trust erode.

## The value of Sublime + Vailmail

Together, Sublime and Valimail restore trust in email, stop more attacks, and remove the manual work that slows security teams down.

1. **Fewer successful phishing and BEC incidents tied to domain or user impersonation**
2. **Higher DMARC enforcement coverage across domains and sending services**
3. **Fewer false positives and fewer manual email reviews**
4. **MTTR for user-reported email reduced from hours to seconds**

# How Sublime + Vailmail deliver

Together, Sublime and Valimail unify email identity and attack protection to prevent more threats, keep defenses current, and reach your optimal state of protection faster.

| | VALIMAIL a digicert company | sublime |
|---|---|---|
| **1. Prevent more threats for employees and customers** | **Valimail stops impersonation at the source.** Enforced DMARC prevents attackers from spoofing your domains or executive identities and gives definitive control over who can send on your behalf. | **Sublime Security is the detection, prevention, and response layer.** It stops more attacks with fewer false positives, and its **Autonomous Security Analyst (ASA)** automates abuse mailbox workflows, reducing MTTR on user-reported email from hours to seconds. |
| **2. Continuously improve defense** | **Valimail provides always-on identity protection** continuously authenticating email and automatically detecting new sending services before unauthorized changes introduce risk. Precision Sender Intelligence and patented dynamic SPF keep authentication accurate as infrastructure evolves – without broken SPF records or manual DNS work. | **Sublime Security delivers adaptive, org-specific detection.** The platform and its AI agents block advanced phishing and BEC while the **Autonomous Detection Engineer (ADÉ)** generates, backtests, and deploys new coverage in hours when new attacks appear. |
| **3. Faster time to protection** | **Valimail** gets organizations to DMARC enforcement up to **4×** faster than other solutions and up to **8×** faster than DIY, using automated discovery, one-click authorization, and zero manual DNS management. | **Sublime** closes detection gaps quickly by turning missed attacks into new, org-specific protections without vendor bottlenecks, accelerating the path from deployment to tailored defense. |

**Sublime's next-gen email security offers the AI agents, ML-powered detection, and advanced, real-time analysis teams need to stay ahead of attackers.**

Get a live demo to see how →