Sublime Security

Why security teams use Sublime

Fewer email-originated incidents, spend less time on email.

How we do it

Not a black box.

Pain Points

1

Detection Efficacy

Malicious/unwanted email gets through, legitimate email gets blocked

2

Lack of Transparency

Can’t tell why something was or wasn’t blocked

3

Inflexible

Can’t customize the tool to fit our unique needs

The Sublime Approach

Transparency and Explainability

BEC or Fraud
Callback Phishing
Credential Phishing
Extortion
Spam
ke
n
HTML Smuggling
Brand Impersonation
Social Engineering
VIP Impersonation
Optical Character Recognition
Computer Vision
Natural Language Processing
Behavioral Analysis
Risk Scoring

Detection Rule

VIP / Executive Impersonation

```
type.inbound

and any($org_vips, .display_name == sender.display_name)

and any(ml.nlu_classifier(body.current_thread.text).inte
    .name == "bec" and .confidence == "high" )

and any(ml.nlu_classifier(body.current_thread.text).enti
    .name == "urgency" or .name == "request" )  and prof

and profile.by_sender().days_known < 30
```

Flexible platform

Granular control

Easily mitigate false positives with rule-level exclusions.

Target mailboxes or teams.

Turn specific detections off.

Craft tailored, AI-powered detections.

Fraud
Activated

VIP Impersonation
✓ 100% Activated

Credential Phishing
✓ 99% Activated

HTML smuggling
✓ 100% Activated

Callback Phishing
✓ 99% Activated

Malware/Ransomware
✓ 100% Activated

Bra
✓ 9

Trusted by

Spotify® · reddit · Brex · ramp · AUTOMOX · Personio

elastic · Vanta · red canary · BlueVoyant · RECON™ INFOSEC · INTEZER

advact advise & act · ActBlue · Primer · cedar · centrica · WATCHES OF SWITZERLAND

Community Financial CREDIT UNION · RLI® DIFFERENT WORKS · KeHE® · Crossbeam · GREYNOISE · UCPS

AMG PETRONAS FORMULA ONE TEAM · sprinklr · FANDUEL · TPICAP · Chick-fil-A · Cal Poly Humboldt.

inductive automation · snyk · pipe · ovo energy · GSA Capital · PAXOS

Comprehensive Email Security

Inbound Email Protection

Abuse Mailbox Automation

Attack Surface Reduction

Herd Immunity

Operationalize Threat Intel

Custom Detections and Policies

Live Demo

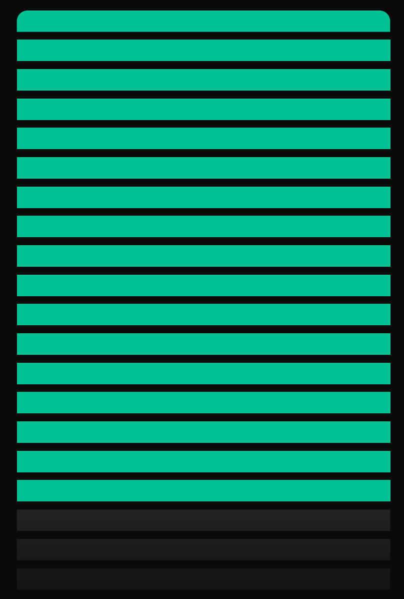
@sublime_sec · https://sublime.security

Customer Case Study: User Report automation / SOC efficiency

Financial Services · 2,700 employees · 6 FTE SOC analysts · Microsoft 365

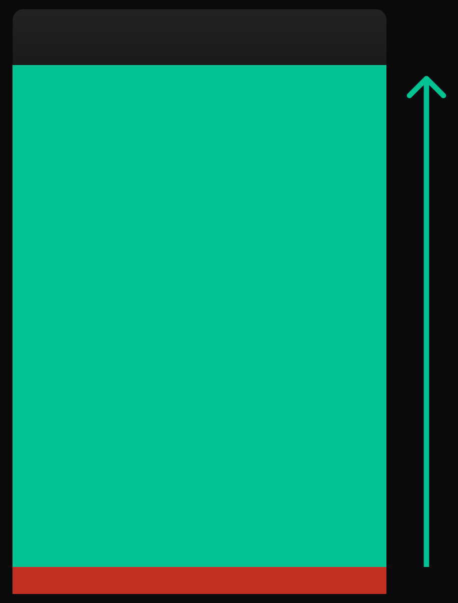
Before Sublime: Reactive (user reports only), 0% automation, 330 tickets/month, ~30% malicious

After Sublime:



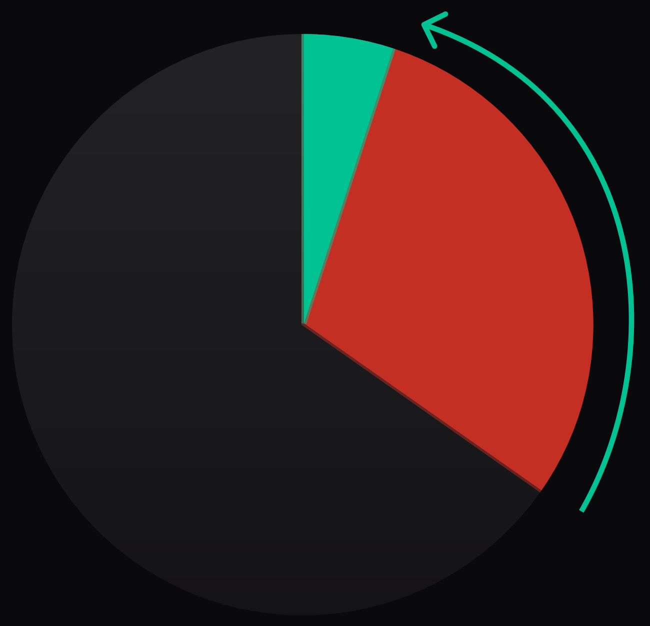
↑ 10 x

increase in total number of incidents resolved



0 % → 96 %

increase in fully automated remediation



20 mins → 5 mins

decrease in time spent per manual remediation

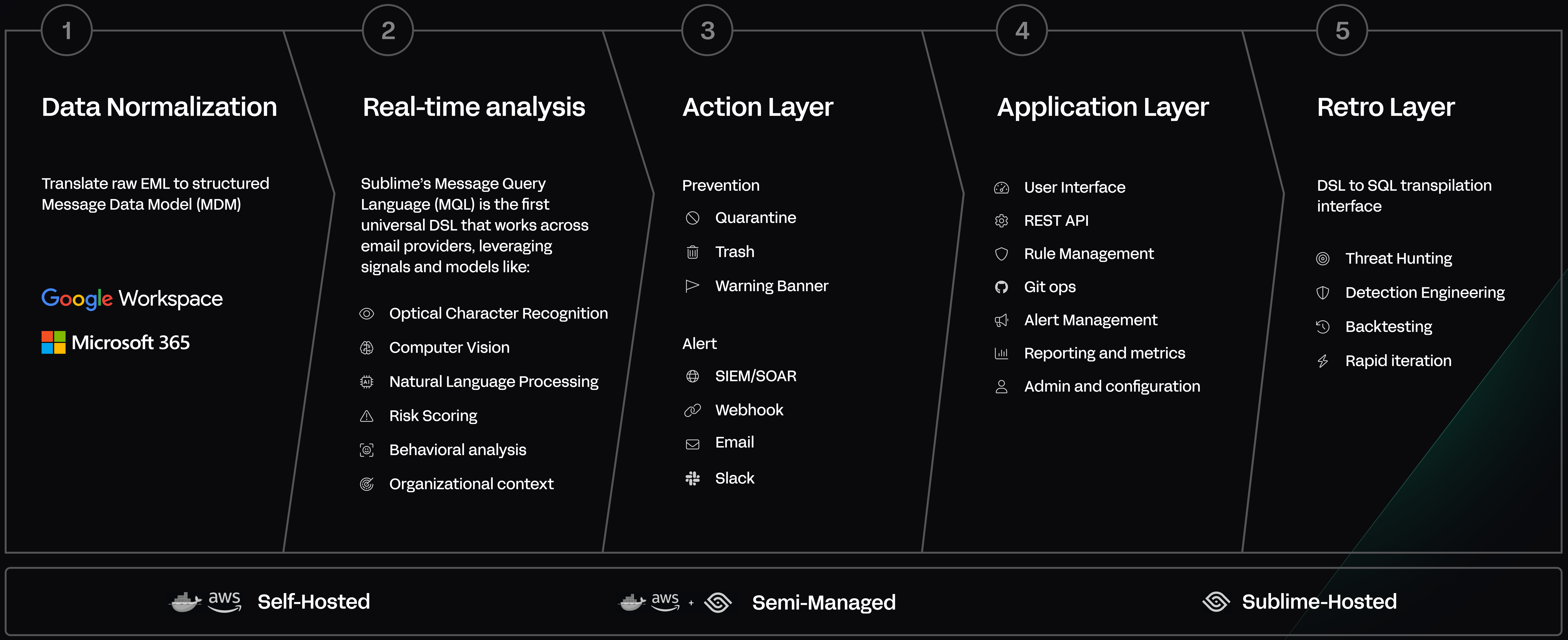
80 hrs
in time savings per month

$90 k
in annual savings

75 %
faster MTTR

150 k hrs
of reduced risk of exposure

Sublime Platform Overview



1

Data Normalization

Translate raw EML to structured Message Data Model (MDM)

Google Workspace

Microsoft 365

2

Real-time analysis

Sublime's Message Query Language (MQL) is the first universal DSL that works across email providers, leveraging signals and models like:

- Optical Character Recognition
- Computer Vision
- Natural Language Processing
- Risk Scoring
- Behavioral analysis
- Organizational context

3

Action Layer

Prevention

- Quarantine
- Trash
- Warning Banner

Alert

- SIEM/SOAR
- Webhook
- Email
- Slack

4

Application Layer

- User Interface
- REST API
- Rule Management
- Git ops
- Alert Management
- Reporting and metrics
- Admin and configuration

5

Retro Layer

DSL to SQL transpilation interface

- Threat Hunting
- Detection Engineering
- Backtesting
- Rapid iteration

aws Self-Hosted

aws + Semi-Managed

Sublime-Hosted