mimecast

Social Media Strategy & Planning

Creating engaging social media content is only a worthwhile endeavor if it gets in front of the right audience. Therefore, in addition to creating localized and global content, I was tasked with full social media strategy and execution responsibilities. This entailed drafting organic and paid social copies for external platforms like LinkedIn, X, and Facebook, crafting copy for internal advocacy tools like EveryoneSocial to boost employee amplification, and managing internal social promotion strategies. These initiatives supported both US-based and international teams to actively promote Mimecast's thought leadership, third-party analyst materials, and new campaign assets.

The Mimecast Social Media team's mission is to not only build a vibrant digital presence, but to ensure internal stakeholders utilize available social amplification materials, while effectively marketing our brand voice to customers, prospects, and industry analysts. My strategic responsibilities also include collaborating with cross-functional subject matter experts and marketing management, analyzing social media performance data, and aligning social initiatives with current go-to-market strategies and broader marketing campaigns. This consists of designing comprehensive, end-to-end social media strategy plans to submit upward for leadership approval, and managing the subsequent execution and community management. While the official social media strategy plans I created for Mimecast are confidential, I have provided a "mock" social media strategy plan here to showcase these capabilities.

Comprehensive Master Plan: Social Media Strategy & Demand Generation Engine

Prepared for: Marketing Leadership & Growth Teams
Target Industry: Enterprise AI-Powered Email Security
Ecosystem Coverage: Microsoft 365, Google Workspace, Hybrid, and Multi-Tenant Environments
Operational Framework: Lean Marketing Team Deployment (1 Dedicated Lead + Cross-Functional Support)

---

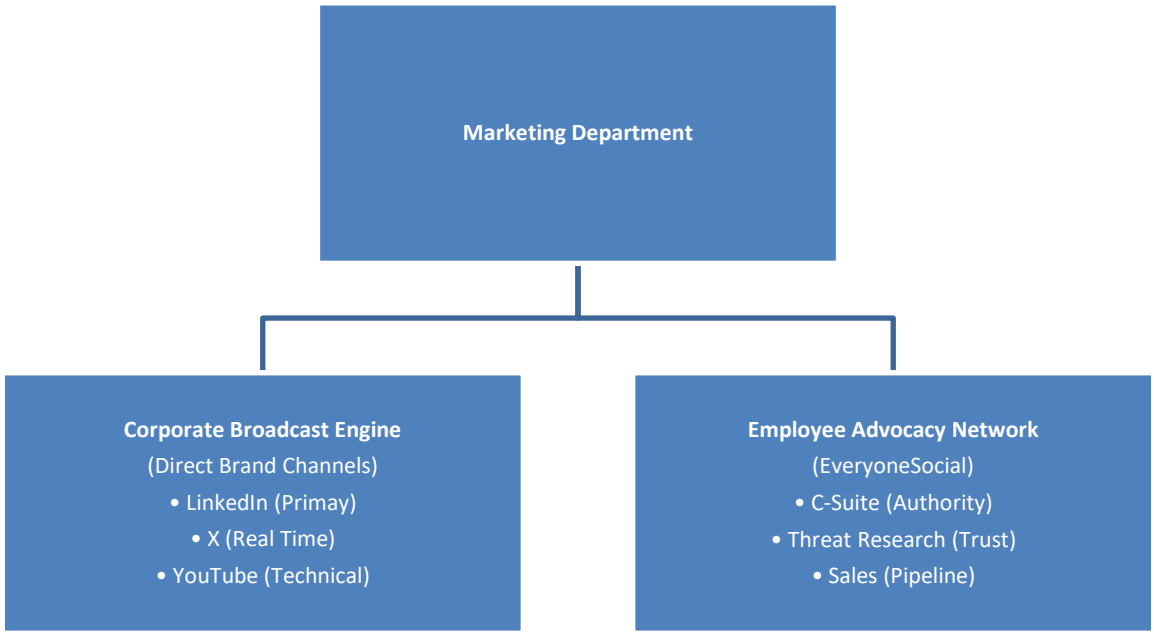
1. Executive Summary

The cybersecurity landscape is undergoing a paradigm shift driven by artificial intelligence. As enterprise threat vectors expand exponentially, legacy, signature-based defense mechanisms are no longer sufficient. To position our organization as the definitive leader in AI-powered threat detection, response, and mitigation, the marketing department must transition from passive social broadcasting to an aggressive, insights-driven social media engine.

This strategy establishes a high-frequency, high-authority social media infrastructure designed to convert complex machine-learning concepts into urgent enterprise value, capture B2B demand, and activate employee networks to outpace legacy competitors. By utilizing our technology's native capability to protect all widely used environments (M365, Google Workspace, Hybrid), we differentiate ourselves from native security tools while maximizing our lean marketing team using a structured, repeatable production workflow.

2. Foundation & Internal Amplification Architecture

Building upon our understanding of the current cybersecurity landscape and our team's experience in conducting social media campaigns for Mimecast thus far, which has entailed everything from writing actual social media posts, promoting those posts using the company's LinkedIn and other social media accounts, as well as promoting them internally using EveryoneSocial, our advanced AI-based cybersecurity social strategy formalizes these workflows into two distinct engines: **The Corporate Broadcast Engine** and **The Employee Advocacy Network**.



The Corporate Broadcast Engine (Multi-Platform Optimization)

Organic reach for corporate pages is continually throttled by platform algorithms favoring highly active, native multimedia, and real-time commentary. To circumvent this, we leverage our main brand accounts across LinkedIn, X, and YouTube as an authoritative external broadcast network. Acting as our centralized broadcasting engine, these channels are optimized to scale brand authority, capture real-time market mindshare, and drive top-of-funnel inbound demand.

Tri-Platform Content Architecture: The marketing team produces and programs platform-specific media weekly, tailoring formats to match algorithmic preferences. LinkedIn receives executive editorial text and native document carousels; X hosts rapid-response threads, breaking Cyber Threat Intelligence (CTI), and real-time industry event commentary; YouTube serves as the visual engine for deep-dive product demos, threat breakdown videos, and technical webinars.

The Multi-Format Multiplier: To maximize production efficiency, all long-form content is built for algorithmic remixing. A single high-production YouTube video or technical webinar is systematically stripped into 60-second YouTube Shorts, high-impact video snippets for LinkedIn, and summarized text threads for X, ensuring continuous presence across feeds without content fatigue.

Algorithmic Engagement Rules: Brand channels adhere strictly to a platform-first engagement model to optimize distribution. This includes prioritizing native uploads over external links (which trigger algorithmic penalties), actively responding to high-value community comments within the critical first 60 minutes of posting, and tag-teaming broadcasts with our C-suite and engineering creators to spark immediate engagement velocity.

The Employee Advocacy Network (EveryoneSocial Optimization)

Organic reach for corporate pages is continually throttled by platform algorithms favoring individual creators. To circumvent this, we turn our internal staff, specifically threat researchers, product engineers, and the C-suite, into a distributed distribution network. With Sales and Marketing already established as the most active cohorts on EveryoneSocial, our amplification efforts will prioritize driving pipeline velocity and social selling.

Curated Content Streams: The marketing team populates EveryoneSocial weekly with pre-vetted, compliant social copy divided into three categories: Thought Leadership, Product/Feature Innovation, and Cyber Threat Intelligence (CTI).

Segmented Gamification: To maintain high internal participation, Sales vs. Marketing will compete on monthly EveryoneSocial leaderboards, with performance metrics directly tied to marketing-funded rewards (e.g., tech gear, professional development stipends).

The "Zero-Edit" Mandate: While copy is provided, employees are trained to add custom context to the first line of their posts. This prevents identical-copy flags from the LinkedIn algorithm and preserves authentic individual voices while maintaining corporate messaging guardrails.

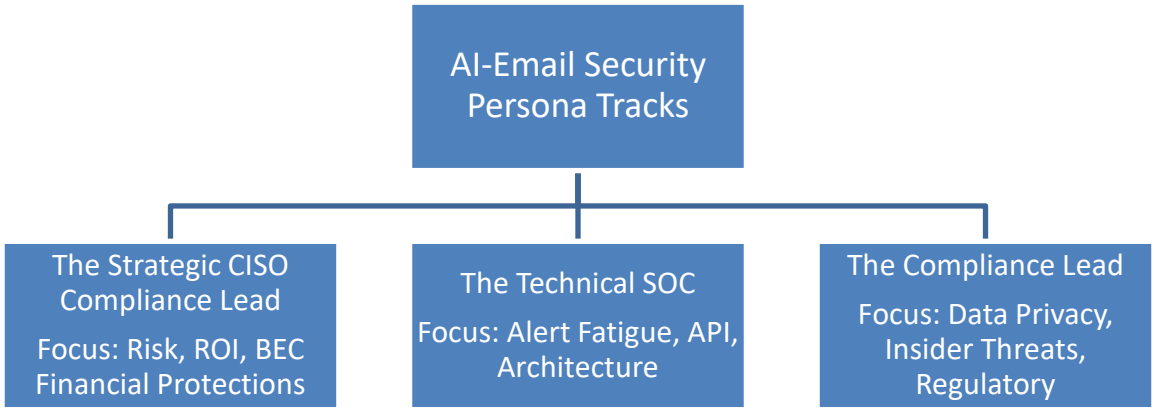
3. Platform Strategy & Segmentation Matrix

Not all social networks yield equal ROI for enterprise B2B sales cycles. Our presence is heavily weighted toward networks where Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), and Security Operations Center (SOC) Directors actively source peer insights and industry trends.

Platform	Primary Objective	Target Audience	Content Archetype	KPI Focus
LinkedIn	High-Value Lead Gen & Core Brand Authority	CISOs, CIOs, VPs of Infrastructure, SecOps Leaders, Compliance Officers	Deep-dive whitepapers, architectural blueprints, customer validation videos, executive op-eds, compliance frameworks.	Marketing Qualified Leads (MQLs), Inbound Inquiries, Content Share Rate.
X	Real-time Zero-Day Exploitations & CTI Dominance	Threat Researchers, Security Engineers, Ethical Hackers	Code snippets, vulnerability breakdowns, live event coverage, hot-takes on recent breaches, rapid-response threat analysis.	Viral Impressions, Amplification (Retweets), Community Engagement.
YouTube	Technical Product Proof & Educational Moats	Enterprise Architects, SOC Analysts, System Administrators	UI/UX walkthroughs, AI-model explanations (LLM vs. Behavioral Analytics), Sandbox testing demos.	Watch Time, Video Completion Rate, Click-Throughs to Documentation.

4.The Multi-Persona Content Matrix

To capture market intent efficiently, the marketing department deploys a three-pronged content track. Each track is designed to address a different core persona's primary driver while explicitly solving for their specific analytical friction.



💼 Persona 1: The Chief Information Security Officer (CISO) / CIO

Core Driver: Reducing systemic organizational risk, preventing Business Email Compromise (BEC) financial losses, and proving security stack ROI to the board.

Content Friction: Highly skeptical of marketing hype; demands quantifiable risk reduction metrics, total cost of ownership (TCO) models, and third-party validation.

Visual Style: Minimalist, data-driven financial charts, enterprise risk maps, and clean monochrome quote cards from peer CISOs.

LinkedIn Carousel:
Slide 1: The True Cost of a BEC Attack in 2026. (Industry Avg: $4.8M)
Slide 2: Why Legacy Secure Email Gateways (SEGs) Missed the Threat Vectors.
Slide 3: How Behavioral AI Neutralized the Exploit Before Financial Wire.
Slide 4: The Math: Reducing Total Cost of Ownership (TCO) by 42%.

Copy Template:
The "Board-Room ROI" Framework
The modern CISO doesn't have an email security problem. They have a financial risk problem.
Legacy Secure Email Gateways (SEGs) rely on static, historical threat signatures. But when an attacker compromises a vendor's actual account and crafts a contextually flawless invoice request, there is no malicious signature to detect.
The result? Business Email Compromise (BEC) that bypasses traditional defenses,

costing organizations millions in unrecoverable wire transfers.
Our latest Enterprise Economic Impact Assessment reveals how shifting from reactive signature matching to proactive, context-aware Behavioral AI alters the economics of email defense:
99.8% Reduction in successful BEC infiltration.
$1.2M Saved annually in direct financial mitigation and remediation resources.
3.1x ROI delivered in the first 120 days by consolidating disparate legacy tools into a single, cloud-native API framework.
Discover how enterprise security leaders are transitioning from SEGs to AI-driven risk mitigation. Read the full peer validation report verified by [Third-Party Testing Firm]. [Link to Gated Report]

🛠️ Persona 2: The SOC Director / Security Architect

Core Driver: Minimizing alert fatigue, automating incident response, and securing collaborative tools without creating communication bottlenecks.

Content Friction: Demands technical deep dives, architectural layout drawings, API documentation, and clear false-positive/false-negative ratios.

Visual Style: High-definition architectural blueprints, interactive API flow diagrams, and real-time screen captures of the admin dashboard executing autonomous mitigations.

Technical Breakdown: An incoming phishing email is allowed to pass through to a user by legacy email security, but our cloud-native API architecture's NLP Engine analyzes the tone and Identity Graph flags the email, creating an autonomous remediation, and keeping the email from being delivered.

Copy Template:
The "Zero-Fatigue Architecture" Deep Dive
If your SOC team spends more than 5 minutes triaging a single user-reported phishing email, your architecture is broken.
Traditional inline email architectures require continuous MX record rerouting, creating complex latency overhead and systemic blind spots.
By utilizing a direct, API-driven deployment model, our cloud-native AI integrates directly into the cloud email workspace in under two minutes.
Here is exactly how our Natural Language Processing (NLP) and behavioral mapping engines process threat vectors in real time, maintaining a **0.001% false-positive ratio**:

1. **Contextual Analysis:** The NLP engine parses email content for intent, tone anomalies, and urgent financial language, looking beyond simple sender verification.
2. **Relationship Graphing:** The platform maps historical communication baselines to instantly flag subtle display-name spoofing and anomalous internal-to-external

communication paths.
3. **Autonomous Remediation:** Rather than generating an analyst alert, the system automatically pulls matching polymorphic threats out of every inbox across the entire tenant in less than three seconds.

No MX record changes. No alert storms. Just pure, machine-speed automated response.
View the complete API documentation and architectural blueprint below. [Link to Technical Documentation/GitHub Sandbox]

⚖️ Persona 3: The IT Identity & Compliance Officer

Core Driver: Managing user access control, monitoring insider threat vulnerabilities, and maintaining strict regulatory compliance.

Content Friction: Seeks clear documentation on data privacy handling, user risk scoring frameworks, and regulatory mapping.

Visual Style: Structured regulatory compliance matrices, data privacy workflow flowcharts, and clear user risk scoring infographics.

Regulatory Mapping: When it comes to regulatory compliance like GDPR Article 32 and required insider threat protection, legacy email security uses mass data harvesting and invasive user monitoring and often still gets it wrong, but our AI architecture uses localized, encrypted telemetry processing and privacy-first anonymized risk scoring to not only get it right, but do it in a way that is not noticeable to users.

Copy Template:
The "Privacy-First Compliance" Framework
Can you detect insider threats and misdirected data leaks without infringing upon employee privacy rights?
For IT Compliance Officers navigating complex global data regulations like GDPR, CCPA, and HIPAA, email security is a delicate balancing act. Legacy solutions often require sweeping, invasive text logging that creates severe internal data liabilities. Our platform changes this dynamic with an advanced, privacy-by-design architecture built specifically to safeguard regulatory compliance:

- **Anonymized Insider Risk Analytics:** Our identity models build dynamic communication baselines that analyze behavioral telemetry, detecting anomalous outbound data movement without exposing personal identifier data to administrators.
- **Localized Data Processing:** Enterprise data is parsed through strict regional constraints, ensuring your email communications are analyzed and processed entirely within your designated data boundaries.

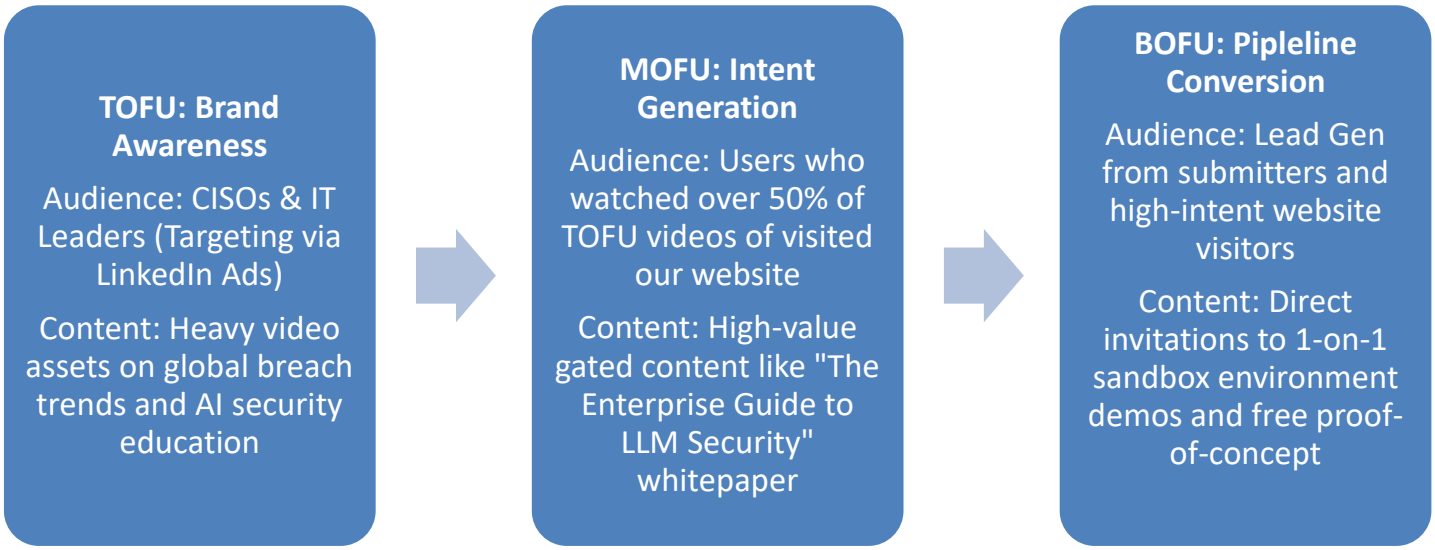
- **Automated Outbound Leak Prevention:** If a user accidentally attaches a sensitive customer database file intended for an external recipient, the AI intercepts the message instantly at the API level, preventing a catastrophic data breach.

Securing human communication shouldn't require compromising user privacy.

Download our comprehensive Data Governance and Regulatory Mapping Guide to see how we align with your compliance frameworks. [Link to Gated Whitepaper]

5. B2B Demand Generation & Paid LinkedIn Ads Funnel

With a small paid advertising budget allocated specifically for LinkedIn Lead Gen campaigns, we will focus our ad spend strictly on accounts within our Ideal Customer Profile (ICP). We use a multi-tiered, full-funnel strategy targeting job titles like CISO, CIO, VP of Information Security, Director of Network Security, and Compliance Officer at target enterprises.



Funnel Execution Architecture

Top of Funnel (TOFU) - Pattern Interruption: Deploy high-impact video or video document ads contrasting human remediation speed against our autonomous AI engine during an active attack. Build custom retargeting audiences based on users who watch more than 50% of the asset.

Middle of Funnel (MOFU) - Intent Generation: Retarget the TOFU engagement pool with single-image or document ads promoting deeply technical guides (e.g., The API Integration Guide vs Traditional SEGs). Route native LinkedIn Lead Gen forms

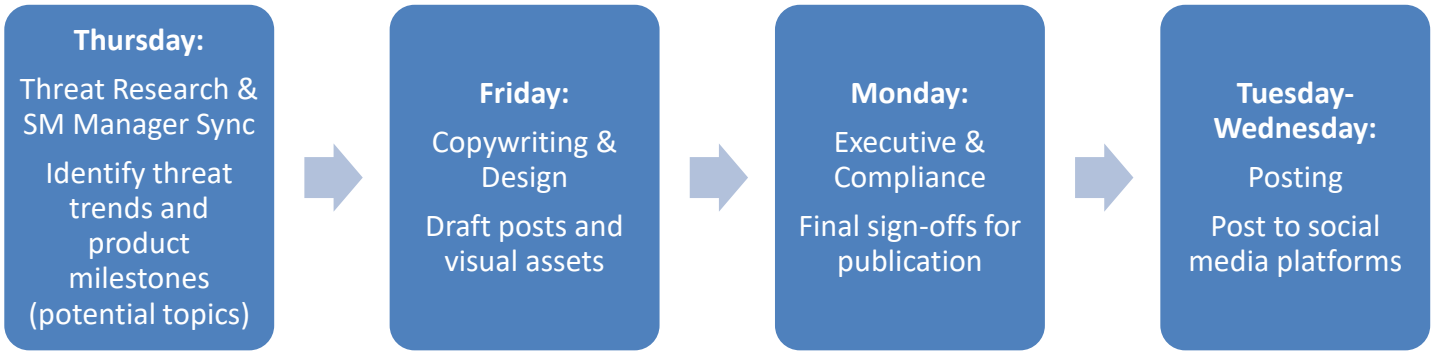
directly into **HubSpot** for immediate account routing.

Bottom of Funnel (BOFU) - Conversion: Target active MOFU leads and specific ABM matching lists with direct invitations to run an Autonomous Threat Scan. This acts as a frictionless proof-of-concept that scans their current inbox infrastructure in under five minutes to reveal active threats bypassing native security.

6. Lean-Team Operational Workflow & Governance

To successfully run all three persona tracks without burning out a single social media manager, the marketing department will operate via a structured "One-to-Many" Content Extraction Model utilizing Smartsheet for project tracking and governance.

Weekly Production Pipeline (Managed via Smartsheet):



Cross-Functional Support Map
Threat Research Team (Input Engine): Drops raw bulleted threat data or sandbox detection logs into a shared repository every Thursday morning.
The Social Media Manager (The Conductor): Also on Thursday, extracts the raw input data and builds out the segmented campaign ideation copy using persona templates.
Copywriter & Designer (The Creators): Copywriter spends 10 minutes on Friday reviewing the ideation copy and creates a draft to send to the Designer. The Designer spends 10 minutes putting the copy into an already approved social media post template.
Executive & Compliance Review (Approval): The Social Media Manager, Product Marketing Manager, and Legal Reviewer each spend 10 minutes on Monday reviewing and approving the final drafts.
Posting (The Final Step): The Copywriter posts the final version to external social media accounts and internal social media promotion platforms.

Cross-Platform Ecosystem Content Blueprint

Use the following framework to create a typical LinkedIn social media post and then use a shortened version for other social media platforms.

Copy Template:

The "Cross-Platform Defiler" Archetype

Multi-tenant enterprises don't just use one cloud ecosystem. Threat actors know this. We recently analyzed a sophisticated credential harvesting campaign that targeted a major logistics enterprise. The organization ran a hybrid infrastructure: **Microsoft 365** for corporate users and **Google Workspace** for their field operations.

- **The Attack Vector:** A polymorphic phishing link that altered its payload depending on the recipient's user agent.
- **The Native Vulnerability:** The security teams had to configure and monitor two completely separate native defense dashboards, creating visibility gaps and slowing down incident mitigation.

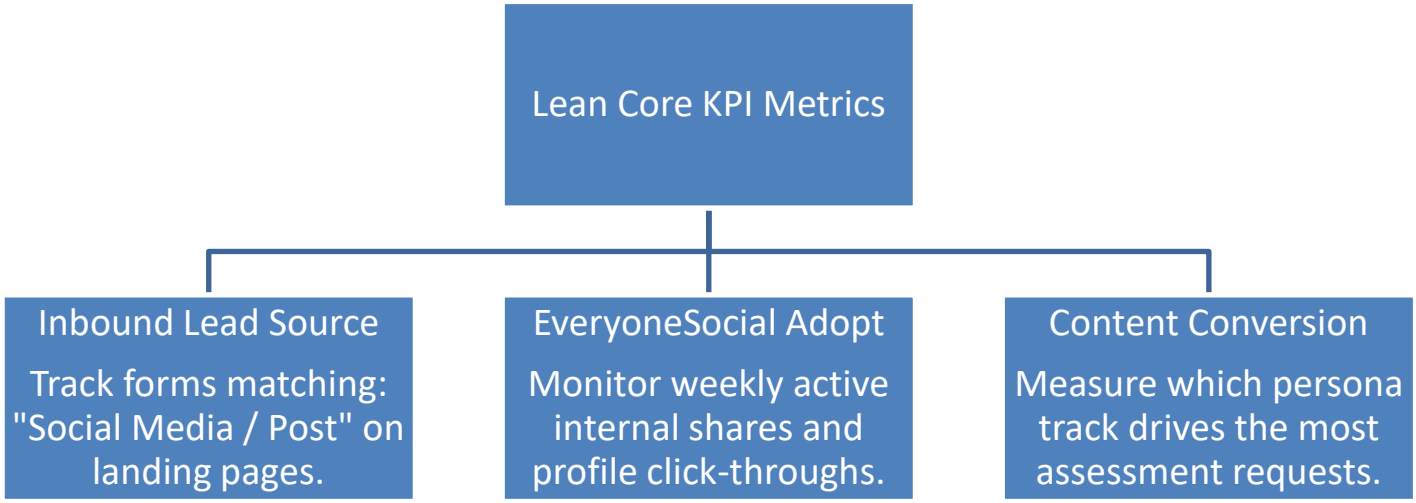
How Behavioral AI Stopped the Vector Domestically:

Our cloud-native security platform integrates directly with both M365 and Google APIs simultaneously. When the anomaly was detected in a Microsoft inbox, our behavioral engine immediately identified the threat profile and automatically removed matching payloads from the Google Workspace tenant in under three seconds.

Zero MX record changes. One single dashboard. Complete cross-platform protection. Read the full architectural deployment map. [Link to ungated technical document]

7. Analytical Framework & HubSpot Integration

By pairing **Smartsheet** for execution tracking with **HubSpot** for automated attribution, we can accurately monitor down-funnel performance.



HubSpot Multi-Touch Attribution: Every social asset deployed internally via EveryoneSocial or externally through corporate handles must append distinct UTM parameters (utm_campaign, utm_content=persona_soc, etc.). This allows HubSpot to automatically credit social interactions when an open opportunity advances to a closed-won deal.

Frictionless Form Intent Tracking: Ensure all inbound demo and assessment landing pages include a required dropdown or free-text field reading: *"How did you first hear about us?"* to capture organic word-of-mouth generated by our employee advocacy network.

EveryoneSocial Velocity Audit: Track the share frequency and click-through rates generated by the Sales team. If a specific persona track yields high click volumes for Sales, adjust our Smartsheet production schedules to prioritize that content category.