HermanEngage

EXAMPLE REPORTS

SAMPLE ACCOUNT: ABBVIE

See what your sellers know before the first message

Three HermanEngage deliverables built for one enterprise account and one senior buyer: a Contact Profile Report, a Contact Report with Engagement Cadence, and an Account Profile Report.

1

Contact Profile Report

Alignment, buying influence, communication profile and discovery questions

2

Contact Report and Engagement Cadence

Professional overview, three emails, LinkedIn, voicemail and call scripts

3

Account Profile Report

Executive view, cited evidence, challenges, opportunities and messaging themes

4

HermanEngage Solution Brief

How HermanEngage works

Illustrative example generated in October 2026 from cited public sources. Contact details are masked and the selling company is shown as "Client." Content is AI-generated and should be reviewed before use.

REPORT 1 · CONTACT PROFILE REPORT

Pete N.

Global CISO & VP of IT Risk Management, AbbVie

NAME	Pete Nxxxxxxx	TITLE	Global Chief Information Security Officer (CISO) & VP of IT Risk Management
EMAIL	peter.nxxxxxxx@abbvie.com	LINKEDIN	linkedin.com/in/pete-nxxxxxxx
COMPANY	AbbVie	USE CASE	Marketing & Sales

INFERRED PERSONALITY TYPE

Type 1 · Evaluator

Engagement alignment

Dimension	Assessment	Rationale
Role match	Strong	Pete is the Global CISO and VP of IT Risk Management, directly responsible for security strategy and risk posture: an ideal target for the Client's solutions.
Level match	Strong	As a senior executive with global responsibilities and board membership, his seniority fits the campaign's Director-and-above targeting.
Subject-area match	Strong	His expertise spans cloud, application security, vulnerability and risk management, matching the campaign's key product areas.
Need	Strong	AbbVie's hybrid cloud and AI adoption, regulatory demands and enterprise scale create a clear need for a unified security maturity assessment.

ALIGNMENT STRENGTHS

- Direct senior leadership responsibility for global security strategy and risk management.
- Broad, deep expertise across compliance, vulnerability management, and cloud and application security.
- Experience with regulated, hybrid and cloud environments that reflect the target customer profile.
- Board membership at Health-ISAC, showing commitment to sector security standards and collaboration.

ALIGNMENT GAPS

- No direct evidence of current use or evaluation of the Client's solutions or competing platforms.
- Few public posts or publications, which limits insight into stated priorities.
- No specific project or technology ownership disclosed publicly to confirm current product scope.

Buying influence

Primary decision-maker for information security strategy

As Global CISO and VP of IT Risk Management, Pete holds major influence and likely final authority over strategic security platform and vendor decisions at AbbVie.

EVIDENCE

His executive titles imply top-level responsibility for security and risk governance.

Strategic advisor to executive and board leaders

Regularly reports information-security and technology risks to IT teams and management, shaping organizational priorities and resourcing.

EVIDENCE

AbbVie filings state the cybersecurity program is led by the CISO, with regular reviews at management and board levels.

Professional context

ROLE AND RESPONSIBILITY

CISO and VP of IT Risk Management at AbbVie

Holds the top security leadership roles at AbbVie, overseeing global information security and IT risk management, including security strategy, compliance, risk mitigation and alignment with global business operations.

EVIDENCE

Current titles on his LinkedIn profile and professional summary.

Board member at Health-ISAC

Contributes to sector-wide security collaboration and intelligence sharing for the healthcare industry, influencing security posture beyond his primary employer.

EVIDENCE

Listed experience as a Board Member at Health-ISAC.

SKILLS AND EXPERTISE

Information security leadership and governance

More than 18 years building and managing effective, sustainable security programs for global organizations, including strategy, governance and risk management.

EVIDENCE

Self-described 18 years of experience; CISO and VP roles at AbbVie and prior CISO roles.

Security program and compliance management

Expertise in PCI DSS compliance, security architecture design, IT audit and disaster recovery planning, showing a strong compliance and controls orientation.

EVIDENCE

Led OfficeMax to PCI compliance quickly and maintained it; skills include PCI DSS, IT Audit and Sarbanes-Oxley.

Security architecture, vulnerability and threat management

Experience with security architecture design, vulnerability assessment, penetration testing and threat management strategy.

EVIDENCE

Managed threat and vulnerability management during breach response at SUPERVALU.

Strategic IT and risk management

Capability in IT strategy, enterprise architecture, business continuity and process improvement, aligning security with business goals.

EVIDENCE

Skills include IT Strategy, Enterprise Architecture and Business Continuity.

Certifications and security tools

Holds the CISSP certification, and his skills listing includes the Client's platform, showing familiarity with cloud and vulnerability management tooling.

EVIDENCE

Skills listing includes CISSP and the Client's platform.

Potential business priorities

Building sustainable, effective security programs

Creating security programs that work across global organizations and last, with ongoing risk management and compliance.

EVIDENCE

Described as having a deep track record of building effective, sustainable programs worldwide.

Risk-based compliance and vulnerability management

Focus on compliance, threat and vulnerability management, identity and access management, and regulatory adherence.

EVIDENCE

Developed compliance and vulnerability strategies at SUPERVALU.

Transforming culture toward risk management

Embedding risk management into daily business and IT processes so the organization stays attentive to security.

EVIDENCE

At OfficeMax, shifted culture from high risk tolerance to risk management built into everyday processes.

Supporting rapid, secure business growth

Balancing security with business pace, enabling agility while keeping governance across complex hybrid and cloud environments.

EVIDENCE

Leadership roles in large, high-growth enterprises.

Communication profile

OBSERVABLE ENGAGEMENT SIGNALS

Proven record building security programs

Sustained leadership that has advanced security capabilities in several large organizations.

EVIDENCE

An 18-year history of building programs at global firms, including AbbVie.

Hands-on breach response experience

Practical insight into operational threat management and compliance remediation.

EVIDENCE

Interim CISO at SUPERVALU, managing payment card breach response.

ENGAGEMENT PREFERENCES

Structured, precise communication

Values clear, organized and logically developed information that reflects a high-integrity leadership style.

EVIDENCE

Personality profile indicates a preference for precise, objective communication with minimal ambiguity.

Detailed, evidence-based discussion

Engages best in thorough conversations that emphasize facts, standards and measurable improvement.

EVIDENCE

Background in compliance and governance precision.

Respectful, professional tone

Responds well to professional, respectful language; casual slang or humor may reduce credibility.

EVIDENCE

Personality guidance advises a professional tone with light, controlled humor only.

ENGAGEMENT DRIVERS

Ensuring correctness and integrity

Driven to ensure quality, ethical compliance and correctness across every part of the security program.

EVIDENCE

Profile and summary emphasize integrity, ethical responsibility and discipline.

Risk mitigation and regulatory compliance

Motivated to minimize risk exposure and meet complex healthcare and IT regulations.

EVIDENCE

Roles focused on PCI DSS compliance, governance and risk management.

Building lasting security capabilities

Aims to implement security solutions and operating models that work long-term across global operations.

EVIDENCE

Established enduring security teams and programs at OfficeMax and AbbVie.

DECISION-MAKING STYLE

Structured, criteria-based decisions

Prefers clear criteria, objectives and standards for evaluating options, reducing ambiguity.

EVIDENCE

Personality traits include rule orientation and structured thinking.

Detail-oriented and analytical

Relies on data, technical evidence and risk assessments to guide security strategy and investment.

EVIDENCE

Leadership in risk assessments and vulnerability management.

PREFERRED COMMUNICATION STYLE

Clear, logical presentation

Favors well-organized messages that avoid ambiguity and get the details right.

EVIDENCE

Guidance stresses clarity, precision and avoiding vague language.

Professional and respectful

Keeps a serious tone that respects roles and responsibilities.

EVIDENCE

Guidance recommends a professional tone with controlled humor only.

Recommended engagement approach

- Lead with a structured, precise and factual approach that emphasizes correctness and quality.
- Present the Client's technical capabilities clearly, tied to regulated hybrid-cloud challenges at AbbVie.
- Focus on risk-based vulnerability management, compliance consolidation and AI security governance.
- Use executive summaries backed by detailed evidence and compliance frameworks.
- Keep claims and data accurate and verifiable; avoid informal language.
- Offer clear options and decision criteria, and invite feedback.

Discovery questions

1. How does AbbVie unify risk visibility and remediation workflows across hybrid and multi-cloud environments today?
2. What are your biggest challenges in governing AI and LLM workloads while keeping innovation moving?
3. How do you prioritize and correlate findings across application, API and infrastructure security?
4. What metrics and evidence do you use to communicate security risk to the board and executive team?
5. How is AbbVie addressing GxP and regulatory expectations for AI and cloud-enabled scientific workflows?
6. Where could a consolidated platform better support AbbVie's evolving cloud and AI security posture?

Consequences of inaction

- Fragmented cloud and application security oversight may increase exposure to breaches affecting critical biopharma operations.
- Insufficient AI governance could lead to compliance violations, data leakage or disruptions to innovation.
- Fragmented vulnerability management slows remediation and raises organizational and regulatory risk.
- Without measurable risk metrics, leadership support and resourcing for security can weaken.
- Poor integration of cloud posture and workload security undermines policy enforcement and widens the attack surface.

REPORT 2 · CONTACT REPORT AND ENGAGEMENT CADENCE

Contact Report: Pete N.

TITLE	Global Chief Information Security Officer (CISO) & VP of IT Risk Management		
COMPANY	AbbVie	EMAIL	peter.nxxxxxxx@abbvie.com
LINKEDIN	linkedin.com/in/pete-nxxxxxxx		

Professional overview

Pete is a proven cybersecurity executive with 18 years of experience, recognized for building effective and sustainable security programs for global organizations. As Global CISO and VP of IT Risk Management at AbbVie, he leads IT risk strategy and security governance.

RELEVANT EXPERIENCE

AbbVie	Leads information security and IT risk management globally.
Health-ISAC	Member of the Board of Directors, contributing to healthcare industry security collaboration.
Blue Cross Blue Shield Association	Former VP & CISO and Interim CIO, overseeing large-scale security and IT strategy.
SUPERVALU (independent consultant)	Interim CISO managing response to a major payment card breach, developing compliance and threat management strategy.
OfficeMax	Established and led global IT security, achieving and sustaining PCI compliance and embedding risk management into business processes.
PricewaterhouseCoopers (PwC)	Director-level security consultant with deep expertise in security strategy, risk assessment and breach response for Fortune 100 clients.

KEY SKILLS AND COMPETENCIES

- Information Security Management
- IT Audit & Compliance (PCI DSS, Sarbanes-Oxley)
- Security Architecture & Vulnerability Assessment
- Enterprise Risk Management & Governance
- Leadership & Process Improvement
- Security Strategy & Business Continuity
- Familiarity with the Client's security platform
- Secure SDLC & Vendor Management
- CISSP certified

Opportunity context

Given Pete's leadership in cybersecurity and risk management, there's a strong opportunity to explore solutions for AbbVie's hybrid-cloud and AI-driven environment. Helping meet GxP and compliance requirements and securing critical workloads, including Allergan Aesthetics consumer platforms hosted on AWS, aligns with his responsibilities and AbbVie's threat landscape.

A five-minute security maturity assessment offers a simple value proposition: a detailed report with analyst and industry best practices for cloud, AI and application security.

Engagement cadence

Three emails, two LinkedIn touches, a voicemail and a live-call opener. Sender: Client Team. Call to action: a five-minute security maturity assessment.

EMAIL 1 **Subject: Explore advanced cloud and AI security for AbbVie's hybrid environment**

Hi Pete,

With your leadership in shaping AbbVie's information security program, I wanted to share a quick way to assess your current cloud, AI and application security maturity. A five-minute security maturity assessment unlocks a detailed report with expert best practices for hybrid environments like yours.

Given the growing complexity of AI adoption and compliance pressure, it could offer clear insights for continued resilience.

Here's the assessment link: security maturity assessment

Best,
Client Team

EMAIL 2 **Subject: Following up: strengthen AbbVie's cloud and AI security posture**

Hi Pete,

I wanted to follow up on the security maturity assessment for cloud, AI and application security. With your role overseeing IT risk management, the insights could help identify areas for improvement and support regulatory compliance.

If you have questions or would like details on solutions for hybrid-cloud environments, I'd be glad to connect.

Here's the link again: security maturity assessment

Best,
Client Team

EMAIL 3 **Subject: Last call: expert insights on AbbVie's security maturity**

Hi Pete,

Checking in one last time about the five-minute security maturity assessment. The detailed report could offer useful perspective as AbbVie advances its cloud and AI security posture.

Let me know if you'd like to discuss how relevant solutions can help meet your security and compliance goals.

Assessment link: security maturity assessment

Best,
Client Team

LinkedIn

Connection request

Hi Pete, I'm reaching out to connect with fellow security leaders focused on cloud and AI risk management. Looking forward to sharing insights.

Follow-up message

Thanks for connecting, Pete. Given your leadership at AbbVie, I'd like to share how our solutions help strengthen security in hybrid-cloud and AI environments. Would you be open to a brief conversation?

Phone

Voicemail script

Hi Pete, this is the Client Team. We know how critical your role is for AbbVie's cloud and AI security. I wanted to share a quick way to assess your security maturity: a five-minute assessment that delivers detailed expert recommendations. I'd appreciate the chance to connect when convenient. Thank you.

Live call opener

Hello Pete, this is the Client Team, and I appreciate your time. Given your leadership in information security and IT risk at AbbVie, I wanted to briefly discuss how relevant solutions can support your hybrid-cloud and AI security goals, especially with today's compliance and risk pressures. Are you exploring solutions in these areas now, or would a quick security maturity assessment with tailored guidance be useful?

REPORT 3 · ACCOUNT PROFILE REPORT

AbbVie

linkedin.com/company/abbvie · As of 2026-10-20 · Based on cited public evidence; non-public information may not be represented.

Executive view

EXECUTIVE ACCOUNT SUMMARY

AbbVie is a strong-priority account: a growing, highly regulated global biopharmaceutical enterprise with documented hybrid-cloud, AWS, Kubernetes, application security and enterprise AI activity. Its public disclosures and targeted hiring show mature cybersecurity governance alongside active needs in cloud visibility, application security scaling, non-human identity and AI security, creating strong relevance for the Client's cloud, application and AI security solutions, without establishing current vendor intent.

RECOMMENDED ACCOUNT PRIORITY

High

Strong firmographic fit and direct evidence of cloud-native engineering, enterprise AI expansion, AppSec program development and cybersecurity maturity initiatives justify prioritizing engagement. No public evidence establishes a current Client relationship, active procurement or specific buying authority.

FIRMOGRAPHIC MATCH

Strong

About 57,000 employees in more than 70 countries, $61.2 billion in 2025 net revenue, and regulated global R&D, manufacturing, consumer-facing and clinical data environments.

TOPIC AND SOLUTION RELEVANCE

Strong

Current AbbVie materials identify cloud services, hybrid AWS, Kubernetes/EKS, CI/CD security, application security posture management, AI-agent governance and AI cybersecurity maturity as active domains.

EVIDENCE CONFIDENCE

High

Primarily supported by AbbVie's 2025 Form 10-K, 2026 financial releases, official announcements and current job descriptions. Installed products, relationships and purchasing intent remain undisclosed.

KEY TAKEAWAYS

- Revenue grew 10.2% year over year in Q2 2026, a supportive backdrop for strategic security programs.
- Technical roles describe hybrid on-premises and AWS environments, Kubernetes/EKS, containers, infrastructure as code and enterprise DevSecOps.
- AbbVie is building capabilities in AI security, agent governance, non-human identity, and application

MATERIAL UNCERTAINTIES

- No public evidence confirms whether AbbVie licenses the Client's or competing cloud, vulnerability, AppSec or AI security platforms.
- Workload distribution across AWS, Azure, GCP and on-premises environments is not publicly quantified.
- Hosting architecture for individual Allergan Aesthetics brand sites is not publicly confirmed.

security testing and posture management.

- The company names cyberattacks, third-party systems, cloud services and emerging AI risks as potentially material concerns.
- Engagement should emphasize measurable risk reduction and integration with existing workflows, not imply AbbVie lacks a mature program.
- Job postings indicate capability priorities but not budgets, procurement timing or individual decision authority.

Company and operational intelligence

COMPANY OVERVIEW AND GROWTH

Observed fact · High

Global biopharmaceutical enterprise

AbbVie describes itself as a diversified, research-based biopharmaceutical company with leadership in immunology, neuroscience, oncology and aesthetics.

WHY IT MATTERS

The breadth of regulated business units and digital environments supports enterprise-level cloud, application and AI security discussions.

Evidence date 2026-02-20 · sec.gov

Observed fact · High

Large global operating footprint

About 57,000 employees in more than 70 countries, with products helping patients in more than 180 countries and territories.

WHY IT MATTERS

Global scale raises the importance of standardized asset visibility, policy enforcement and risk reporting.

Evidence date 2026-05-01 · abbvie.com

Observed fact · High

Continued double-digit quarterly growth

Q2 2026 net revenue was $16.99 billion, up 10.2% as reported, led by immunology and neuroscience.

WHY IT MATTERS

Growth increases the workloads, integrations and digital assets security teams must govern.

Evidence date 2026-07-31 · investors.abbvie.com

TECHNOLOGY FOOTPRINT

Observed fact · High

Hybrid cloud and AWS environments

Engineering descriptions reference hybrid solutions with on-premises and cloud-hosted components, production AWS use and cloud-native AWS security services.

WHY IT MATTERS

Aligns directly with cloud posture, workload and hybrid-cloud risk visibility use cases.

Evidence date 2026-10-18 · careers.abbvie.com

Observed fact · High

Kubernetes, EKS and containerized workloads

Technical roles describe Docker, Kubernetes, Amazon EKS, Helm, container security and service-account governance in production.

WHY IT MATTERS

Creates direct relevance for container, Kubernetes, workload and cloud configuration security.

Evidence date 2026-10-19 · careers.abbvie.com

Observed fact · High

Enterprise DevSecOps toolchain

A platform-architecture role references GitHub, AWS, JFrog, CI/CD, infrastructure as code, software supply-chain security and AI-assisted development tools.

WHY IT MATTERS

Application security positioning should focus on developer-workflow integration, consolidated findings and policy-driven controls.

Evidence date 2026-10-19 · careers.abbvie.com

Observed fact · High

Application security testing and posture management

AppSec roles reference SAST, DAST, IAST, software composition analysis, ASPM, CI/CD integration, container scanning and developer remediation workflows.

WHY IT MATTERS

Closely matches the Client's application security capabilities; outreach should find where existing tools leave coverage or workflow gaps.

Evidence date 2026-10-19 · careers.abbvie.com

HIRING TRENDS · TARGETED AND SELECTIVE

Observed fact · High

Dedicated AI security hiring

Recruiting a principal agentic AI security engineer to build autonomous security agents and drive an AI Cybersecurity Maturity program spanning controls, discovery, inventory, incident response and policy.

WHY IT MATTERS

A strong signal for technically credible AI security engagement focused on operational challenges.

Evidence date 2026-10-19 · careers.abbvie.com

Observed fact · High

Expanding AppSec platform capabilities

Openings cover application security architecture, testing-tool administration, ASPM, CI/CD integration and internal AppSec workflow tooling.

WHY IT MATTERS

Indicates an active AppSec development area, not necessarily a net-new procurement event.

Evidence date 2026-10-19 · careers.abbvie.com

Observed fact · High

Cloud identity and scientific computing

Recruiting for non-human identity and cloud IAM governance, plus hybrid HPC architecture spanning AWS, on-premises computing, GPUs and scientific workloads.

WHY IT MATTERS

Indicates targeted investment in securing machine identities and complex scientific cloud environments.

Evidence date 2026-10-19 · careers.abbvie.com

Strategy and market position

STRATEGIC INITIATIVES, PRIORITIES AND ORGANIZATION

Observed fact · High

Global AppSec program development

A DevSecOps opening describes building a global, enterprise-grade application security program with testing integrated into CI/CD and developer workflows.

WHY IT MATTERS

A direct opening to discuss coverage consolidation, risk prioritization and remediation orchestration.

Evidence date 2026-10-19 · careers.abbvie.com

Observed fact · High

AI-agent and machine-identity governance

Seeking a platform lead to establish a unified strategy for non-human identities, AI-agent governance and cloud IAM across partner-owned platforms.

WHY IT MATTERS

Cloud and AI outreach should address workload identities, agent inventory, least privilege and cross-platform observability.

Evidence date 2026-10-19 · careers.abbvie.com

Observed fact · High

Diversified growth and commercial execution

AbbVie's 2026 objectives include maximizing its diversified revenue base and executing launches and investments across key products.

WHY IT MATTERS

Connect resilience and risk reduction to uninterrupted launches, customer services and global operations.

Evidence date 2026-02-20 · sec.gov

Observed fact · High

Board and Audit Committee oversight

The board reviews information security and technology risks regularly; the Audit Committee oversees them within enterprise risk management.

WHY IT MATTERS

Use business-risk, resilience and measurable control-effectiveness language suited to governance reporting.

Evidence date 2026-02-20 · sec.gov

Observed fact · High

CISO-led cybersecurity program

The cybersecurity program is led by the CISO, who regularly engages technology teams and management on information security risks and opportunities.

WHY IT MATTERS

The CISO and senior security leaders are the right audience, but individual authority should not be assumed.

Evidence date 2026-02-20 · sec.gov

GO-TO-MARKET AND COMPETITIVE POSITIONING

AbbVie competes through differentiated therapies and portfolio breadth in markets where innovation, clinical outcomes and new indications matter. Competitors are advancing differentiated products too, reinforcing the need to protect R&D data, digital operations and time to market.

Company	Lead technique	Evidence	Confidence
Eli Lilly and Company	Product/features	Positioning EBGLYSS in atopic dermatitis around differentiated maintenance dosing and new clinical data, competing in an immunology market relevant to AbbVie.	High
Johnson & Johnson	Product/features	Advancing TREMFYA with differentiated indications and long-term data in inflammatory bowel disease and psoriatic arthritis, where AbbVie also competes.	High
Revance	Product/features	Markets DAXXIFY as a peptide-formulated neuromodulator with differentiated onset and duration, competing with Allergan Aesthetics' Botox franchise.	High

INDUSTRY AND MARKET CONTEXT

Observed fact · High

Regulators formalizing expectations for AI in medicines

The FDA and EMA have established common good-AI-practice principles for the medicines lifecycle, and EMA continues guideline work covering development, manufacturing and monitoring.

WHY IT MATTERS

AI security messaging should include traceability, governance, data integrity and defensible controls, not only generic cyber threats.

Evidence date 2026-06-04 · ema.europa.eu

Observed fact · High

FDA highlights connected manufacturing risk

FDA guidance notes that connected operational technologies in medical-product manufacturing can increase cyber risk, and calls for modern cybersecurity practices.

WHY IT MATTERS

Discussions may acknowledge dependencies between enterprise IT, cloud analytics and regulated manufacturing.

Evidence date 2025-06-20 · fda.gov

Challenges and opportunity assessment

BUSINESS CHALLENGES AND IMPLICATIONS

Observed fact · High

Complex cyber and third-party exposure

AbbVie reports its software, cloud services and third-party systems face increasingly frequent and sophisticated attacks that could expose sensitive information or disrupt operations.

WHY IT MATTERS

Supports risk-based cloud and exposure-management messaging without suggesting AbbVie has suffered a material breach.

Evidence date 2026-02-20 · sec.gov

Observed fact · High

AI security and reliability risk

AbbVie states AI-generated analyses could be deficient or amplify regulatory and cybersecurity risks, while ineffective adoption could reduce competitiveness.

WHY IT MATTERS

Directly supports AI security engagement around inventory, model and workload exposure, testing and governance evidence.

Evidence date 2026-02-20 · investors.abbvie.com

Observed fact · High

Fragmented machine-identity landscape

A cloud IAM opening describes the need to bridge a fragmented landscape of non-human identities, AI agents and cloud access into coherent, observable governance.

WHY IT MATTERS

Cloud security discovery should include workload and agent identities in attack-path and exposure analysis.

Evidence date 2026-10-19 · careers.abbvie.com

POTENTIAL RESPONSES AND TARGET ACCOUNT ALIGNMENT

Supported assessment · Moderate

Hypothesis: unify cloud workload and posture visibility

AbbVie may benefit from consolidating cloud posture, workload, container, Kubernetes and vulnerability information into one risk view across hybrid environments.

WHY IT MATTERS

Position the Client's cloud security as an assessment option after establishing existing tools, ownership and measurable gaps. Objective: reduce blind spots, prioritize exploitable exposures and standardize control reporting.

Evidence date 2026-10-19 · careers.abbvie.com

Supported assessment · High

Enterprise security leadership alignment

Board oversight, CISO leadership and formal cyber-risk governance make executive risk measurement and control-effectiveness reporting relevant themes.

WHY IT MATTERS

Lead with measurable reduction of material exposure, resilience and governance evidence.

Evidence date 2026-02-20 · sec.gov

Supported assessment · High

Cloud and infrastructure alignment

Hybrid AWS, Kubernetes/EKS, containers, infrastructure as code and scientific HPC create direct alignment with CNAPP and workload security use cases.

WHY IT MATTERS

Use practitioner language about workloads, clusters, images, identity, posture, attack paths and pipeline controls.

Evidence date 2026-10-19 · careers.abbvie.com

Supported assessment · High

Application security alignment

Active work in AST, ASPM, API-driven tooling and CI/CD integration closely aligns with web, API and DevSecOps security scope.

WHY IT MATTERS

Emphasize finding correlation, developer context, API coverage and remediation workflows.

Evidence date 2026-10-19 · careers.abbvie.com

Suggested account messaging themes

Supported assessment · High

Secure growth across hybrid cloud

Connect AbbVie's growing AWS, container and Kubernetes estate to unified posture, workload and exposure visibility that supports innovation without slowing engineering.

WHY IT MATTERS

For cloud security, infrastructure and engineering leaders.

Evidence date 2026-10-19 · careers.abbvie.com

Supported assessment · High

Turn AI governance into operational controls

Position AI security around discovering models and agents, mapping data and identity exposure, testing adversarial risk and producing evidence for AbbVie's AI maturity program.

WHY IT MATTERS

For AI engineering, data platform, security architecture and governance audiences.

Evidence date 2026-10-19 · careers.abbvie.com

Supported assessment · High

Reduce AppSec noise without disrupting developers

Emphasize correlation, deduplication, risk prioritization and remediation integration across AST, APIs, containers and CI/CD, rather than another isolated scanner.

WHY IT MATTERS

For AppSec, DevSecOps and engineering platform leaders.

Evidence date 2026-10-19 · careers.abbvie.com

Sources

Evidence in this report is drawn from investors.abbvie.com, careers.abbvie.com, abbvie.com, news.abbvie.com, sec.gov (AbbVie 2025 Form 10-K), ema.europa.eu, fda.gov, investor.lilly.com, jnj.com, revance.com. Each finding lists its source and evidence date.

Solution Brief

HermanEngage

CREATE OUTREACH WITH UNDERSTANDING

Make the first message relevant

Find and enrich relevant contacts, or turn existing lists into targeted, enriched data sources. HermanEngage™ uses HermanCQI,™ the Complete Quotient Indicator, to estimate contact profiles and shape outreach around the recipient. Prepare messages that give the conversation a stronger starting point.

The HermanScience™ insight

In a conversation, people adjust to feedback. Written outreach must earn a reply before that exchange can begin. HermanEngage uses estimated HermanCQI profiles to inform the first message, helping teams consider how a recipient may prefer to communicate.



The business challenge

- Poor targeting: broad, unsegmented lists waste effort and limit engagement.
- Fragmented channels: disconnected touchpoints create inconsistent experiences.
- Inefficient lead management: slow follow-up lets opportunities slip.
- Disconnected data: scattered tools hide useful insights and make return on investment harder to assess.

The HermanScience™ solution

HermanEngage combines audience discovery and enrichment with HermanCQI-informed engagement. Audience Finder prepares selected contacts, or teams begin with an approved list. Engagement Studio uses the engagement brief and estimated contact profiles to prepare reports and aligned outreach materials. Teams review and download the completed package. The data is yours.

Individual relevance in AI-assisted outreach

© 2026 HermanScience™. All rights reserved.

HOW IT WORKS

How it works

1. Find and enrich target contacts, or start with an approved list.

2. Define the engagement goal, audience, call to action and tone.

3. Select deliverables and optional sender style; review credits and launch.

4. HermanEngage uses HermanCQI to estimate contact profiles and align engagement messaging.

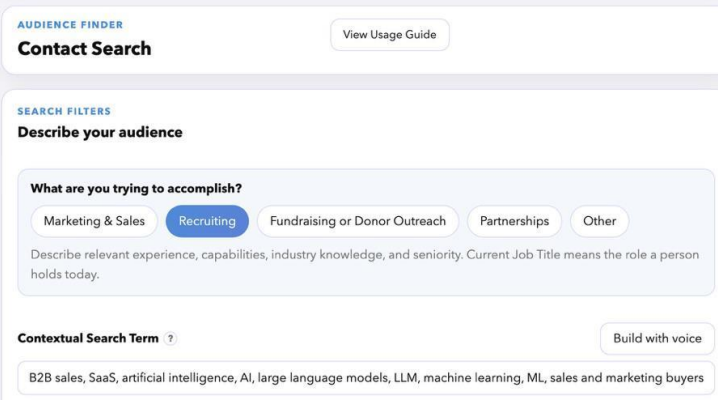
5. Download completed work within 24 hours and review it before use.

Key capabilities

- Audience Finder: define an audience, review candidates and enrich selected contacts.
- HermanCQI profiling: estimate target contacts' profiles to inform messaging.
- Profile reports: contact engagement guidance and cited company context.
- Engagement Cadences: aligned email, social, voicemail and phone materials.
- Build controls: optional sender style, credit estimates and progress tracking.

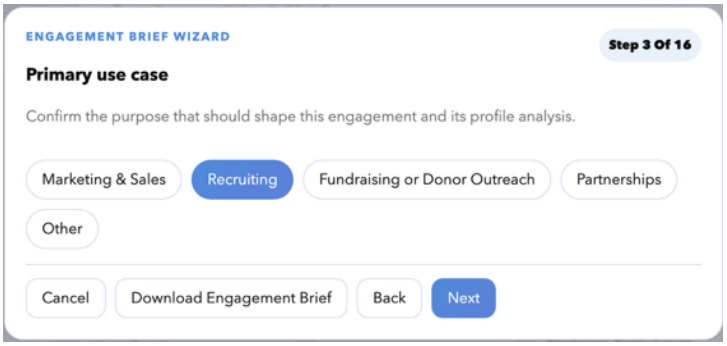
Start with Audience Finder or an approved contact list.
Imported contacts require valid LinkedIn URLs.

Audience Finder



Define whom you want to reach.

Engagement Studio



Set the purpose that guides your outreach.

Illustrative screens; interface may change.

Individual relevance in AI-assisted outreach

© 2026 HermanScience™. All rights reserved.

BUSINESS OBJECTIVES AND USE CASES

Business outcomes

- More relevant outreach through profile-aligned messaging.
- Improved response and engagement.
- Less repeated research and preparation.
- Lower outreach operating costs.
- Messages aligned with the goal and sender style.

Use cases

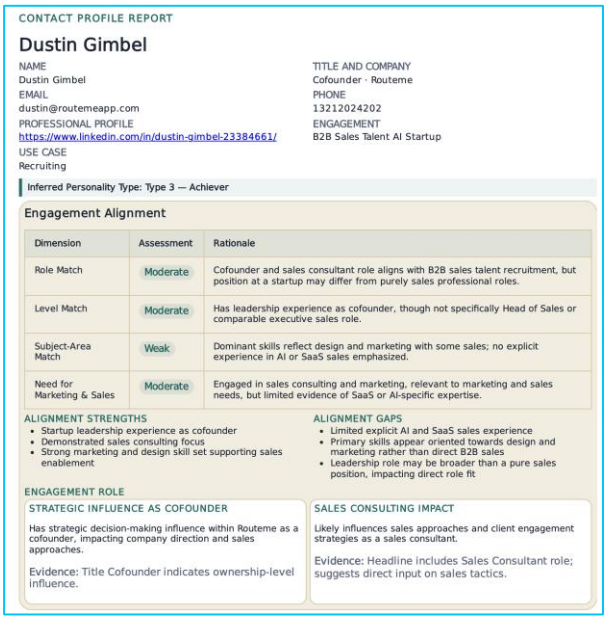
- Account-based outreach: combine company and contact context.
- Sales development: coordinate email, social and phone materials.
- Campaign planning: align work to an engagement brief.
- Existing-list activation: prepare contacts for targeted outreach.
- Move beyond broad programs to personalized engagement.

Relevance, repeatability and control

Relevance: use estimated contact profiles to inform individual messages.

Repeatability: one engagement brief guides multiple tailored reports and outreach materials.

Control: keep credit estimates, build progress and deliverable availability visible.


CONTACT PROFILE REPORT

Dustin Gimbel

NAME
Dustin Gimbel
EMAIL
dustin@routemeapp.com
PROFESSIONAL PROFILE
https://www.linkedin.com/in/dustin-gimbel-23384661/
USE CASE
Recruiting

TITLE AND COMPANY
Cofounder · Routeme
PHONE
13212024202
ENGAGEMENT
B2B Sales Talent AI Startup

Inferred Personality Type: Type 3 — Achiever

Engagement Alignment

Dimension	Assessment	Rationale
Role Match	Moderate	Cofounder and sales consultant role aligns with B2B sales talent recruitment, but position at a startup may differ from purely sales professional roles.
Level Match	Moderate	Has leadership experience as cofounder, though not specifically Head of Sales or comparable executive sales role.
Subject-Area Match	Weak	Dominant skills reflect design and marketing with some sales; no explicit experience in AI or SaaS sales emphasized.
Need for Marketing & Sales	Moderate	Engaged in sales consulting and marketing, relevant to marketing and sales needs, but limited evidence of SaaS or AI-specific expertise.

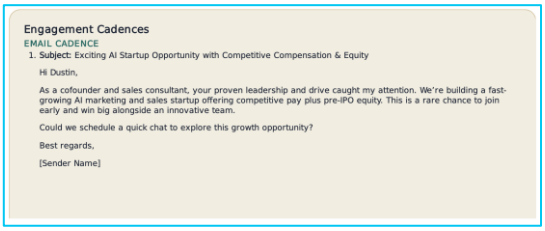
ALIGNMENT STRENGTHS
- Startup leadership experience as cofounder
- Demonstrated sales consulting focus
- Strong marketing and design skill set supporting sales enablement

ALIGNMENT GAPS
- Limited explicit AI and SaaS sales experience
- Primary skills appear oriented towards design and marketing rather than direct B2B sales
- Leadership role may be broader than a pure sales position, impacting direct role fit

ENGAGEMENT ROLE

STRATEGIC INFLUENCE AS COFOUNDER
Has strategic decision-making influence within Routeme as a cofounder, impacting company direction and sales approaches.
Evidence: Title Cofounder indicates ownership-level influence.

SALES CONSULTING IMPACT
Likely influences sales approaches and client engagement strategies as a sales consultant.
Evidence: Headline includes Sales Consultant role; suggests direct input on sales tactics.


Engagement Cadences

EMAIL CADENCE

1. **Subject:** Exciting AI Startup Opportunity with Competitive Compensation & Equity

Hi Dustin,

As a cofounder and sales consultant, your proven leadership and drive caught my attention. We're building a fast-growing AI marketing and sales startup offering competitive pay plus pre-IPO equity. This is a rare chance to join early and win big alongside an innovative team.

Could we schedule a quick chat to explore this growth opportunity?

Best regards,

[Sender Name]


Contact Profile: Dustin Gimbel

Professional Summary

Name: Dustin Gimbel

Title: Cofounder & Sales Consultant at Routeme

Email: dustin@routemeapp.com

Mobile: +1 321-202-4202

LinkedIn: https://www.linkedin.com/in/dustin-gimbel-23384661/

Location: Orlando, Florida, United States

Total Experience: 12+ years

Professional Experience
- Cofounder at Routeme
- Private-Label Sales Account Executive at Wash And Wik
- Marriott International (role unspecified)
- Digital & Print Designer at Live Nation Entertainment
- User Interface Designer at Allnean Inc.
- Advertising Graphic Designer at Nissan Motor Corporation
- Graphic Design Specialist at Shrw, Llc

Core Skills & Competencies
- Graphic Design and Adobe Creative Suite (Illustrator, Photoshop, InDesign)
- Social Media Marketing and Photography
- Web Design, User Interface Design, and Product Design
- Marketing Strategy and Art Direction
- Entrepreneurship and Leadership
- Strong communication with a sales consulting focus
- Technical skills including HTML and Microsoft Word

Recent LinkedIn Posts Highlights
- *"When the incumbents copy/paste your features and positioning - you know you're doing it right."*
- *"Real world context, Real world integrations, Real world navigation before you get there."*
- *"Just causally making power moves with SIXT."*

Contact Personality Profile Summary

Dustin values success, efficiency, and results. He is goal-oriented, driven, and professional with a distinct focus on leadership and delivering outcomes quickly. He appreciates clear, concise communication that is direct and impactful without unnecessary detail or emotional content. Dustin prefers professional discussions centered on achievement and progress, and values recognition for his performance.

Sample Contact Profile Report

Individual relevance in AI-assisted outreach

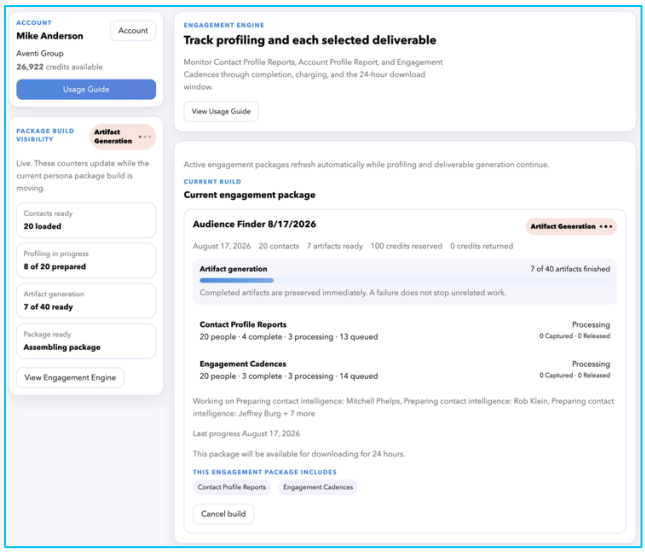
© 2026 HermanScience™. All rights reserved.

WHY HERMANSCIENCE

Why HermanScience™

HermanCQI is central to HermanEngage's approach. Beyond finding contacts and enriching their information, HermanEngage estimates each target contact's HermanCQI profile and uses it to shape engagement messaging. It connects audience selection with recipient-specific communication, while optional sender personalization lets teams choose their own communication style.

The data is yours. Download completed reports and outreach materials for your team to review and retain. Generated files are available for 24 hours. Keep downloaded files according to your organization's policies.



Engagement Engine

Explore HermanEngage

Explore how HermanEngage can support your next outreach initiative. Bring a target audience or an approved contact list to the discussion.

https://hermanengage.com

Contact: admin@hermanscience.com

Start every conversation with understanding.

The Human-AI Performance Layer

© 2026 HermanScience™. All rights reserved.