

Whisper



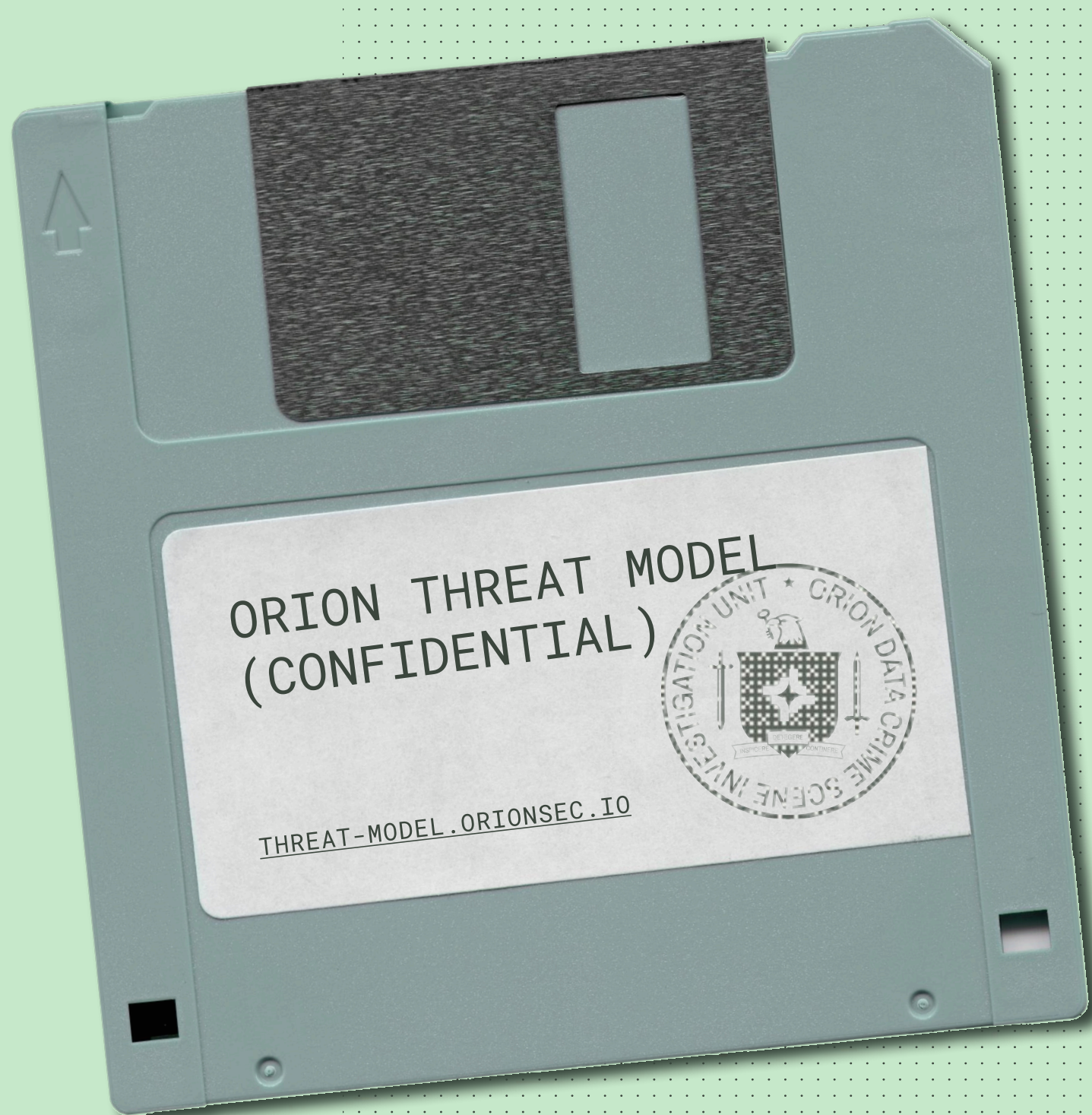
Data Loss Threat Model

A MODERN DATA LOSS THREAT MODELING
FRAMEWORK FOR THE AGE OF AI

*Freebies smell sweet
Loses my funding and
stay with enemies smile!*



ONLINE VERSION »» [THREAT-MODEL.ORIONSEC.IO](https://threat-model.orionsec.io)





How to use this guide

Data loss isn't a new problem. But the paths it takes keep multiplying. Every new tool your team adopts creates a potential new exfiltration path, making it harder than ever to stop sensitive data from leaving your organization.

The ORION Security Data Loss Threat Model gives security teams a full overview of the threat landscape as it exists today, from traditional challenges to new ones that emerged in the AI era.

When reading this guide, ask yourself these questions:

- Are these exfiltration paths relevant to my organization?
- Do I have visibility into these paths?
- Do I have the ability to prevent data exfiltration via these paths without blocking productivity?

This guide gives you a clear framework for assessing your organization's security requirements.

Data loss ends here.

ORION Security



Contents

Traditional DLP threat modeling

Traditional DLP threat modeling / Sources

Traditional DLP threat modeling / Destinations

T1. Wired upload to external storage

T2. Download to untrusted device

T3. Upload to untrusted application

T4. External share to an outsider

T5. External share with anonymous link

T6. Email to external recipient

T7. Direct message to external recipient

AI-era DLP threat modeling

AI-era DLP threat modeling / Sources+Destinations

A1. Submit or Upload to Shadow AI

A2. Access Granted to Enterprise Data

A3. Access Granted to Local Context

A4. Agents Use Unauthorized AI Service

A5. Unauthorized Skills Send Data with Unauthorized Services

A6. Shadow MCP Exfiltrates Enterprise Data via Coding Agent

A7. Agent or Browser Sharing Data with Unauthorized External Users

5

6

7

8

10

12

18

20

22

24

26

27

28

30

32

34

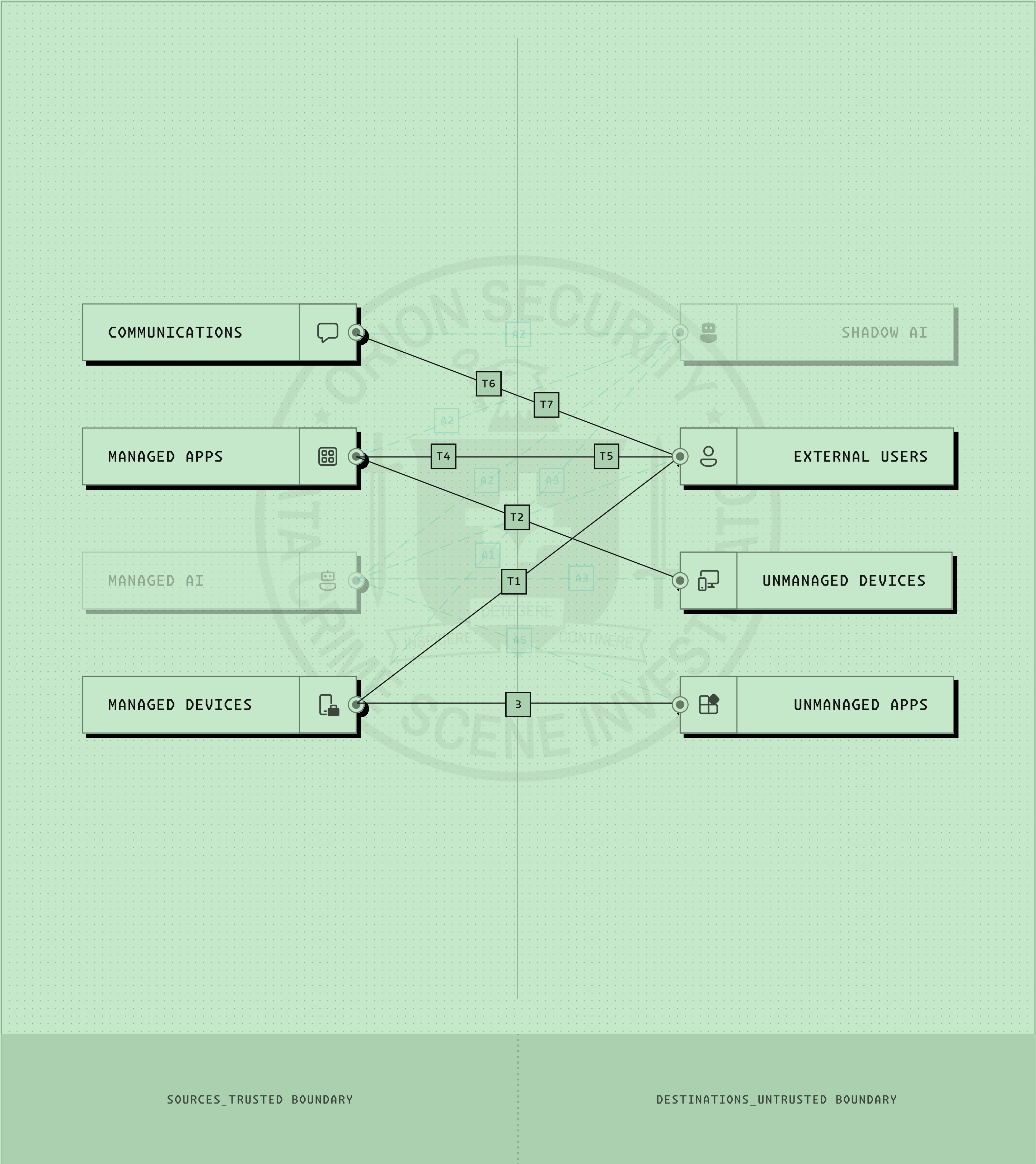
36

38

40



Traditional DLP threat modeling





Traditional DLP threat modeling / Sources

SOURCES // TRUSTED BOUNDARY			
	communications	Company-approved communication platforms used for business collaboration and communication.	    
	Managed Applications	Organization-approved applications and SaaS platforms that are governed by enterprise identity, security, compliance, and data protection controls.	File Storage & Content Repositories  Source Code & Development Platforms  CRM & Customer Systems  Work Management & Collaboration  Cloud Infrastructure & Development Platforms 
	Managed Devices	Corporate-managed endpoints and devices.	 



Traditional DLP threat modeling / Destinations

DESTINATIONS // UNTRUSTED BOUNDARY			
	external users	Individuals or organizations outside the enterprise trust boundary.	
	Unmanaged Applications	Applications, services, or SaaS platforms that are not approved, monitored, or governed by the organization.	Personal File Storage  File Transfer Services  Personal Development Platforms  Personal Communications  Personal Task Management Platforms 
	Unmanaged Devices	Devices that are not enrolled in or governed by enterprise security controls, regardless of ownership.	



Traditional DLP threat modeling / Use case

T1. Wired upload to external storage

Sensitive enterprise data is transferred from a managed device to an unmanaged physical device or peripheral outside enterprise governance.

EXAMPLE	ENFORCEMENT
Uploading customer data to a personal USB drive / external hard drive, printing confidential financial reports.	 BROWSER EXTENSION  ENDPOINT SENSOR

SOURCE	DESTINATION
 MANAGED DEVICES	 UNMANAGED DEVICES

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

T1.

WIRED UPLOAD TO EXTERNAL
STORAGE

SUMMARY :

A senior software engineer downloaded a code repository containing proprietary company source code from the company's GitHub environment, compressed it, and copied the archive to a personal USB storage device connected to a managed corporate laptop.

FILE :

 Auth.zip

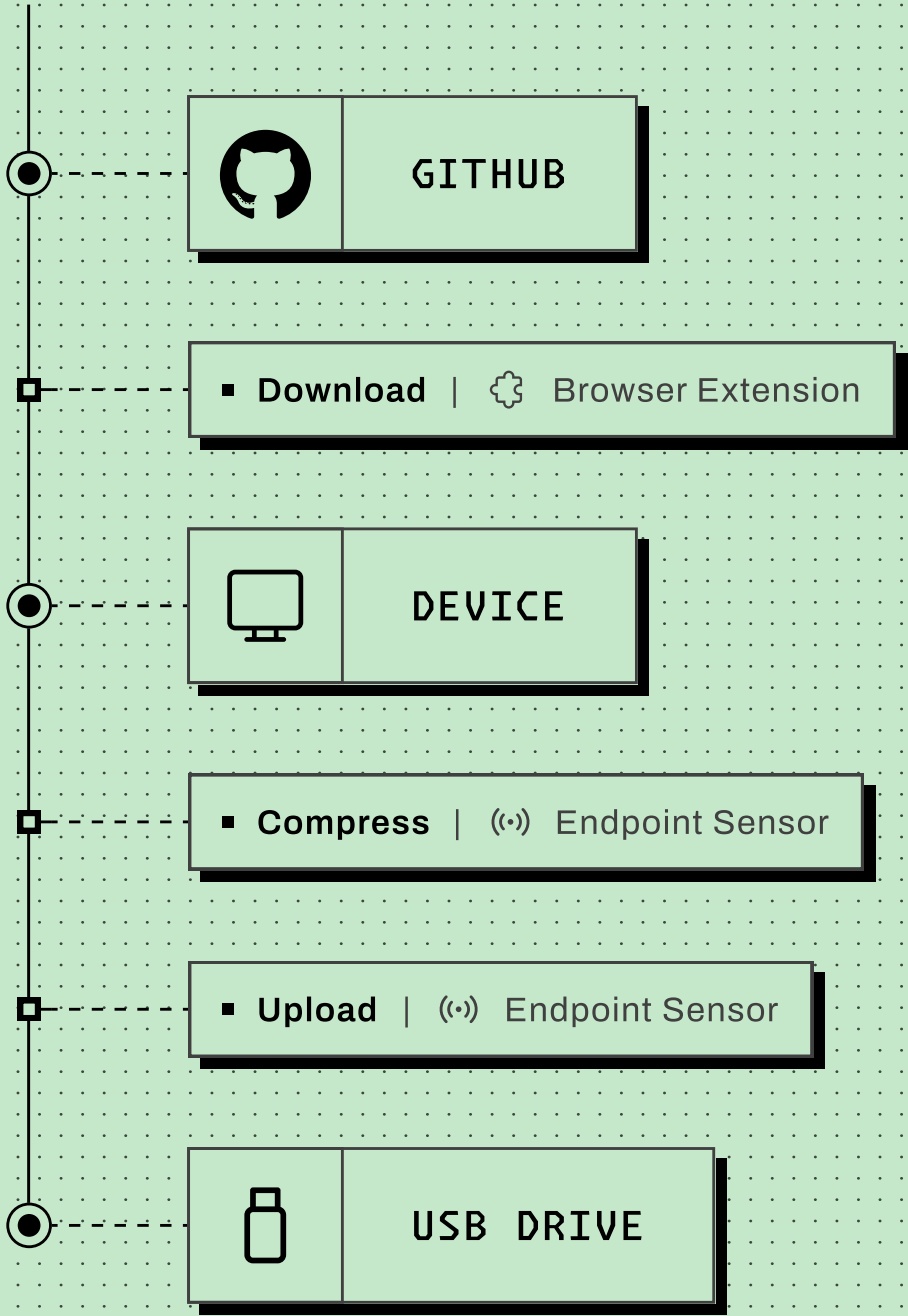
CONTENTS :

Proprietary company
source code

USER :

NAME : Michael Chen
ROLE : Senior Software Engineer
EMAIL : michael.chen@acme.com
DEPT : Engineering

TRACE



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY



Traditional DLP threat modeling / Use case

T2. Download to untrusted device

Users transfer enterprise data from managed systems to unmanaged devices where organizational security controls cannot be enforced.

EXAMPLE	ENFORCEMENT
Downloading source code to a personal laptop or confidential documents to a personal mobile device.	 API

SOURCE	DESTINATION
 MANAGED APPLICATION	 UNMANAGED DEVICE

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

T2.

DOWNLOAD TO UNTRUSTED
DEVICE

SUMMARY :

A sales employee accesses
and downloads a Salesforce
report to their personal
mobile device.

FILE :

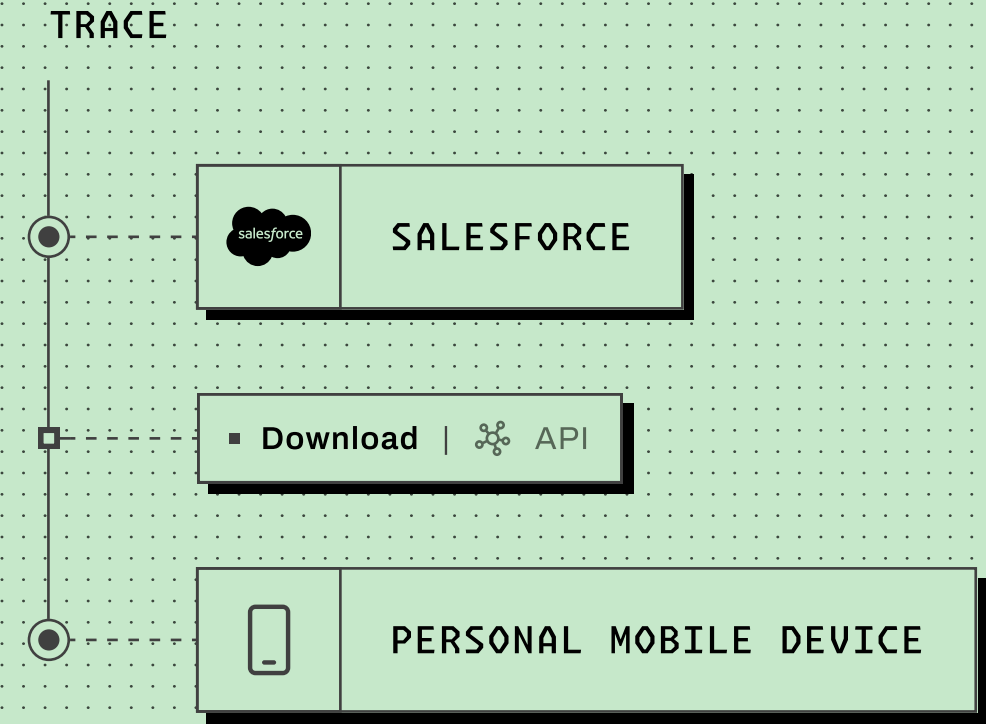
 enterprise-customers-q1.csv

CONTENTS :

Proprietary company
source code

USER :

NAME : Olivia Parker
ROLE : Strategic Account Executive
EMAIL : olivia.parker@company.io
DEPT : Sales



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY



Traditional DLP threat modeling / Use case

T3. Upload to untrusted application

Users submit enterprise data to unmanaged applications or services that are not approved or governed by the organization.

EXAMPLE	ENFORCEMENT
Uploading documents / copying information to personal Notion, GitHub, or consumer SaaS applications. Sending enterprise data via WhatsApp.	 BROWSER EXTENSION  ENDPOINT SENSOR

SOURCE	DESTINATION
 MANAGED DEVICES	 UNMANAGED DEVICE

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

T3.1

UPLOAD TO UNTRUSTED
APPLICATION

SUMMARY :

A radiology technician captures a screenshot of a diagnostic imaging system and uploads the image to a personal Google Drive account.

FILE :

 IMG_4821.png

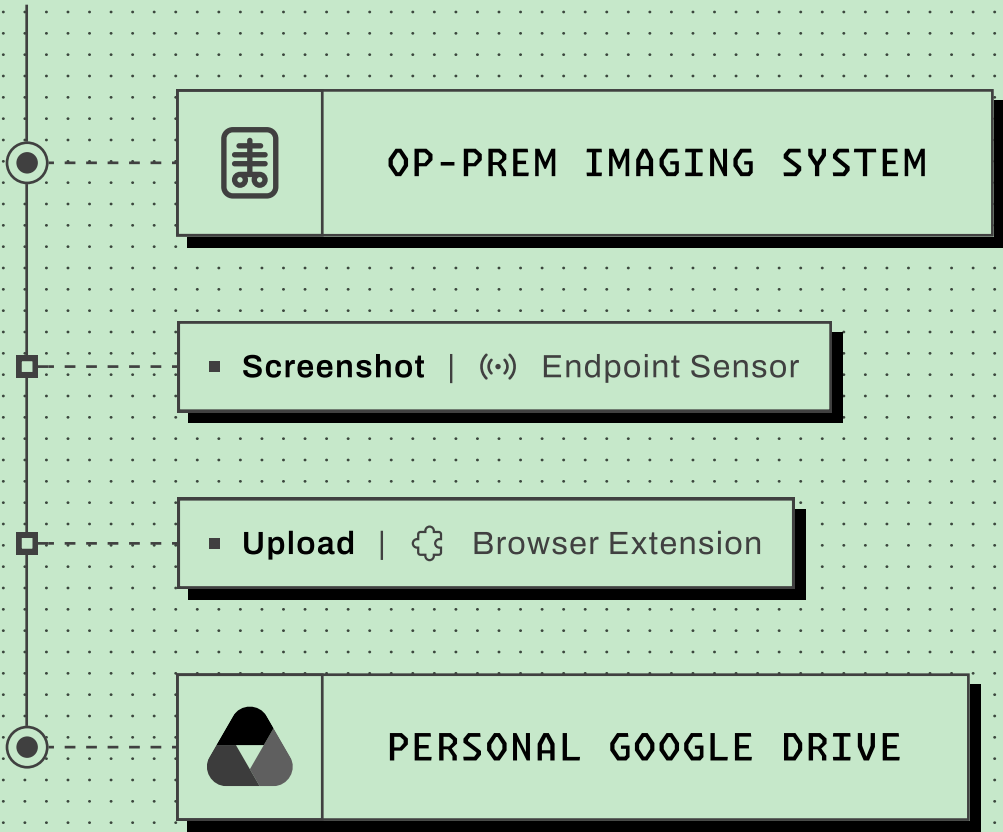
CONTENTS :

PHI - Patient chest X-ray image

USER :

NAME : Sarah Mitchell
ROLE : Radiology Technician
EMAIL : sarah.mitchell@hospital.org
DEPT : Diagnostic Imaging

TRACE



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

T3.2

UPLOAD TO FILE TRANSFER
SERVICE

SUMMARY :

A creative director exports an image from the company's digital asset management platform and uploads the file to WeTransfer.

FILE :

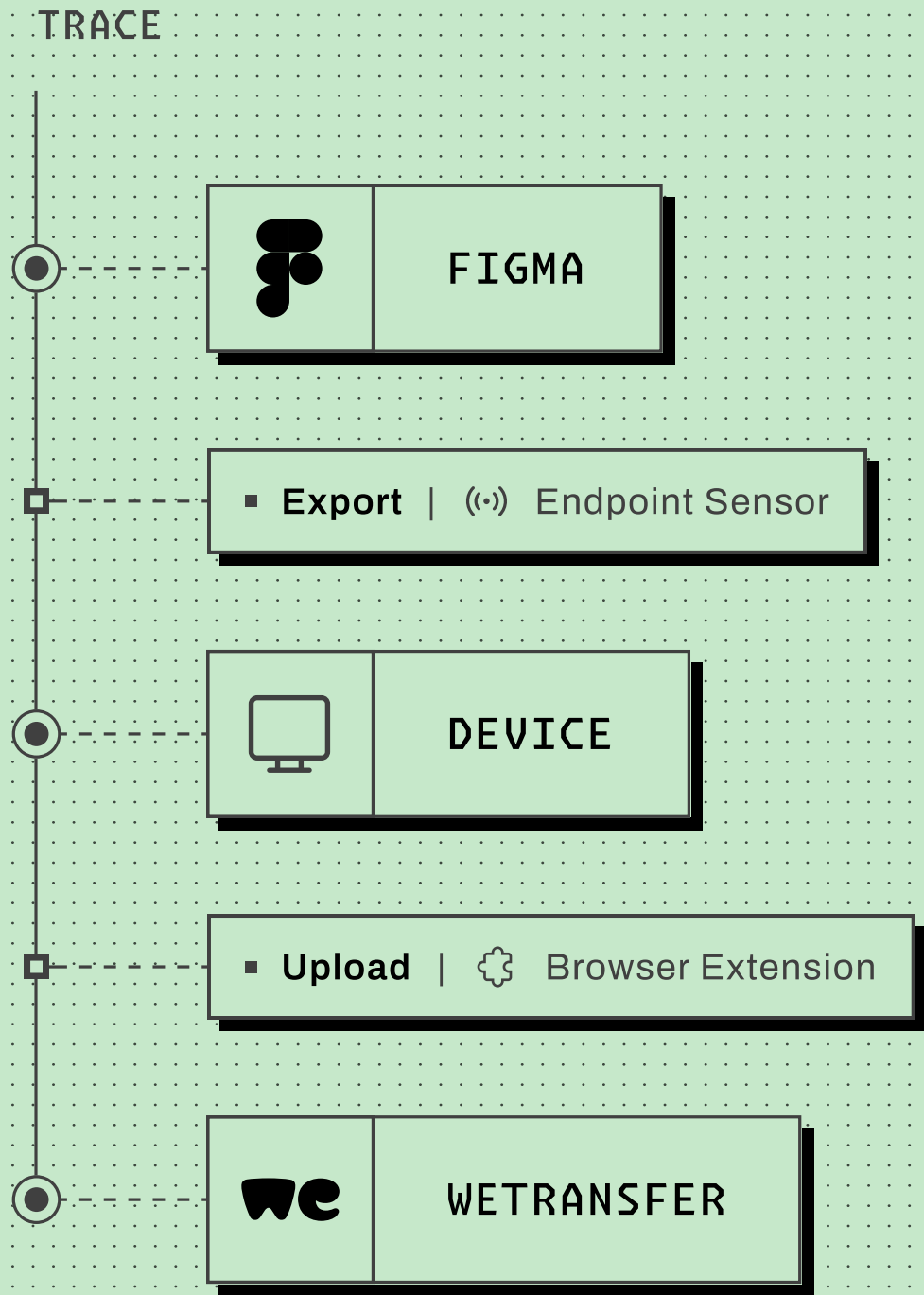
 final111.png

CONTENTS :

Unreleased advertising campaign

USER :

NAME : Emma Rodriguez
ROLE : Creative Director
EMAIL : emma.rodriguez@company.io
DEPT : Marketing



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

T3.3

UPLOAD TO PERSONAL
DEVELOPMENT PLATFORM

SUMMARY :

A DevOps engineer exports from the company's internal GitLab environment and uploads the archive to a personal GitHub repository.

FILE :

 infra-automation.zip

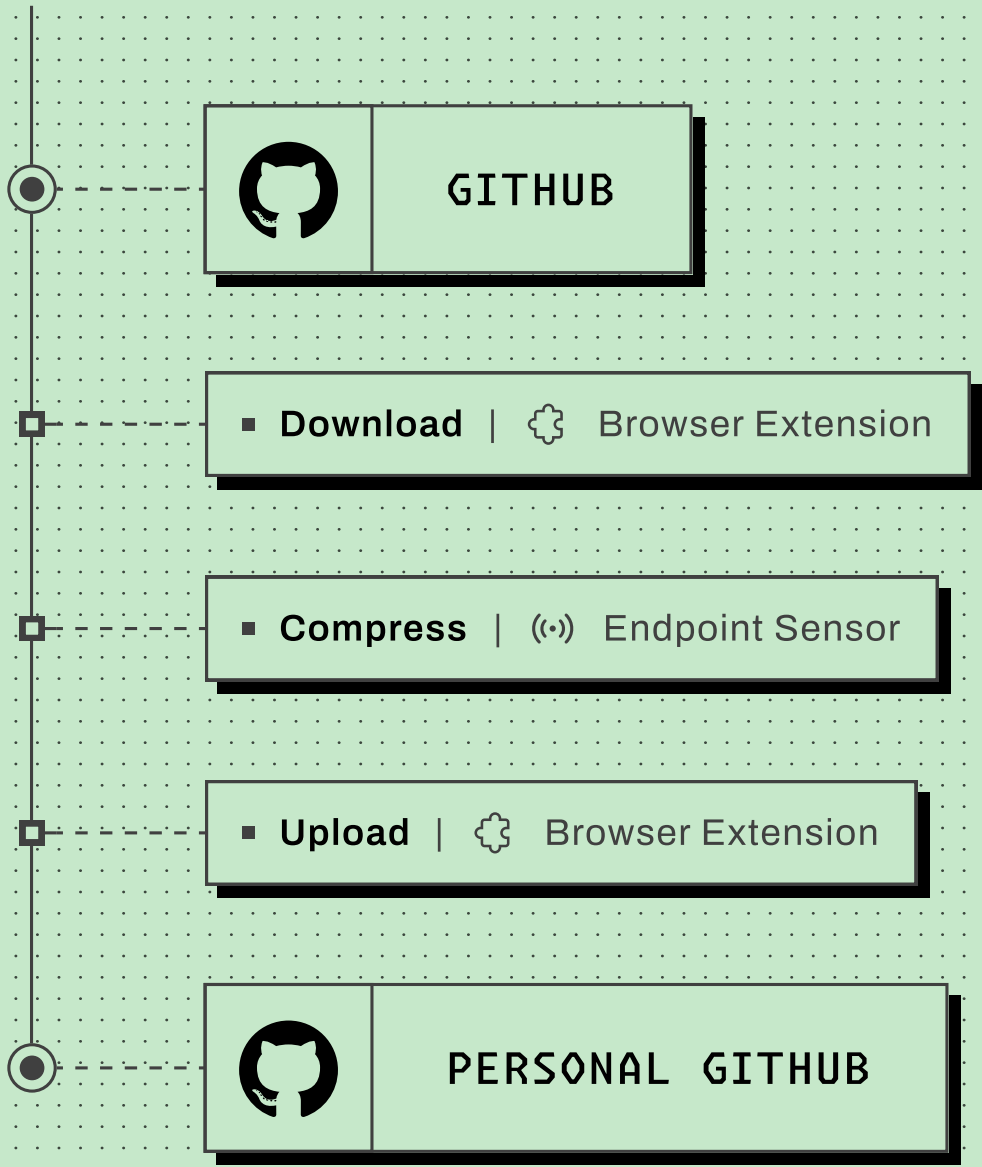
CONTENTS :

Repository containing infrastructure automation scripts and deployment templates

USER :

NAME : Daniel Wong
ROLE : Senior DevOps Engineer
EMAIL : daniel.wong@company.io
DEPT : Infrastructure Engineering

TRACE



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

T3.4

UPLOAD TO PERSONAL
COMMUNICATIONS APP

SUMMARY :

A product manager captures a
screenshot of a presentation
and sends the image to a
personal WhatsApp account.

FILE :

 Screenshot_250412_14231.png

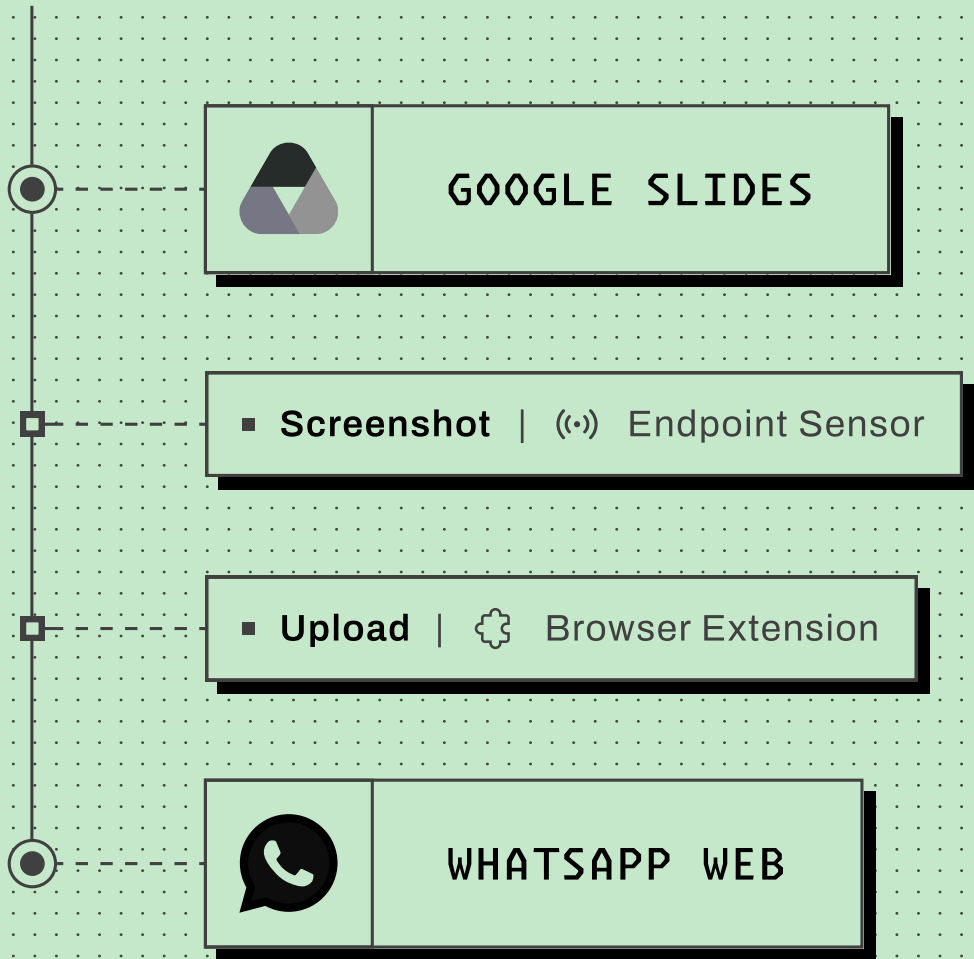
CONTENTS :

Image of internal roadmap containing
unreleased product features

USER :

NAME : Rachel Thompson
ROLE : Senior Product Manager
EMAIL : rachel.thompson@company.io
DEPT : Product

TRACE



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

T3.5

UPLOAD TO PERSONAL
WORKSPACE

SUMMARY :

An engineering manager
copies data from an internal
Google Slides presentation
and pastes the content into a
personal Notion workspace.

FILE :

 clipboard-detection-62508397

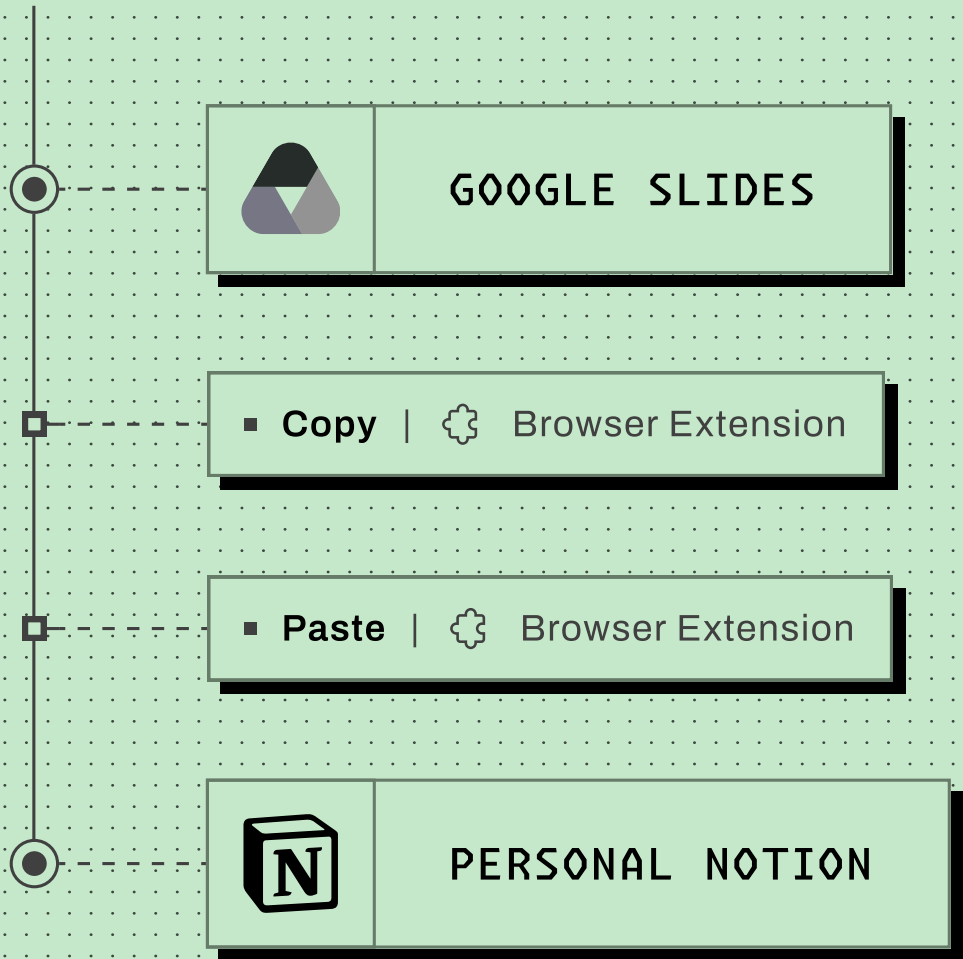
CONTENTS :

Employee compensation information -
annual compensation planning data

USER :

NAME : Jason Reed
ROLE : Engineering Manager
EMAIL : jason.reed@company.io
DEPT : Engineering

TRACE



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY



Traditional DLP threat modeling / Use case

T4. External share to an outsider

Users intentionally or unintentionally share sensitive enterprise data directly with external individuals or organizations.

EXAMPLE	ENFORCEMENT
Sharing a Google Drive folder with a customer, partner, contractor, or personal account.	 API

SOURCE	DESTINATION
 MANAGED APPLICATION	 EXTERNAL USER

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

T4

EXTERNAL SHARE TO AN
OUTSIDER

SUMMARY :

A customer success manager
shares a presentation from
Google Drive with their own
personal Gmail account.

FILE :

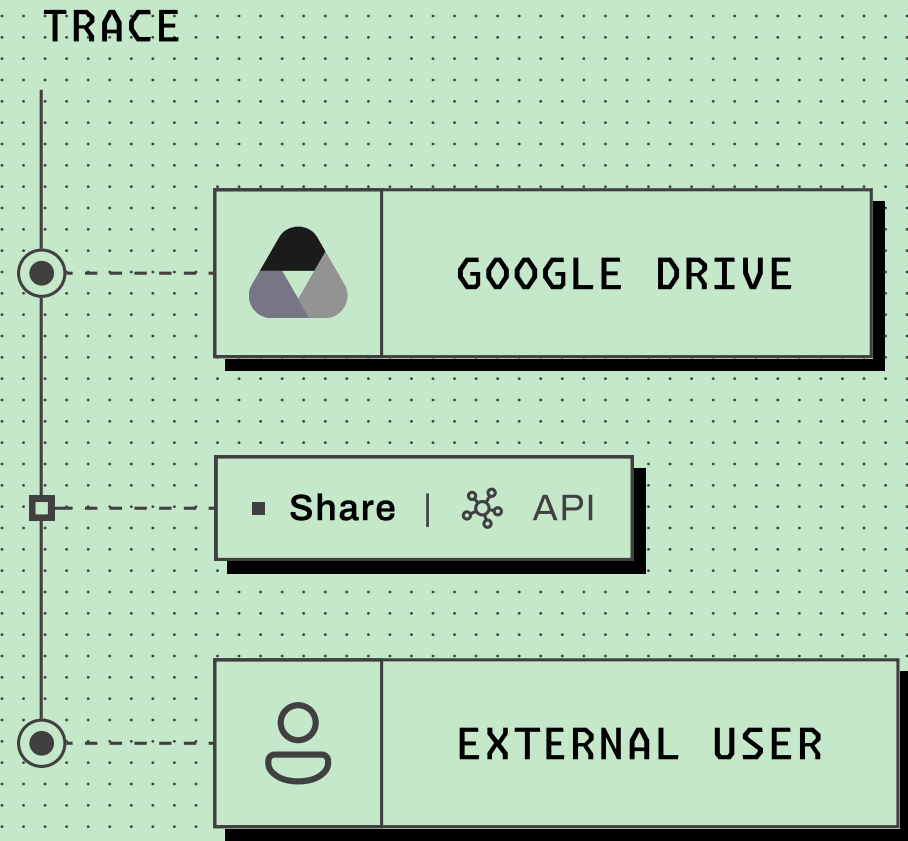
 customer-health-review-q2

CONTENTS :

Quarterly customer health review
containing customer usage metrics,
renewal forecasts, and account health
assessments

USER :

NAME : Emily Turner
ROLE : Customer Success Manager
EMAIL : emily.turner@company.io
DEPT : Customer Success



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY



Traditional DLP threat modeling / Use case

T5. External share with anonymous link

Users expose enterprise data through publicly accessible or anonymous sharing mechanisms that bypass identity-based access controls.

EXAMPLE	ENFORCEMENT
Creating an "Anyone with the link" share for a confidential document.	 API

SOURCE	DESTINATION
 MANAGED APPLICATION	 EXTERNAL USER

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

T5

EXTERNAL SHARE WITH
ANONYMOUS LINK

SUMMARY :

A finance manager duplicates
a Google Drive presentation
and creates an "Anyone with
the link" sharing link on the
copied file.

FILE :

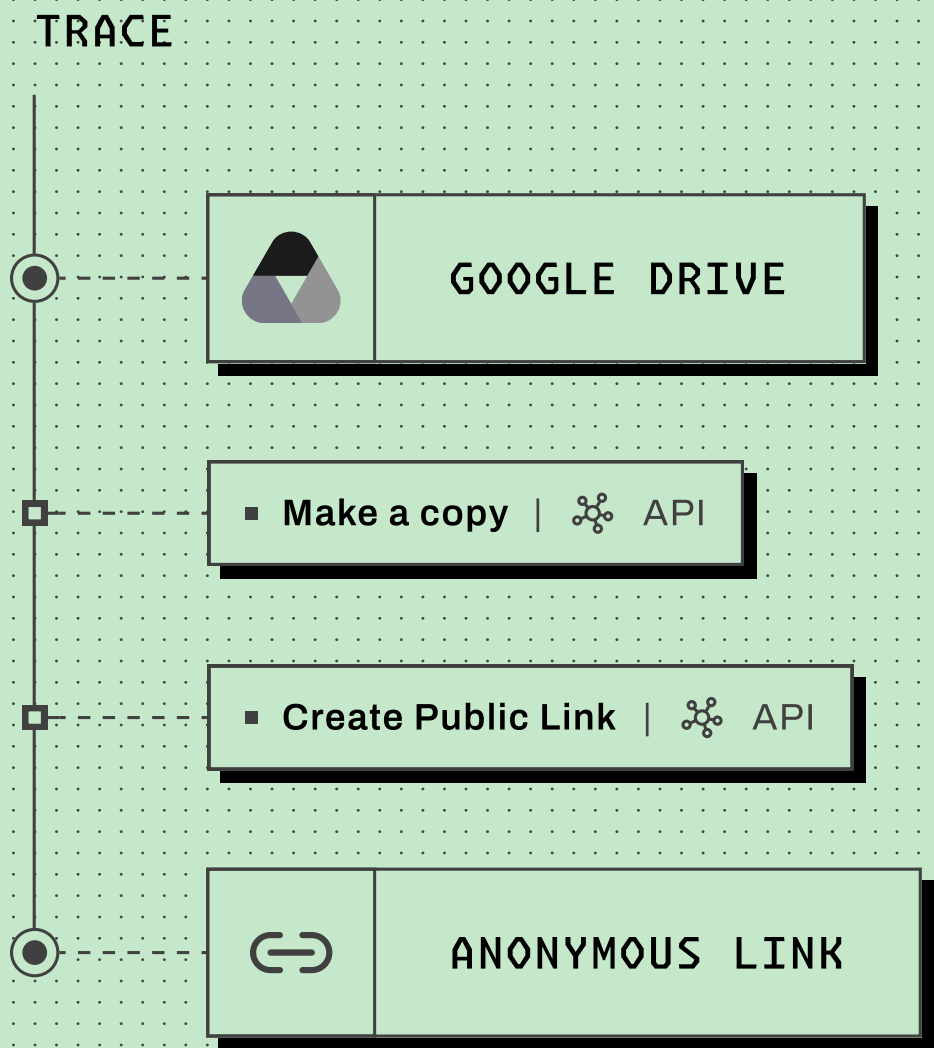
 board-update-q4-copy

CONTENTS :

Board presentation containing
revenue forecasts, acquisition plans,
and upcoming financial targets.

USER :

NAME : Alex Morgan
ROLE : Finance Manager
EMAIL : alex.morgan@company.io
DEPT : Finance



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY

Traditional DLP threat modeling / Use case

T6. Email to external recipient

Users transmit sensitive enterprise information to recipients outside the organization through email.

EXAMPLE	ENFORCEMENT
Sending customer records, source code, or financial reports to untrusted external email addresses.	 API

SOURCE	DESTINATION
 COMMUNICATIONS	 EXTERNAL RECIPIENT

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

T6

EMAIL TO EXTERNAL
RECIPIENT

SUMMARY :

An account executive
downloads a spreadsheet
from Salesforce via his
personal mobile device and
emails it to an external
consulting firm that used to
assist with sales strategy but
is no longer under an NDA.

FILE :

 customer-renewal-analysis.xlsx

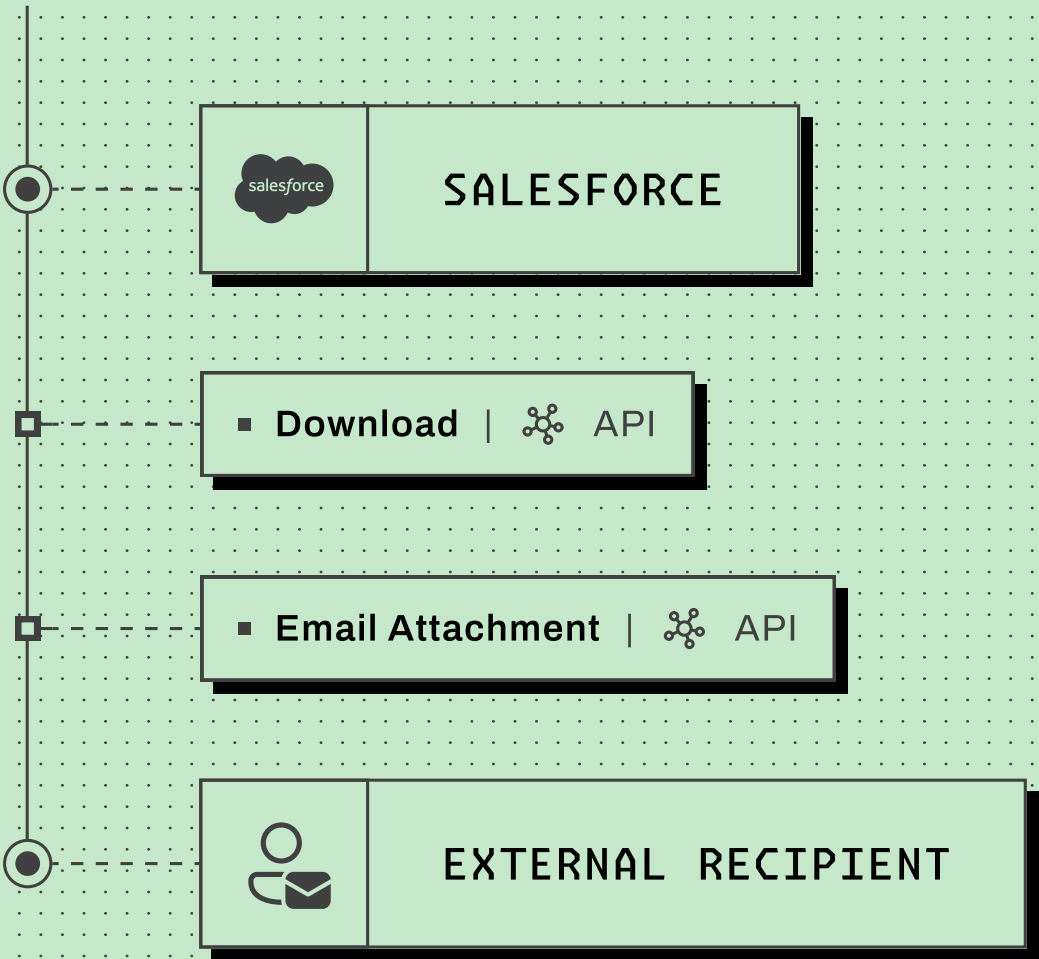
CONTENTS :

Spreadsheet containing renewal
probabilities, pricing concessions, and
customer health metrics

USER :

NAME : David Hughes
ROLE : Enterprise Account Executive
EMAIL : david.hughes@company.io
DEPT : Sales

TRACE

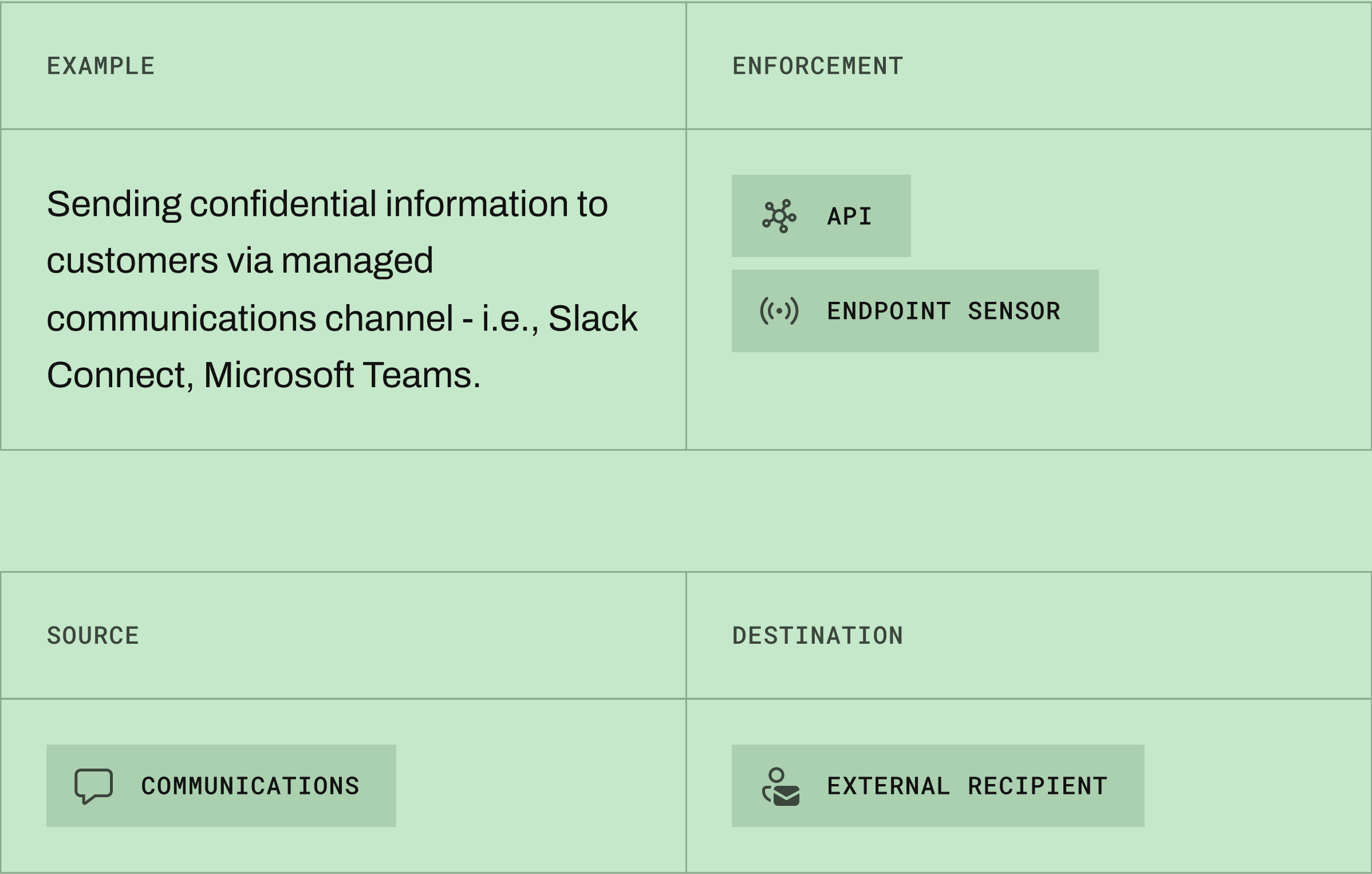


ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY

Traditional DLP threat modeling / Use case

T7. Direct message to external recipient

Users share sensitive enterprise information with external recipients through messaging or collaboration platforms.



INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

T7

DIRECT MESSAGE TO EXTERNAL
RECIPIENT

SUMMARY :

A product designer captures a screenshot of an internal development platform and sends it through a Slack Connect direct message to an external design agency.

FILE :

 Screenshot_2025_153412.png

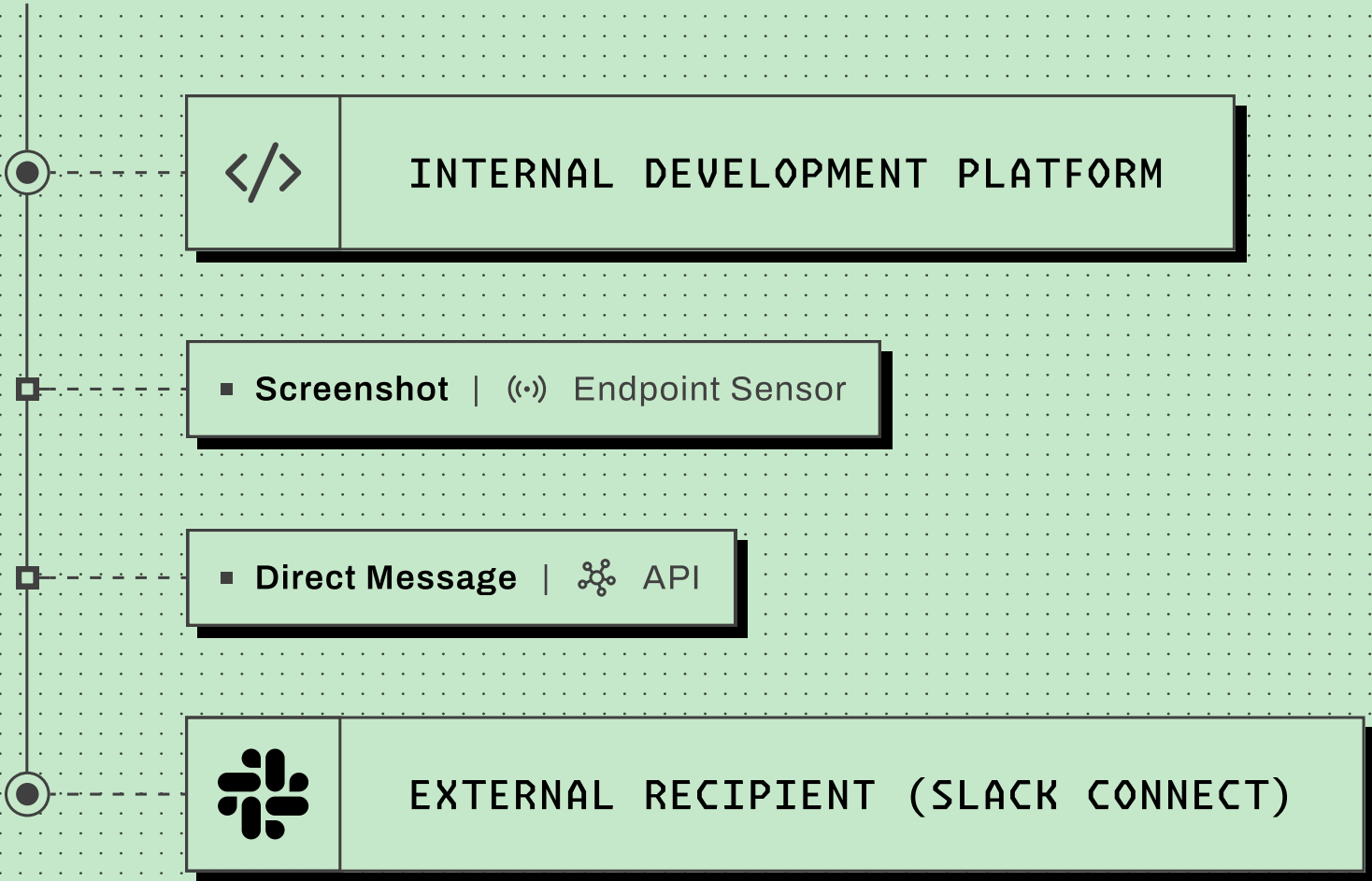
CONTENTS :

Screenshot of unreleased product features and user interface designs.

USER :

NAME : Sophia Nguyen
ROLE : Senior Product Designer
EMAIL : sophia.nguyen@company.io
DEPT : Product Design

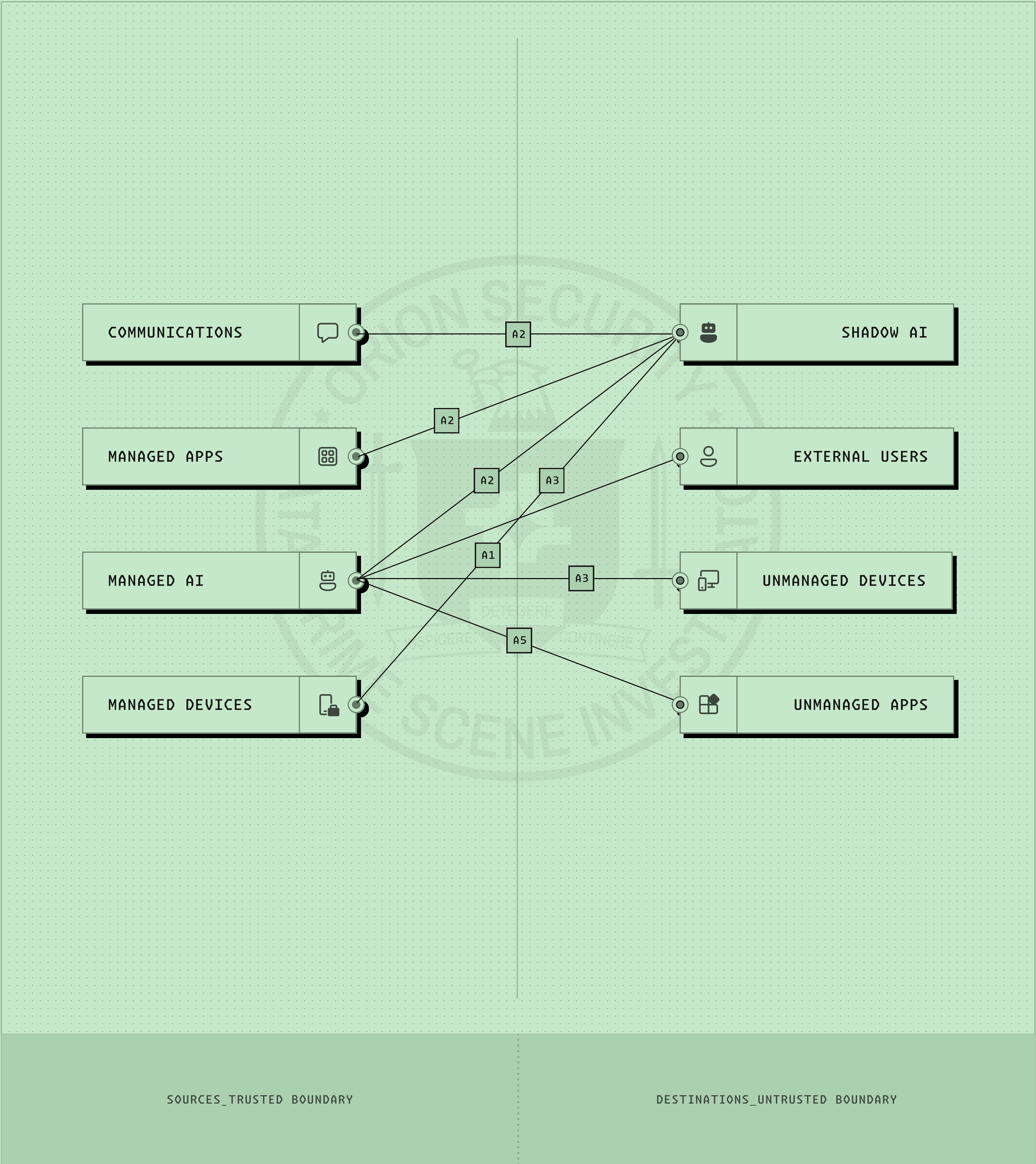
TRACE



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY



AI-era DLP threat modeling





AI-era DLP threat modeling / Sources+Destinations





AI-era DLP threat modeling / Use case

A1. Submit or Upload to Shadow AI

Users submit enterprise data directly to an unapproved AI application through prompts, file uploads, screenshots, recordings, or other inputs.

EXAMPLE	ENFORCEMENT
• Pasting source code into personal ChatGPT • Uploading a customer contract to personal Gemini • Submitting a screenshot of a medical record to Claude • Uploading a board presentation to Perplexity	 BROWSER EXTENSION

SOURCE	DESTINATION
 MANAGED DEVICE	 SHADOW AI

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

A1

SUBMIT OR UPLOAD TO
SHADOW AI

SUMMARY :

A customer success manager
shares a presentation from
Google Drive with their own
personal Gmail account.

FILE :

 statement-of-work-final.pdf

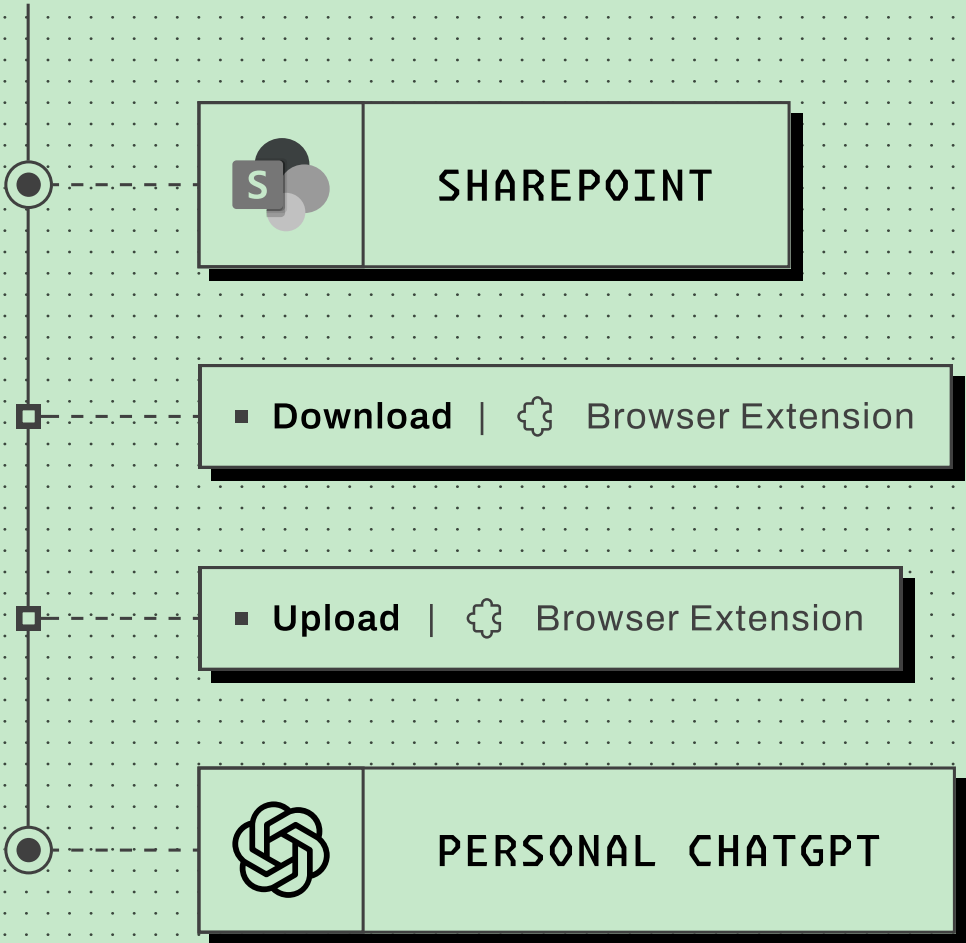
CONTENTS :

PDF containing confidential
compensation information for
subcontractors, project budgets, and
non-public project details.

USER :

NAME : Michael Bennett
ROLE : Senior Project Manager
EMAIL : michael.bennett@company.io
DEPT : Professional Services

TRACE



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY



AI-era DLP threat modeling / Use case

A2. Access Granted to Enterprise Data

A shadow AI application is connected to enterprise systems, allowing it to access, retrieve, or process organizational data through integrations, browser sessions, or connected repositories.

EXAMPLE	ENFORCEMENT
• Personal ChatGPT connected to corporate Google Drive • Personal Claude connected to SharePoint • AI browser accessing Salesforce through an authenticated session • Personal Cursor connected to company code repository	 API

SOURCE	DESTINATION
 MANAGED APPLICATION	 SHADOW AI

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

A2

ACCESS GRANTED TO
ENTERPRISE DATA

SUMMARY :

A marketing manager connects a personal ChatGPT account to the company's Google Drive to assist with campaign planning. After the connection is established, the AI gains access to sensitive data stored within the corporate environment.

FILE :

N/A

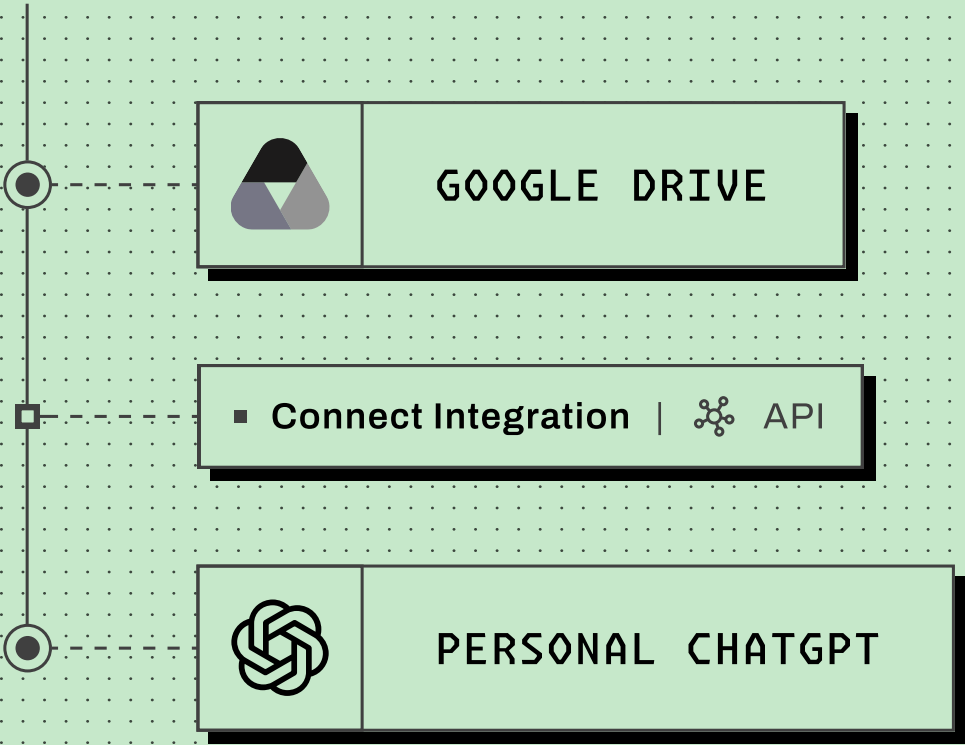
CONTENTS :

Customer presentations, marketing plans, budget spreadsheets, and sales enablement materials.

USER :

NAME : Olivia Harris
ROLE : Senior Marketing Manager
EMAIL : olivia.harris@company.io
DEPT : Marketing

TRACE



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY



AI-era DLP threat modeling / Use case

A3. Access Granted to Local Context

A shadow AI application, agent, browser, or coding assistant gains access to sensitive local files, source code, documents, clipboard contents, screenshots, or application context from a managed device.

EXAMPLE	ENFORCEMENT
• Personal Cursor indexing local source repositories • AI browser accessing downloaded contracts • AI assistant reading local project files	🔍 ENDPOINT SENSOR

SOURCE	DESTINATION
📱 MANAGED DEVICE	🤖 SHADOW AI

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

A3

ACCESS GRANTED TO LOCAL
CONTEXT

SUMMARY :

A software engineer installs a personal Cursor workspace on a managed corporate laptop and grants it access to the local development environment. The AI assistant indexes files stored on the device.

FILE :

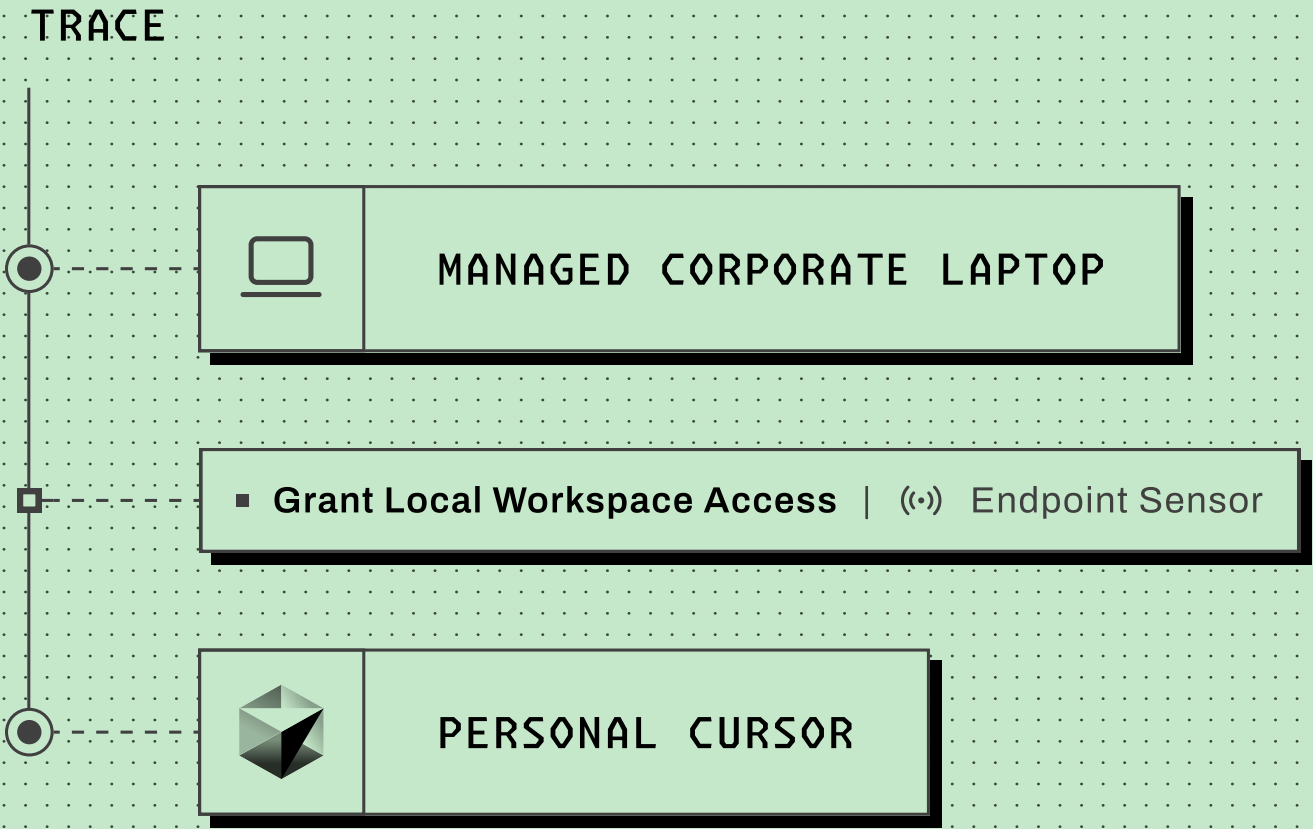
N/A

CONTENTS :

Source code repositories, engineering documentation, architecture diagrams, and configuration files

USER :

NAME : Daniel Cho
ROLE : Staff Software Engineer
EMAIL : daniel.cho@company.io
DEPT : Engineering



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY



AI-era DLP threat modeling / Use case

A4. Agents Use Unauthorized AI Service

A managed AI system sends enterprise data to an external AI service that has not been approved by the organization.

EXAMPLE	ENFORCEMENT
• Enterprise agent routing prompts to an unapproved LLM provider • Internal AI workflow invoking a consumer AI service • Enterprise copilot using an unauthorized model endpoint • Managed AI agent sending customer data to a third-party AI API	 API

SOURCE	DESTINATION
 MANAGED AI	 SHADOW AI

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

A4

AGENTS USE UNAUTHORIZED AI
SERVICE

SUMMARY :

A Salesforce Einstein agent receives a request to summarize a document to identify at-risk accounts. The agent routes the data to an unapproved Gemini API endpoint for additional analysis.

FILE :



customer-escalations-q2.xlsx

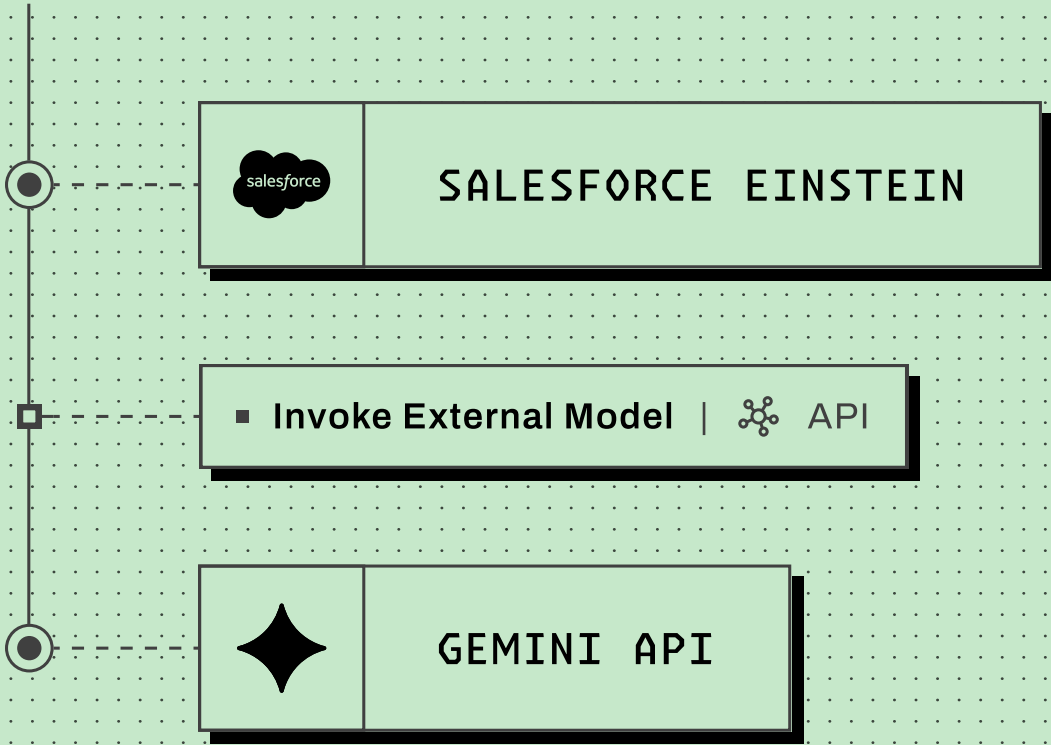
CONTENTS :

Spreadsheet containing customer escalations

USER :

NAME : Sarah Williams
ROLE : Director of Customer Success
EMAIL : sarah.williams@company.io
DEPT : Customer Success

TRACE



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY



AI-era DLP threat modeling / Use case

A5. Unauthorized Skills Send Data with Unauthorized Services

A managed AI agent executes a skill, tool, plugin, extension, or connector that transfers enterprise data to an unauthorized destination.

EXAMPLE	ENFORCEMENT
• A malicious skill is used to make Cursor send data to an unauthorized service • A custom GPT invokes an external action to write enterprise data to an unmanaged SaaS application	 API  BROWSER EXTENSION

SOURCE	DESTINATION
 MANAGED AI	 UNMANAGED APPLICATION

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

A5

UNAUTHORIZED SKILLS SEND
DATA WITH UNAUTHORIZED
SERVICES

SUMMARY :

A finance analyst uses an enterprise AI assistant to analyze a document. During the analysis, the assistant invokes an unauthorized MCP server that writes financial data to a personal Notion workspace.

FILE :

 fy26-budget-forecast.xlsx

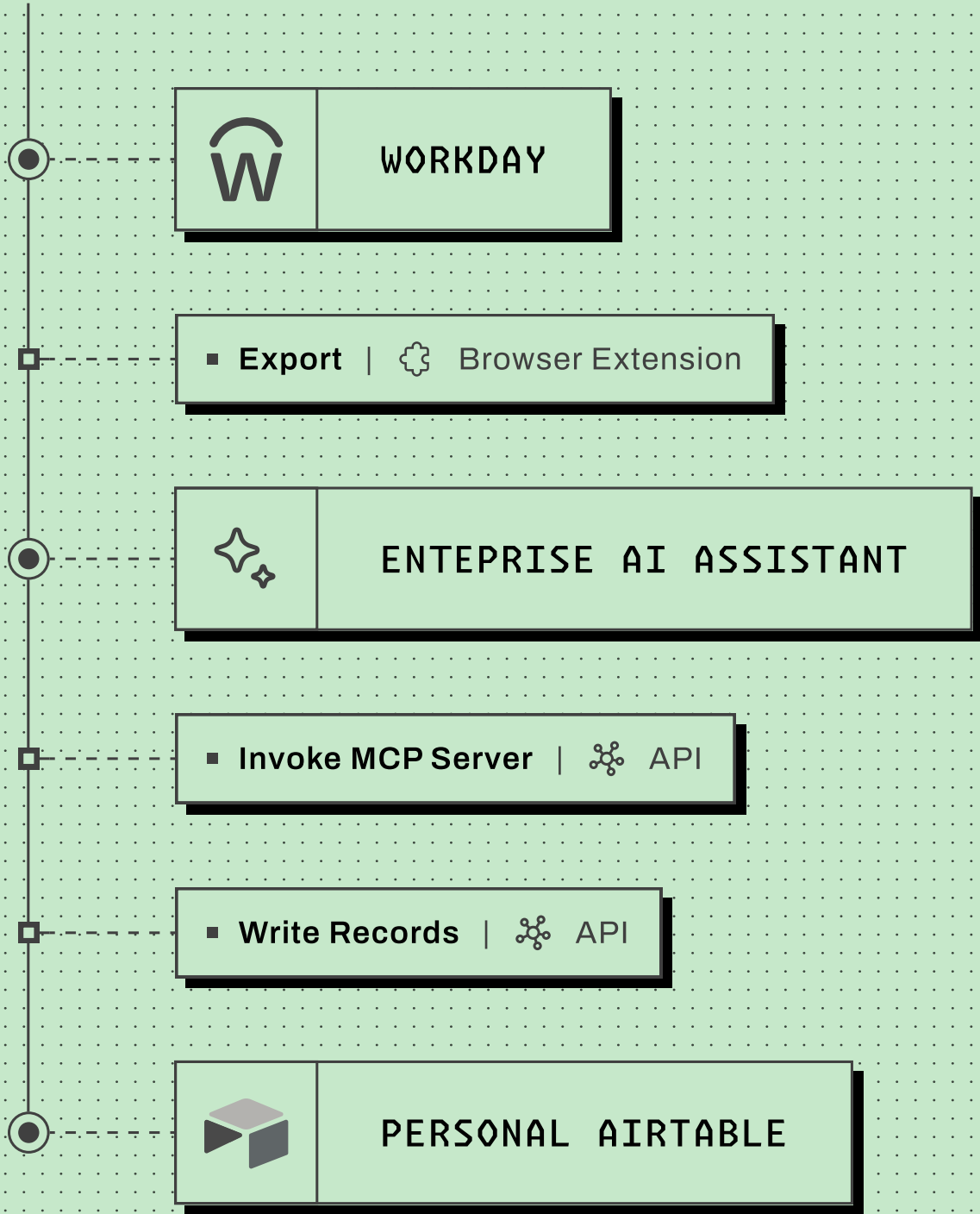
CONTENTS :

Spreadsheet containing departmental budgets, hiring plans, operating expenses, and revenue projections.

USER :

NAME : Emily Watson
ROLE : Senior Financial Analyst
EMAIL : emily.watson@company.io
DEPT : Finance

TRACE



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY



AI-era DLP threat modeling / Use case

A6. Shadow MCP Exfiltrates Enterprise Data via Coding Agent

A user connects an unapproved MCP server to a managed AI coding agent. The MCP server acts as a bridge, pulling enterprise data from authorized sources and routing it to an unauthorized external destination outside organizational governance and visibility.

EXAMPLE	ENFORCEMENT
• A personal MCP server connected to Claude Code reading local source repositories and transmitting contents to an external endpoint • An unapproved MCP connector pulling files from corporate Google Drive through a coding agent into an uncontrolled third-party service • A shadow MCP tool exfiltrating authentication credentials and architecture documents to an attacker-controlled server	 API  ENDPOINT SENSOR

SOURCE	DESTINATION
 MANAGED AI	 UNMANAGED APPLICATION

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

A6

SHADOW MCP EXFILTRATES
ENTERPRISE DATA VIA CODING
AGENT

SUMMARY :

A software engineer installs Claude Code on a managed corporate laptop and configures an unapproved MCP server to extend the assistant's capabilities. The MCP server requests access to the engineer's local development environment and Google Drive to provide additional coding context. Once connected, the server reads sensitive data stored locally on the drive and transmits it to an external server controlled by the MCP provider outside of the organization.

FILE :

 api-specs-internal.zip

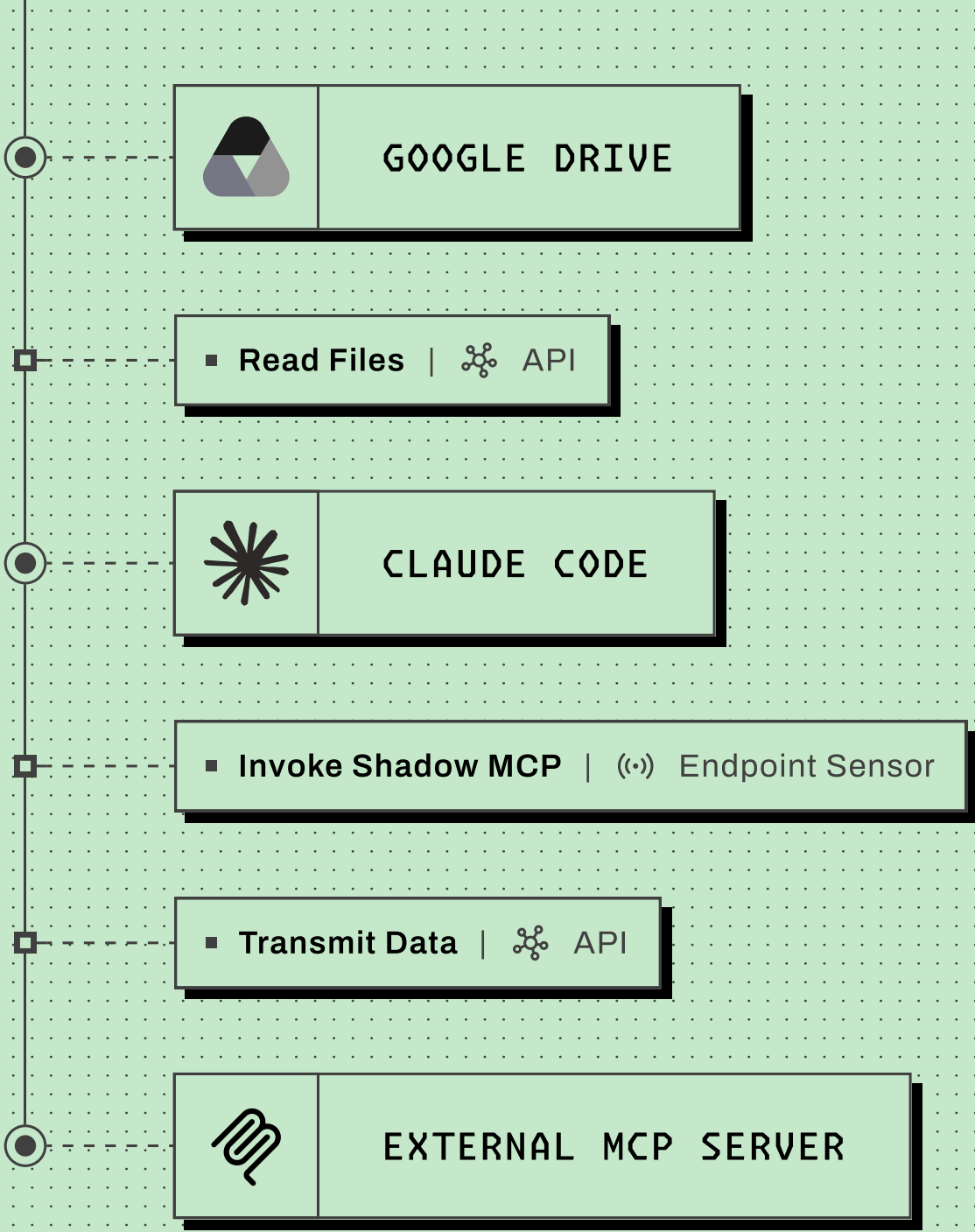
CONTENTS :

Internal architecture documents,
API specifications, and
authentication secrets.

USER :

NAME : Marcus Bell
ROLE : Senior Software Engineer
EMAIL : marcus.bell@company.io
DEPT : Engineering

TRACE



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY



AI-era DLP threat modeling / Use case

A7. Agent or Browser Sharing Data with Unauthorized External Users

An AI assistant, browser, or autonomous agent shares enterprise data with external users through generated content, automated communications, document modifications, or workflow actions.

EXAMPLE	ENFORCEMENT
• AI agent emailing confidential roadmap information to a customer • AI browser sharing Salesforce records with an external party • Autonomous workflow posting confidential information to an external channel	 BROWSER EXTENSION

SOURCE	DESTINATION
 MANAGED AI	 EXTERNAL USERS

INCIDENT EXAMPLE

TRADITIONAL DLP THREAT
MODELING / USE CASES

A7

AGENT OR BROWSER SHARING
DATA WITH UNAUTHORIZED
EXTERNAL USERS

SUMMARY :

A product manager asks an enterprise AI assistant to prepare a customer update summarizing upcoming product enhancements. While generating the response, the assistant includes confidential information sourced from internal product planning systems. The generated document is automatically emailed to a customer.

FILE :

roadmap-summary.docx

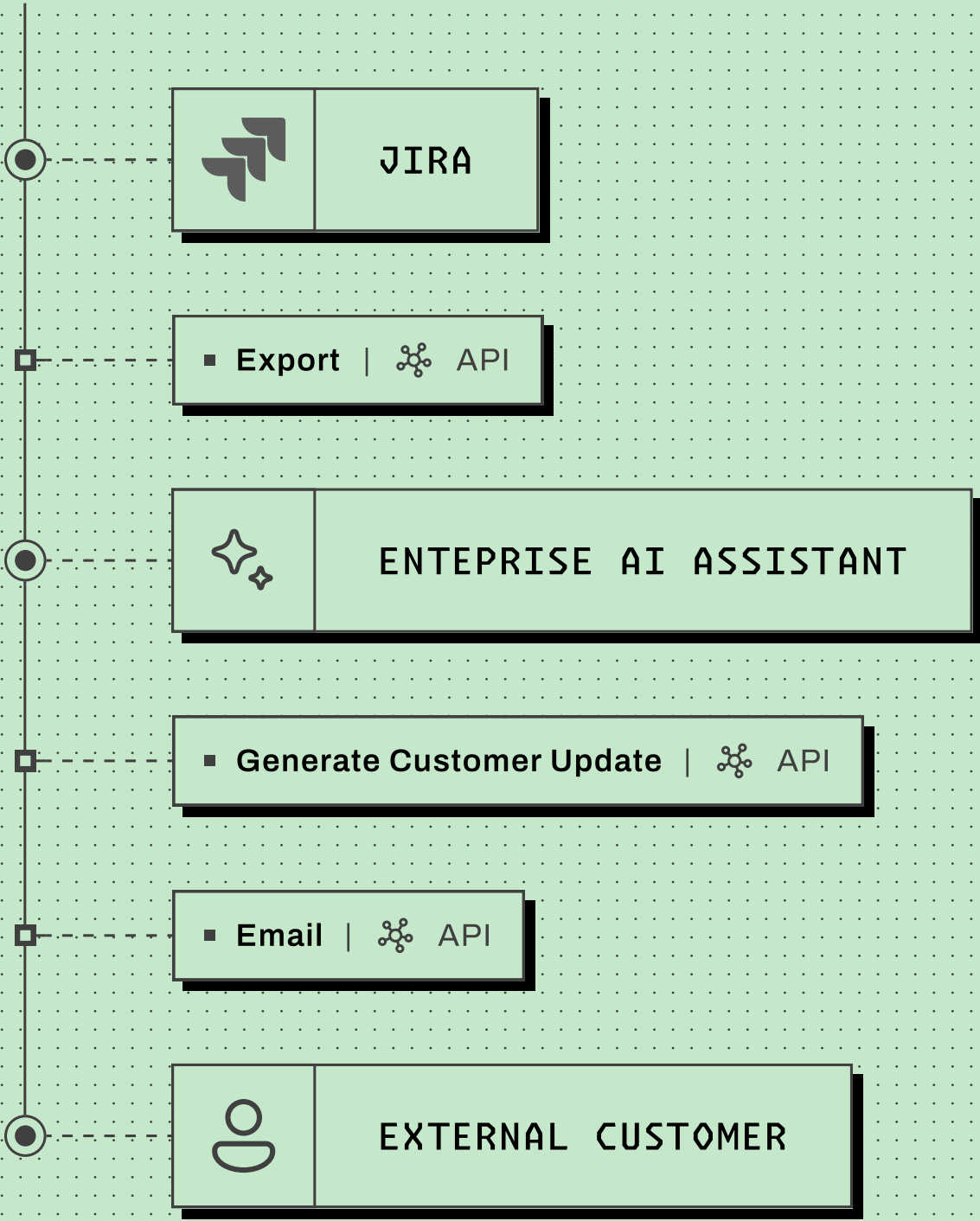
CONTENTS :

Information about unreleased features and planned launch dates.

USER :

NAME : Ryan Mitchell
ROLE : Senior Product Manager
EMAIL : ryan.mitchell@company.io
DEPT : Product

TRACE



ALL USE CASES ARE BASED ON REAL
DETECTIONS MADE BY ORION SECURITY

