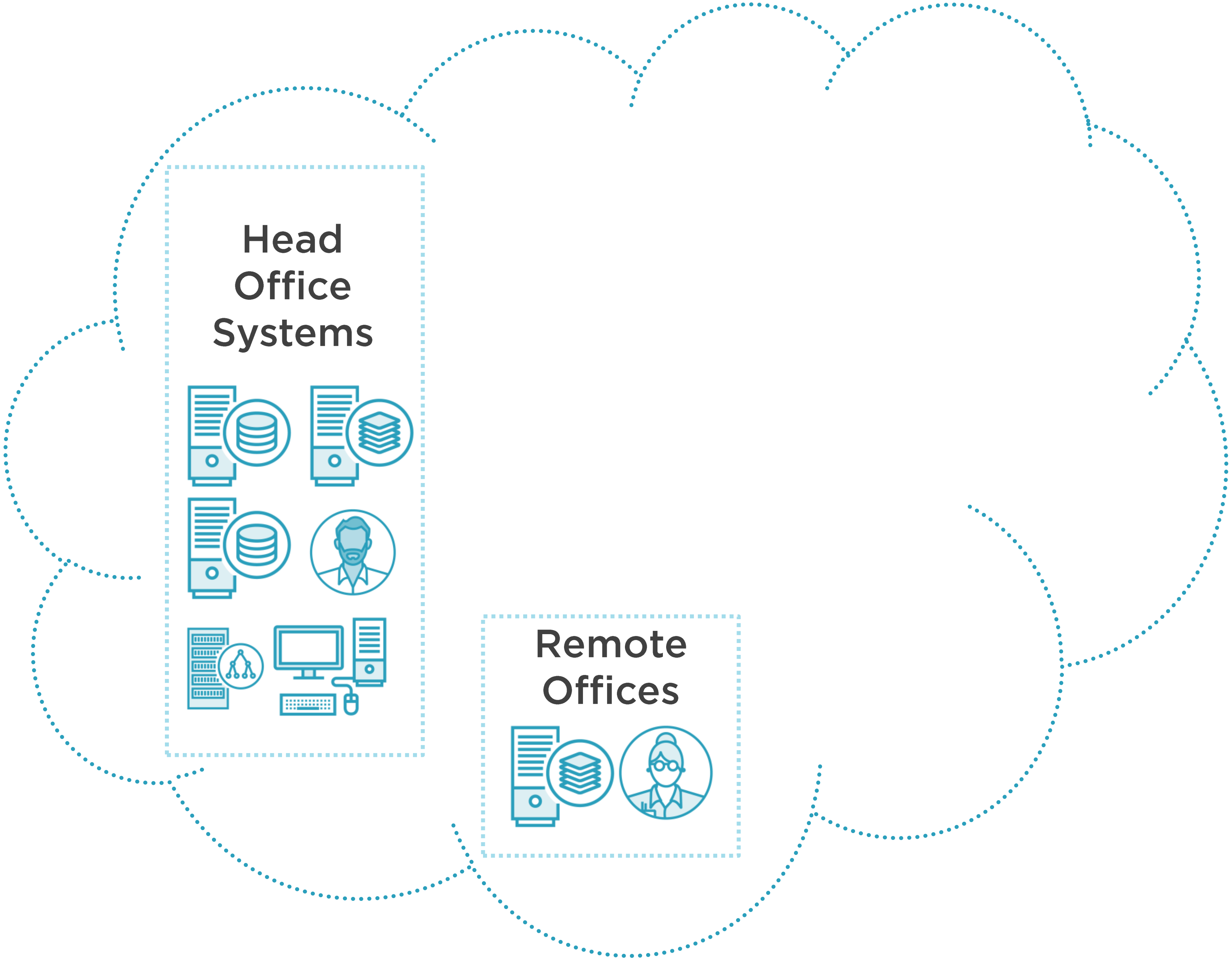
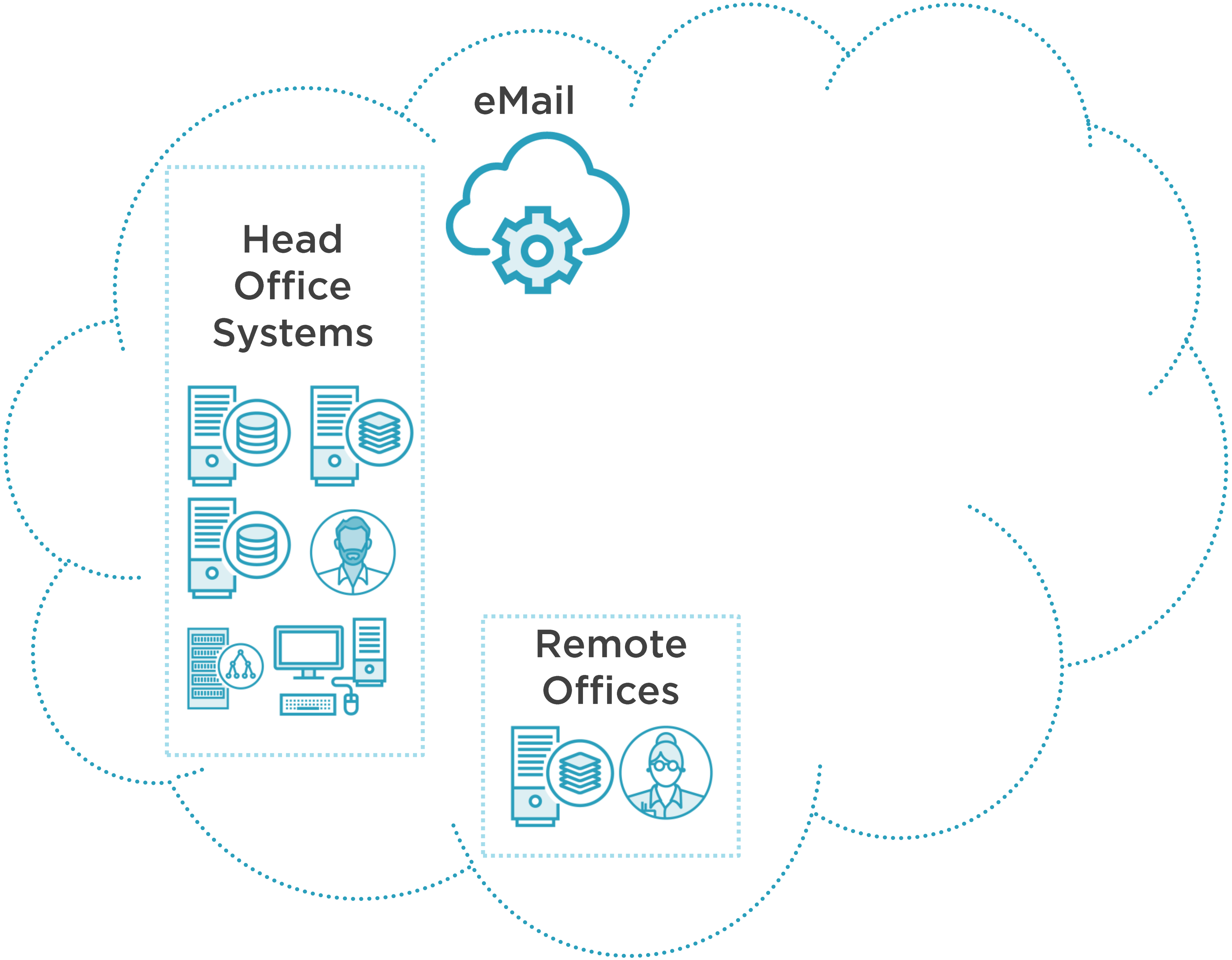
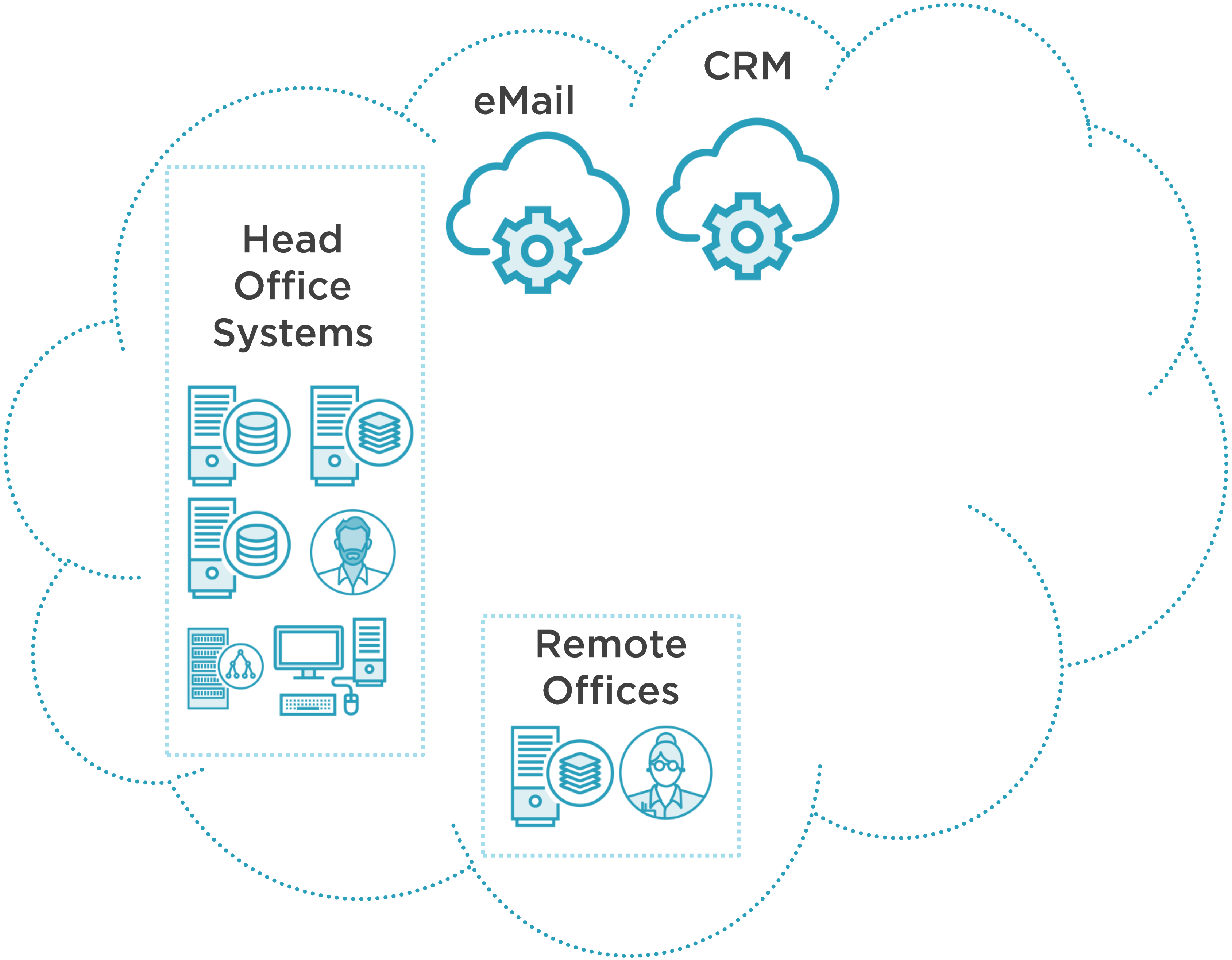

Head Office Systems
Remote Offices



eMail

Head Office Systems

Remote Offices

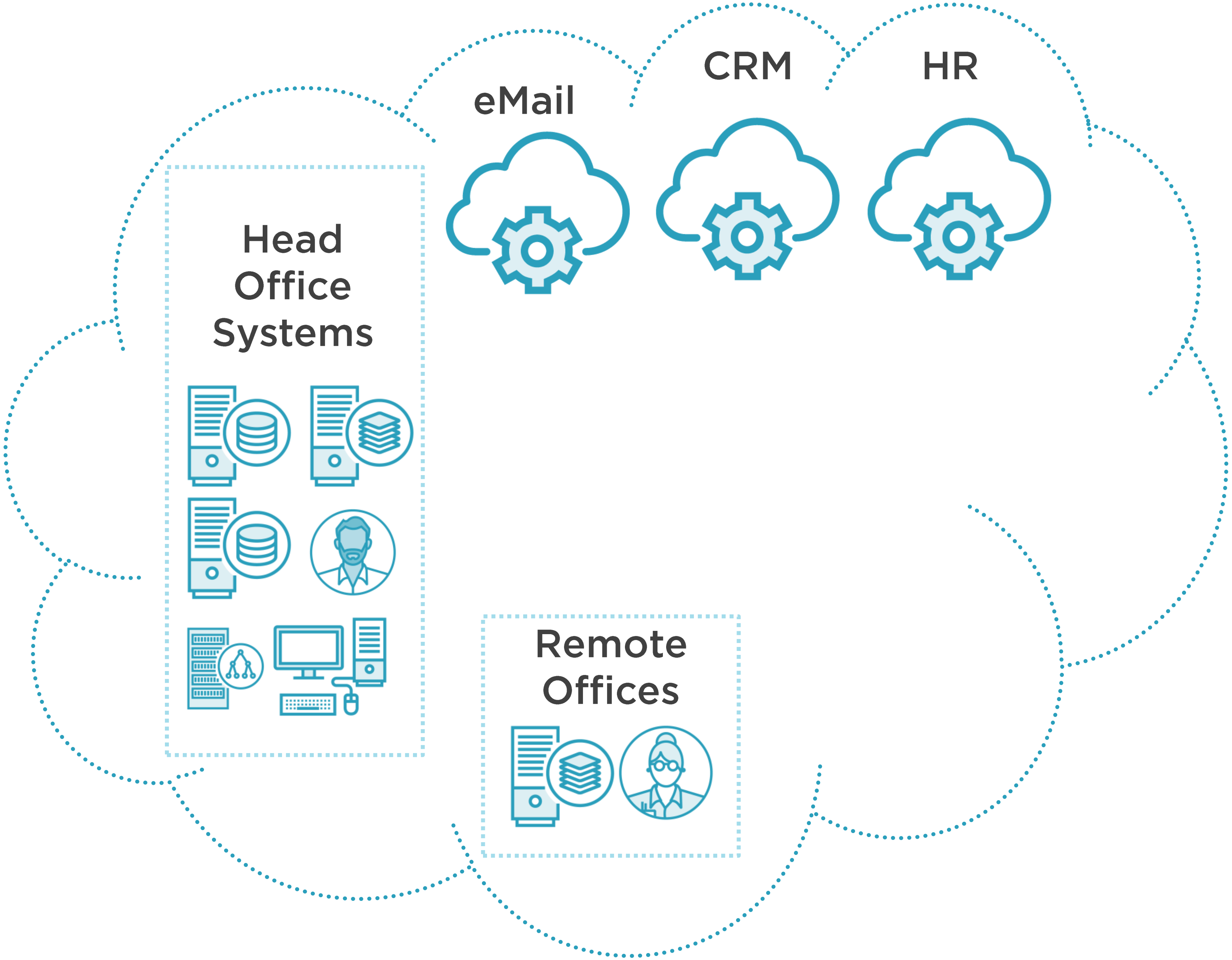


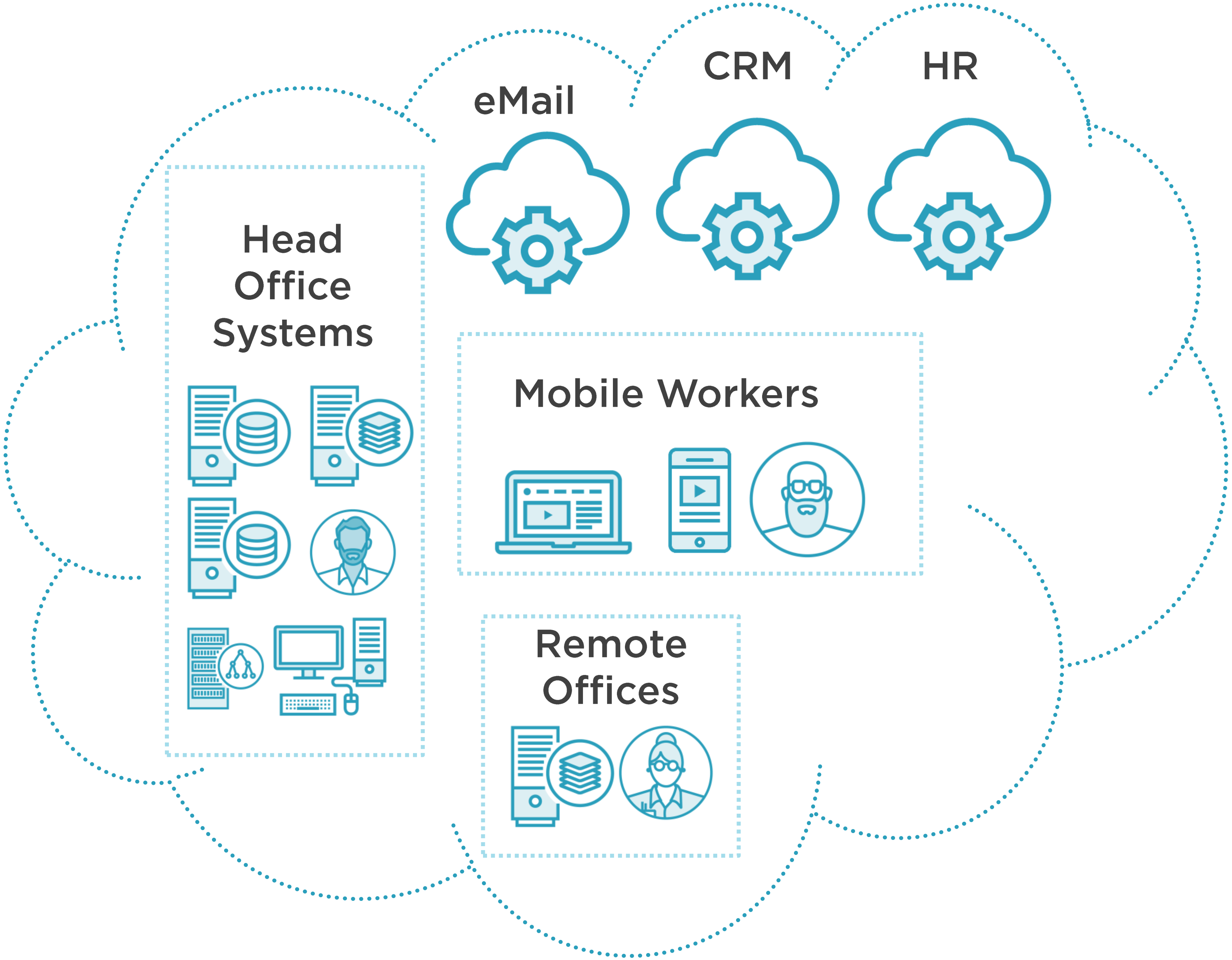
eMail

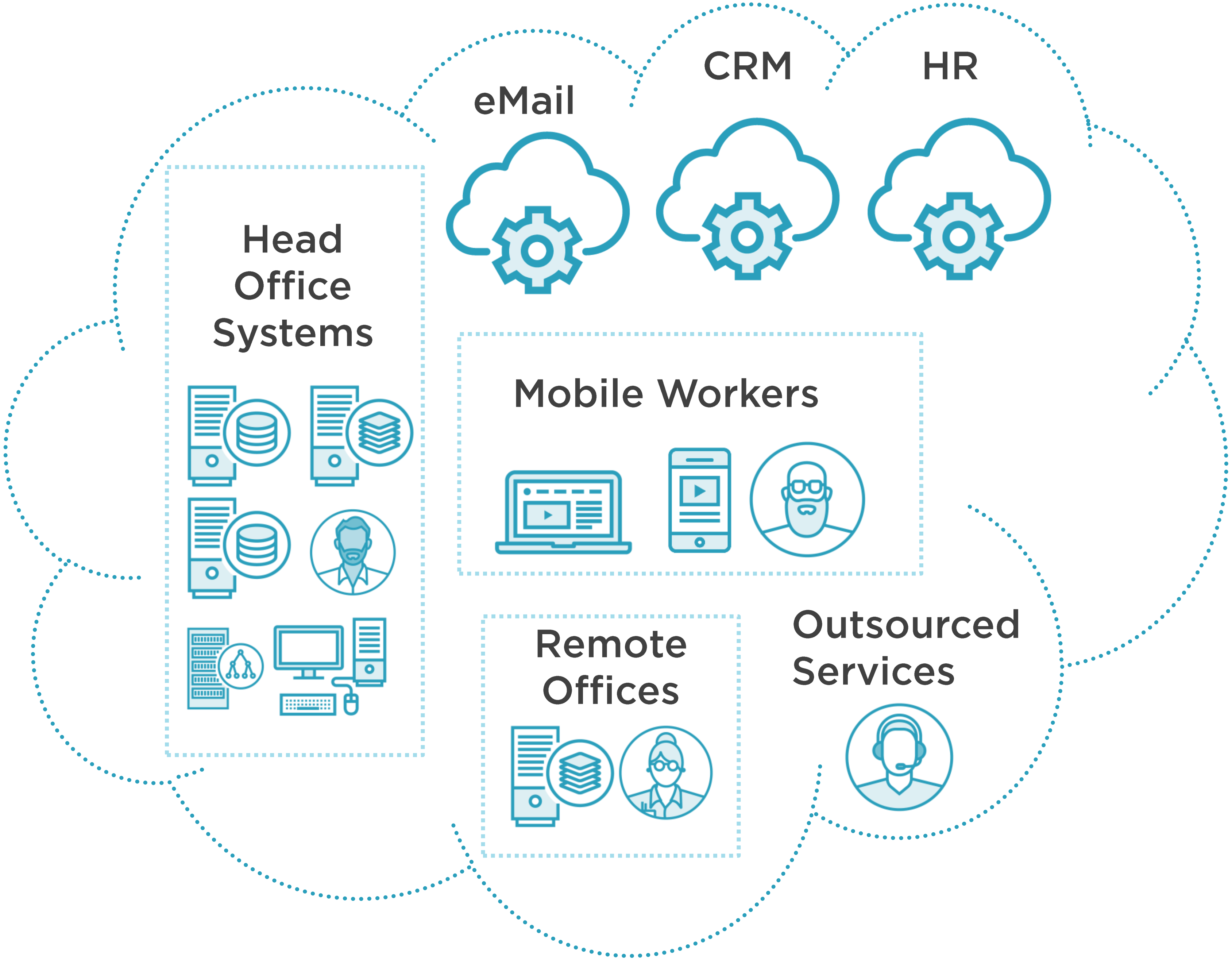
CRM

Head Office Systems

Remote Offices


eMail
CRM
HR
Head Office Systems
Remote Offices


eMail
CRM
HR
Head Office Systems
Mobile Workers
Remote Offices



eMail

CRM

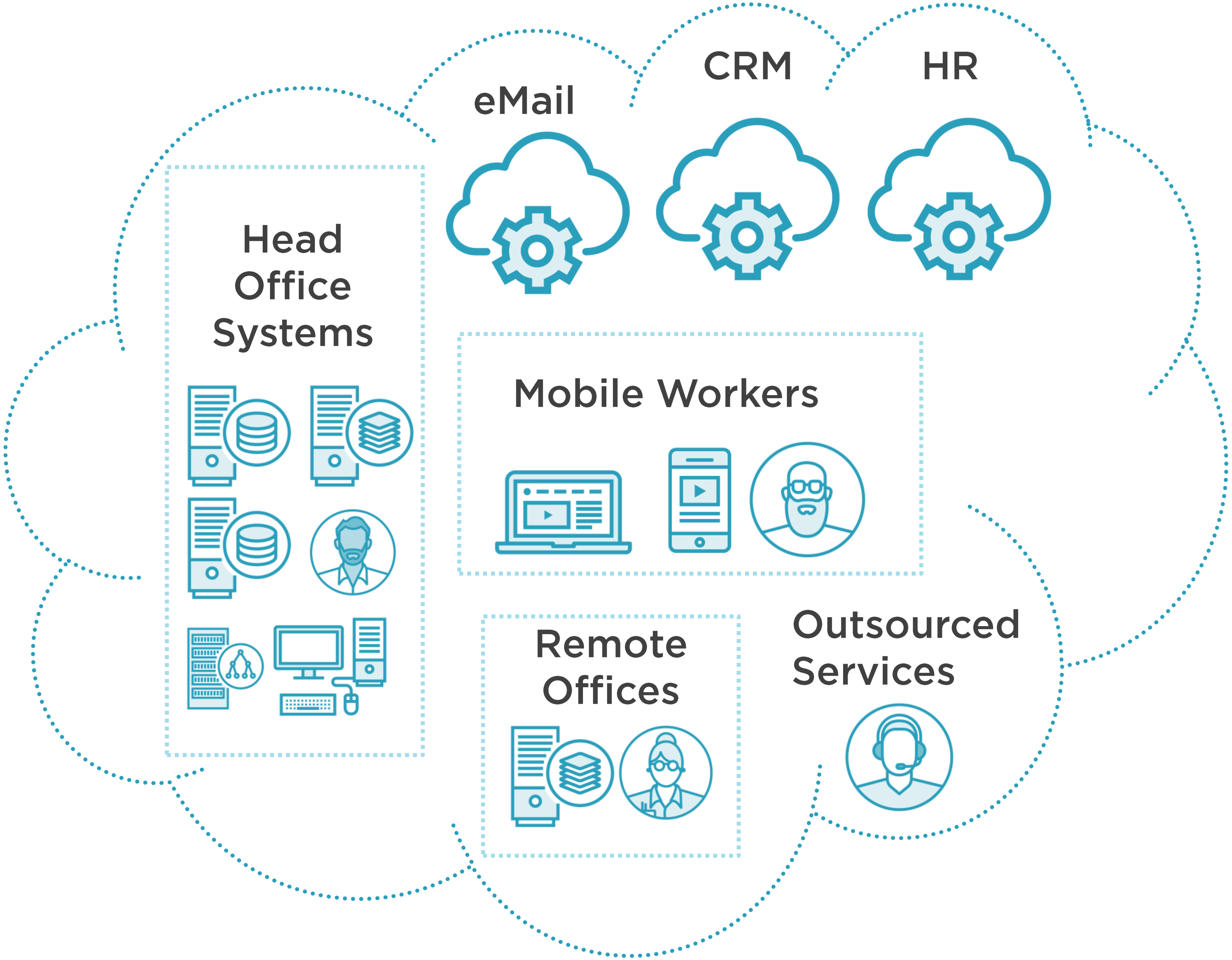
HR

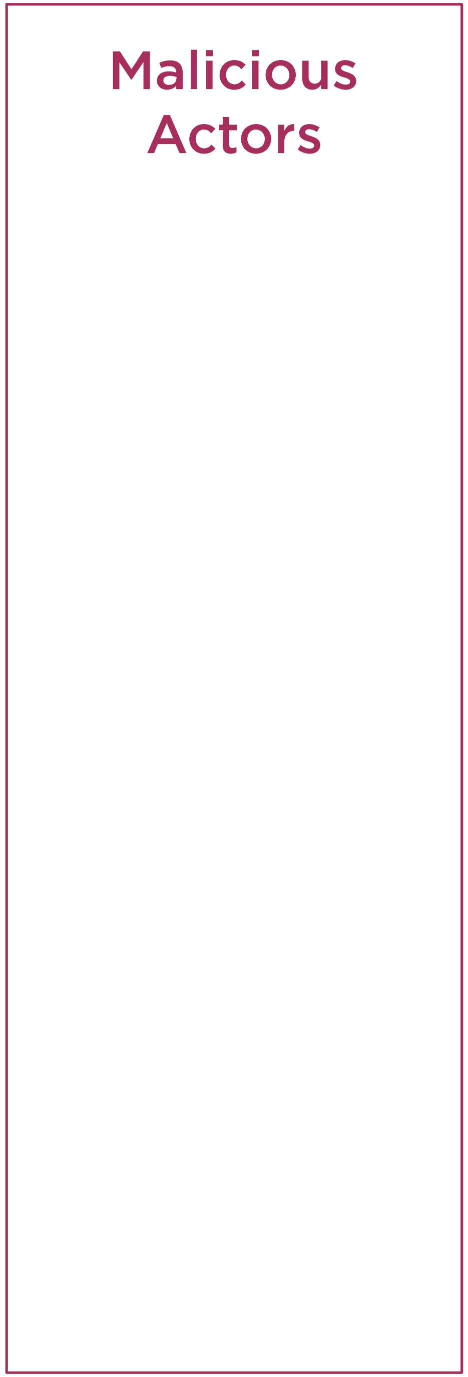
Head Office Systems

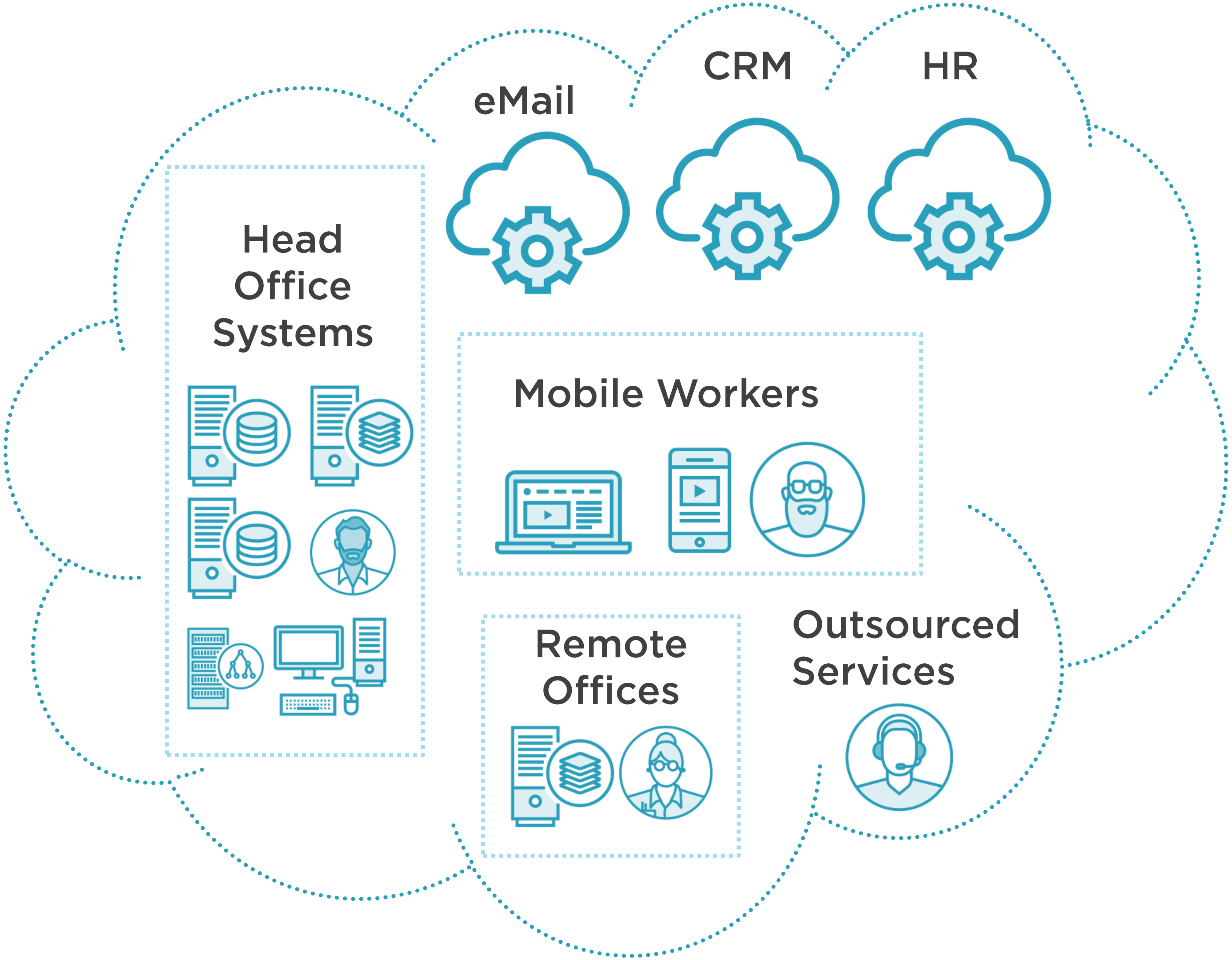
Mobile Workers

Remote Offices

Outsourced Services


eMail
CRM
HR
Head Office Systems
Mobile Workers
Remote Offices
Outsourced Services


Malicious Actors



eMail

CRM

HR

Head Office Systems

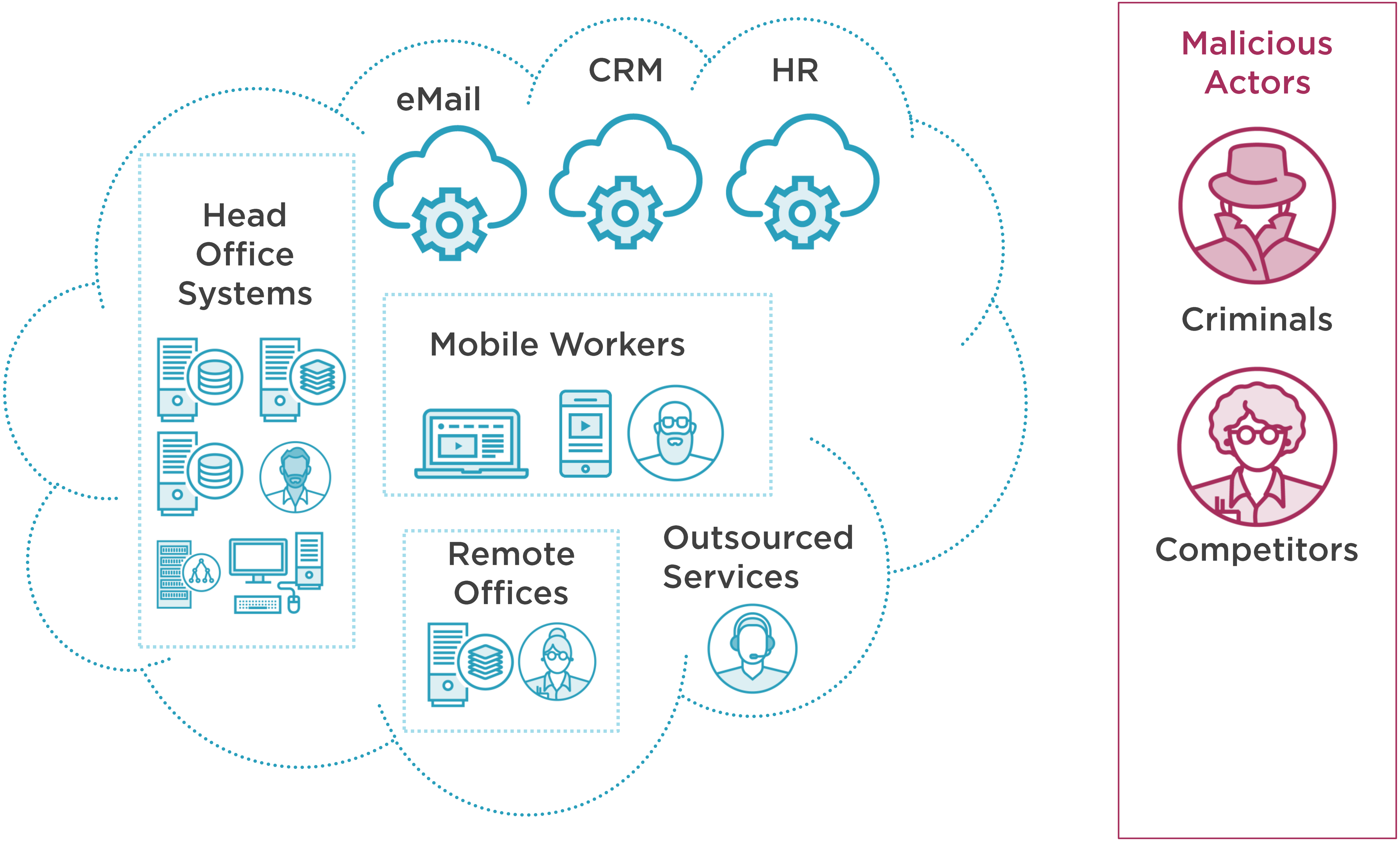
Mobile Workers

Remote Offices

Outsourced Services

Malicious Actors

Criminals



eMail

CRM

HR

Head Office Systems

Mobile Workers

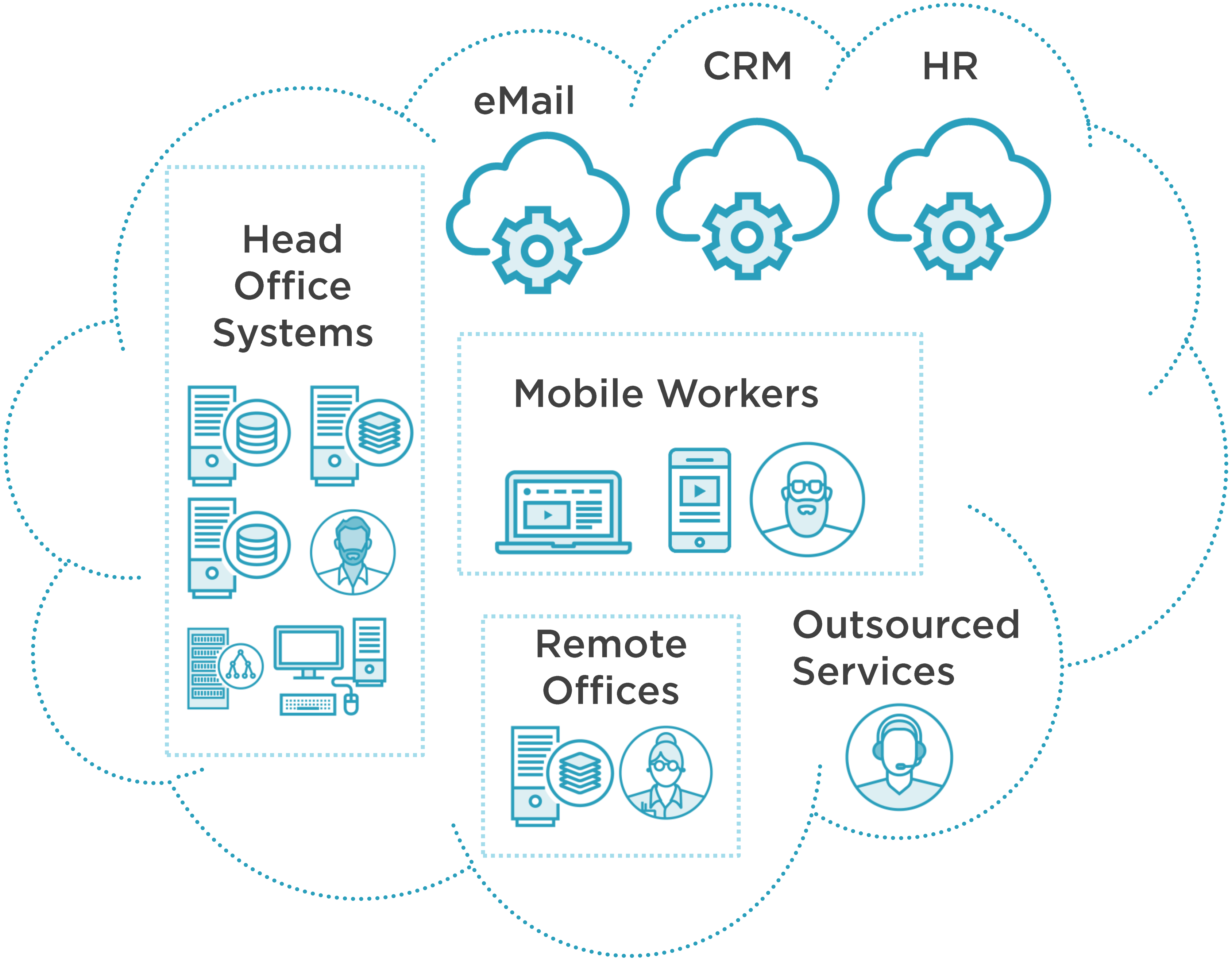
Remote Offices

Outsourced Services

Malicious Actors

Criminals

Competitors



eMail

CRM

HR

Head Office Systems

Mobile Workers

Remote Offices

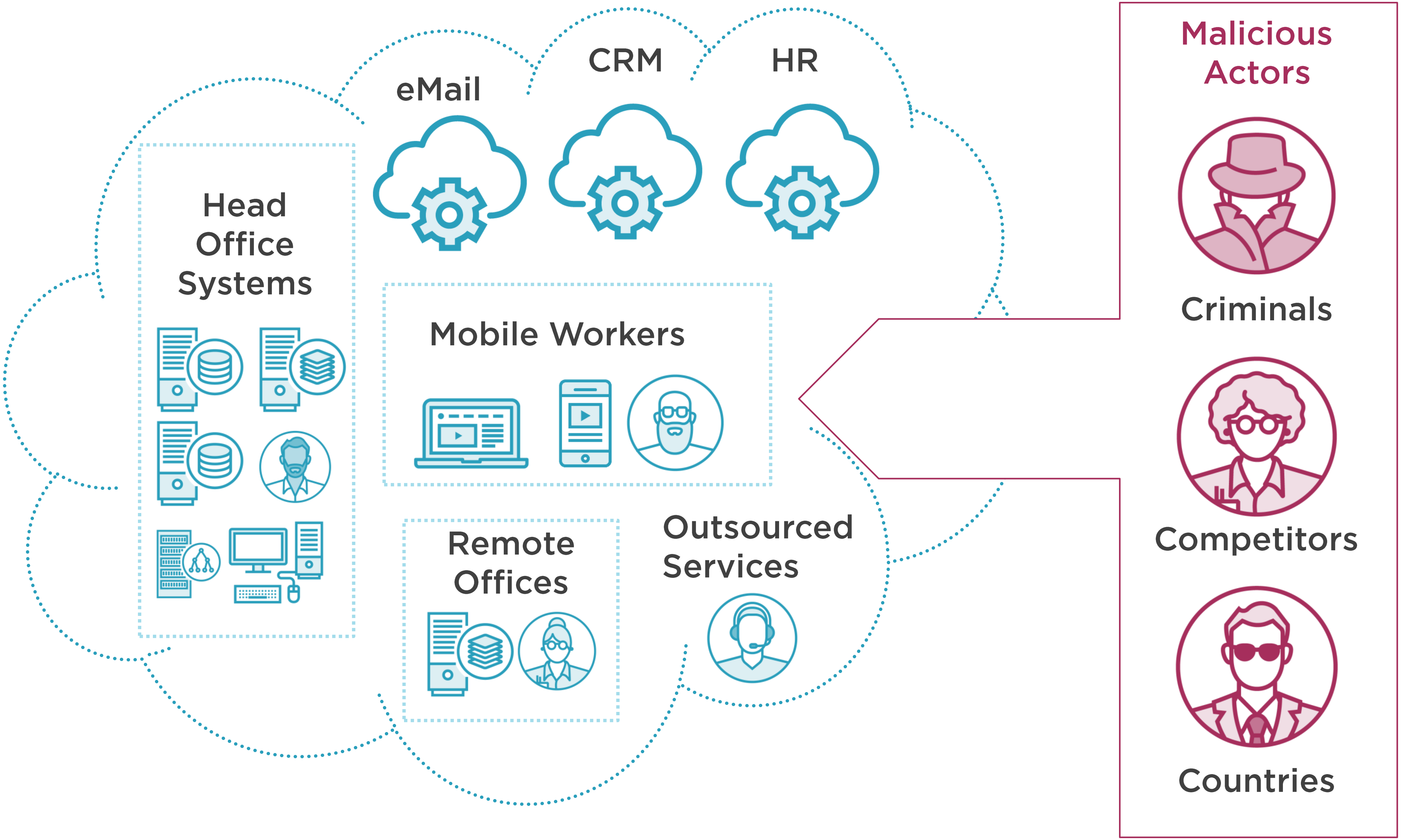
Outsourced Services

Malicious Actors

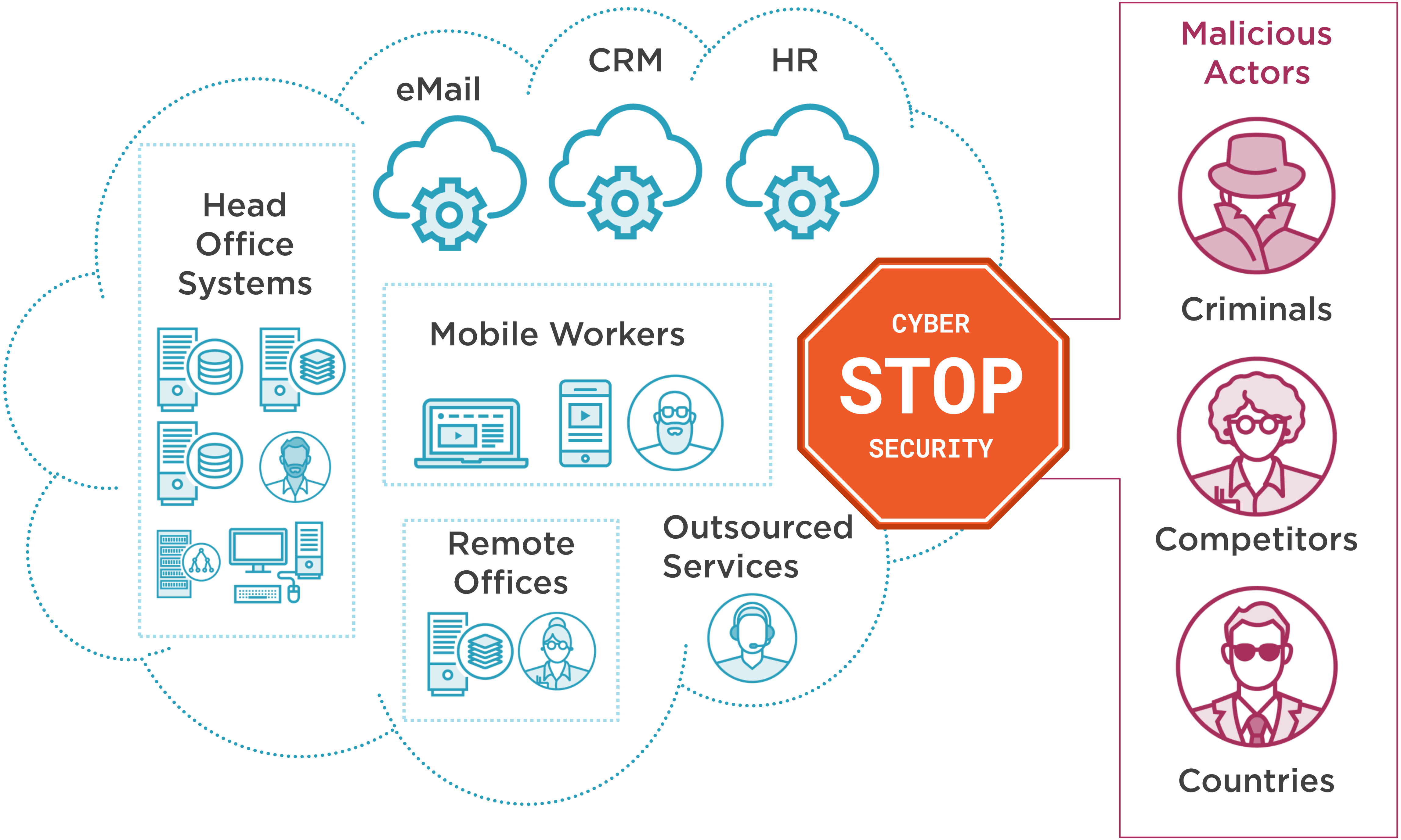
Criminals

Competitors

Countries



eMail
CRM
HR
Head Office Systems
Mobile Workers
Remote Offices
Outsourced Services
Malicious Actors
Criminals
Competitors
Countries


eMail
CRM
HR
Head Office Systems
Mobile Workers
Remote Offices
Outsourced Services
CYBER
STOP
SECURITY
Malicious Actors
Criminals
Competitors
Countries

Cyber Security: US NIST

The ability to protect or defend the use of an enterprise’s internet-connected systems and data from an attack.

Cyber Security: UK NCSC

The protection of internet connected systems, the data on them, and the services they provide, from unauthorized access, harm or misuse.

This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so

Gain access to confidential information

Make information unavailable

Tamper with information

Availability

Data is there
when it is needed

Integrity

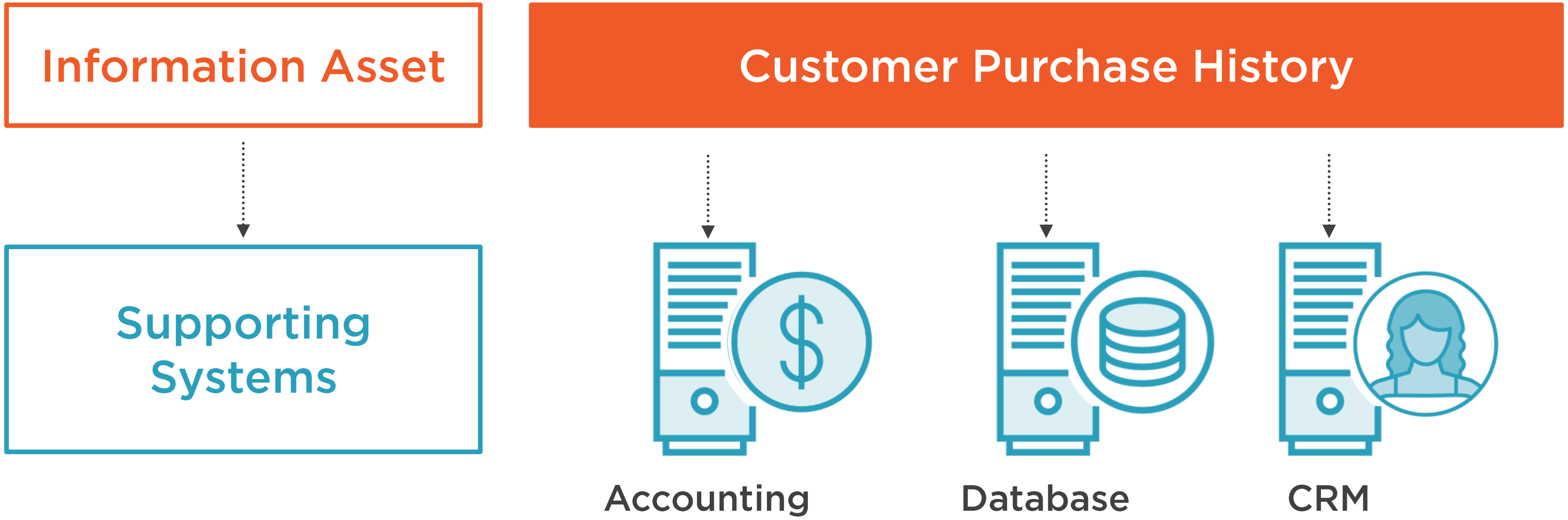
Data is accurate and hasn’t been tampered with

Confidentiality

Data is only accessed by authorized people

Information Asset: A set of data that has value to the organization

Information Assets and Systems



Information Asset

Supporting Systems

Customer Purchase History

Accounting

Database

CRM

Cyber Security

Protecting the confidentiality, integrity & availability

of an organization’s information assets

from malicious actors

(and accidents)

Impact: Operational, financial, regulatory or reputational

What do Criminals Want?

Cash: Payments / money transfer

What do Criminals Want?

Cash: Payments / money transfer

Things that can be turned into cash

What do Criminals Want?

Cash: Payments / money transfer

Things that can be turned into cash

Information someone else would find valuable

Criminals also extort money

Criminals also extort money – threaten to expose information

Criminals also extort money – threaten to corrupt data

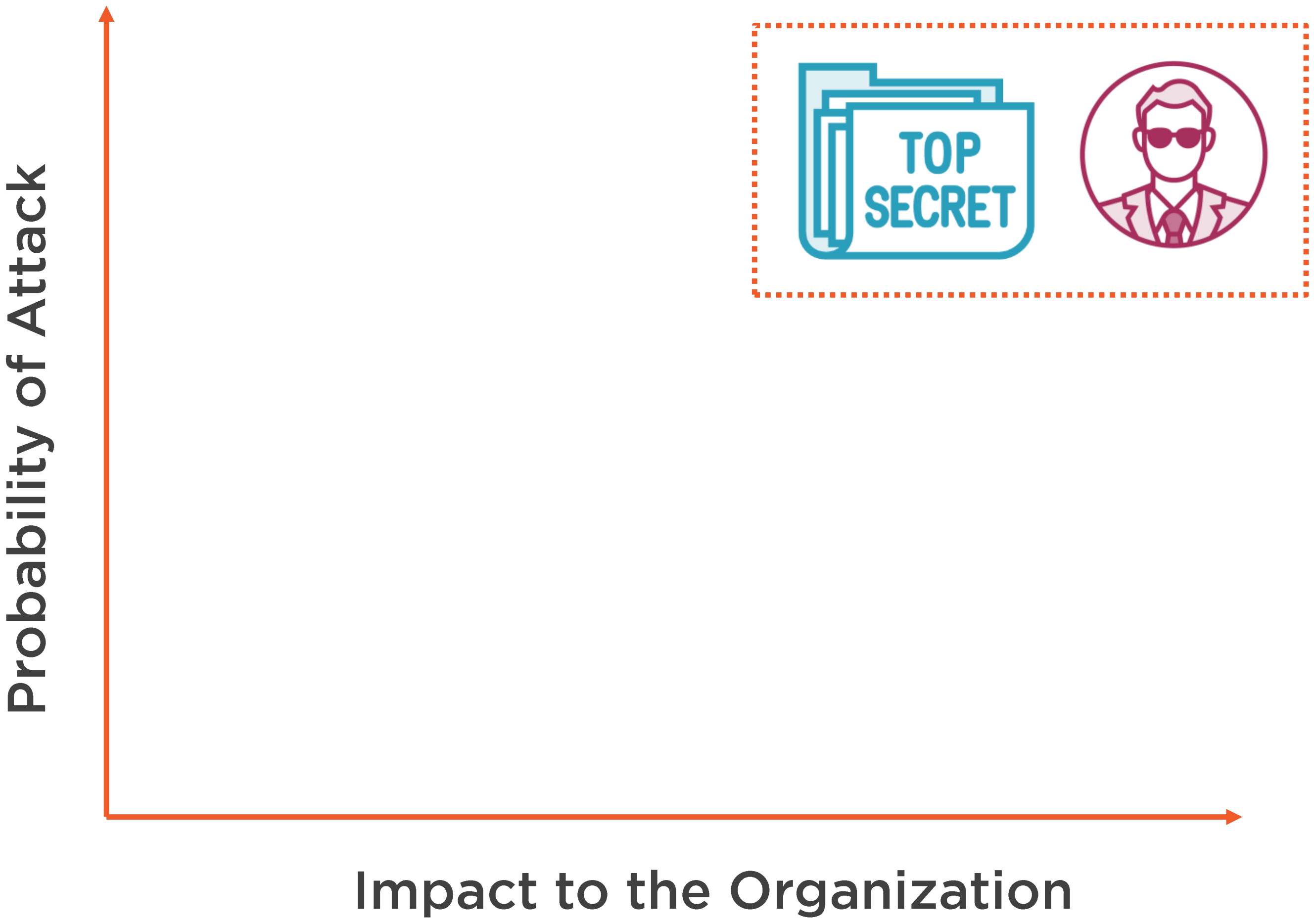
Criminals also extort money – threaten to make systems unavailable

Competitors and countries take data for their own use

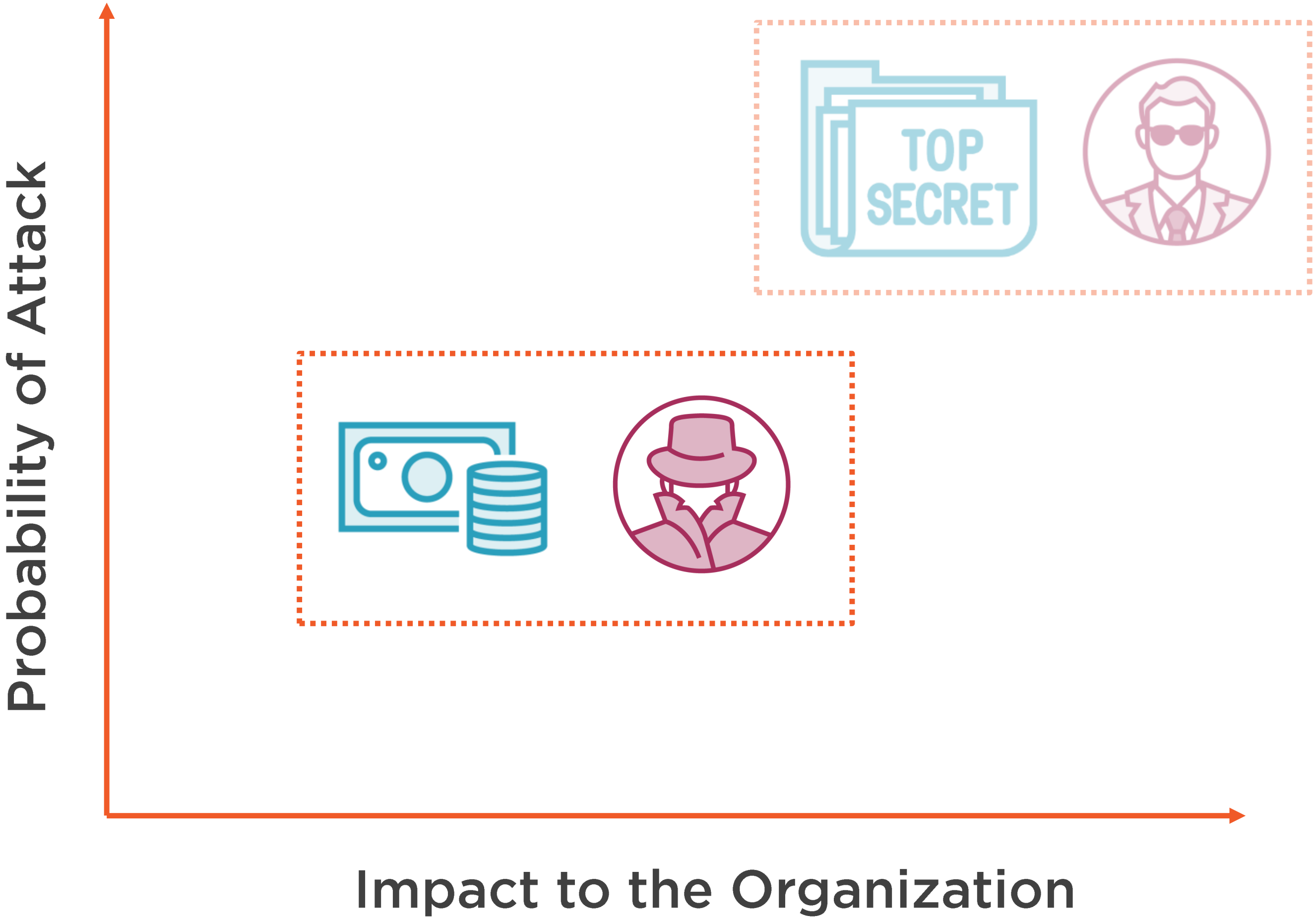
Cyber Risk Assessment

Cyber Risk Assessment

Cyber Risk Assessment

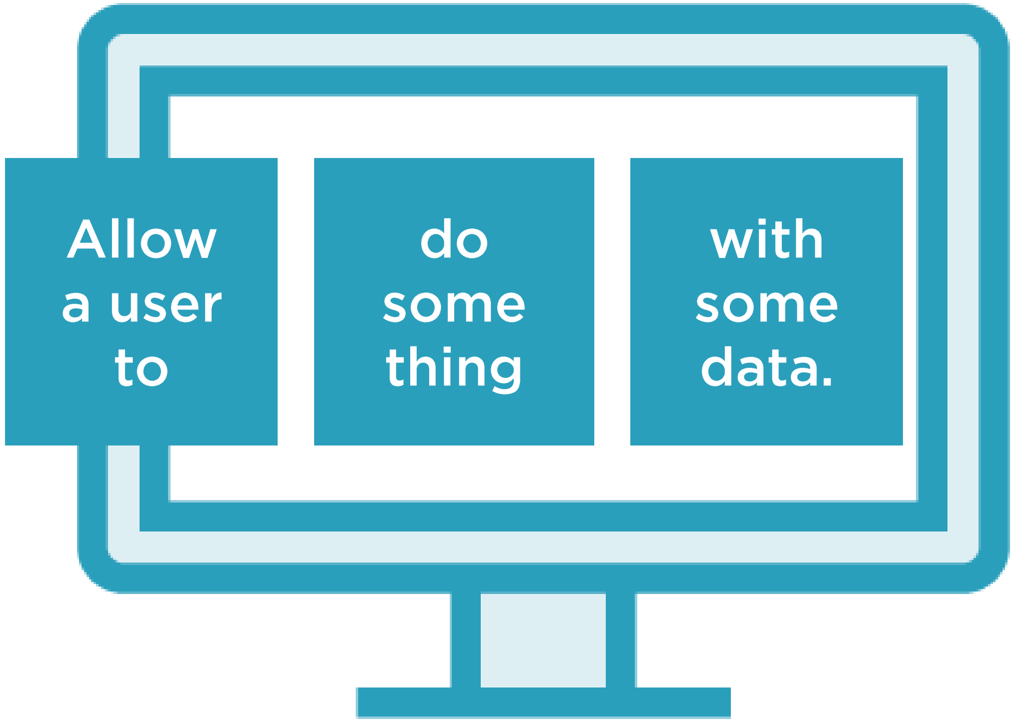


Cyber Risk Assessment



do some thing

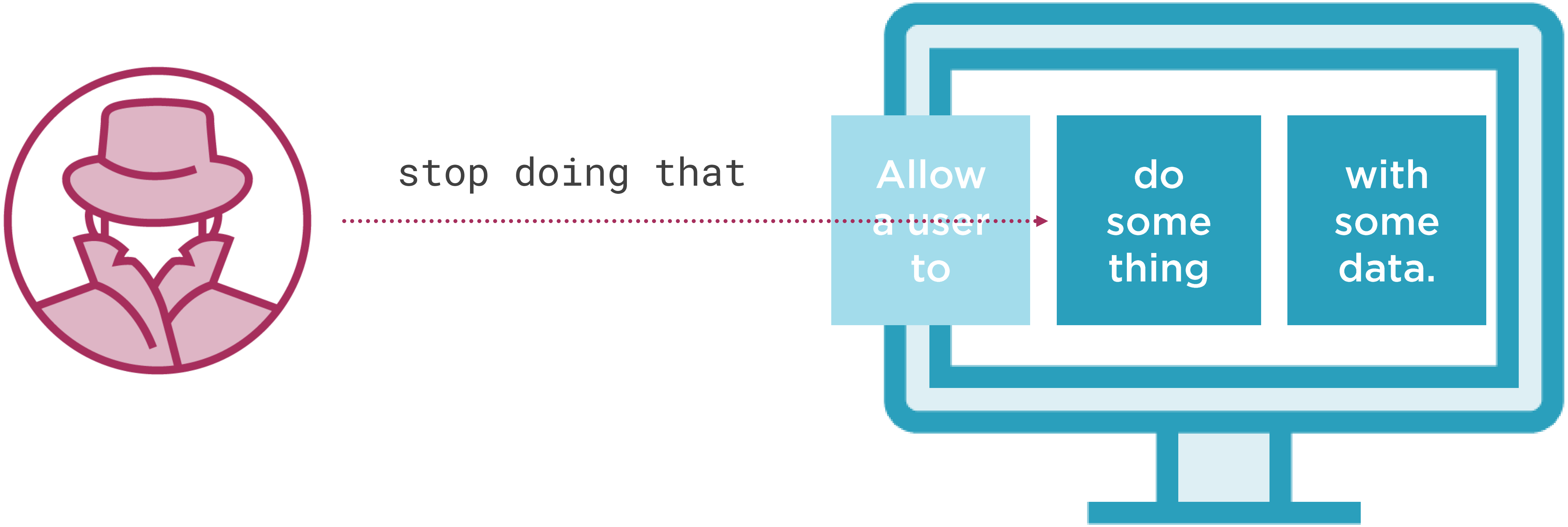
with some data.

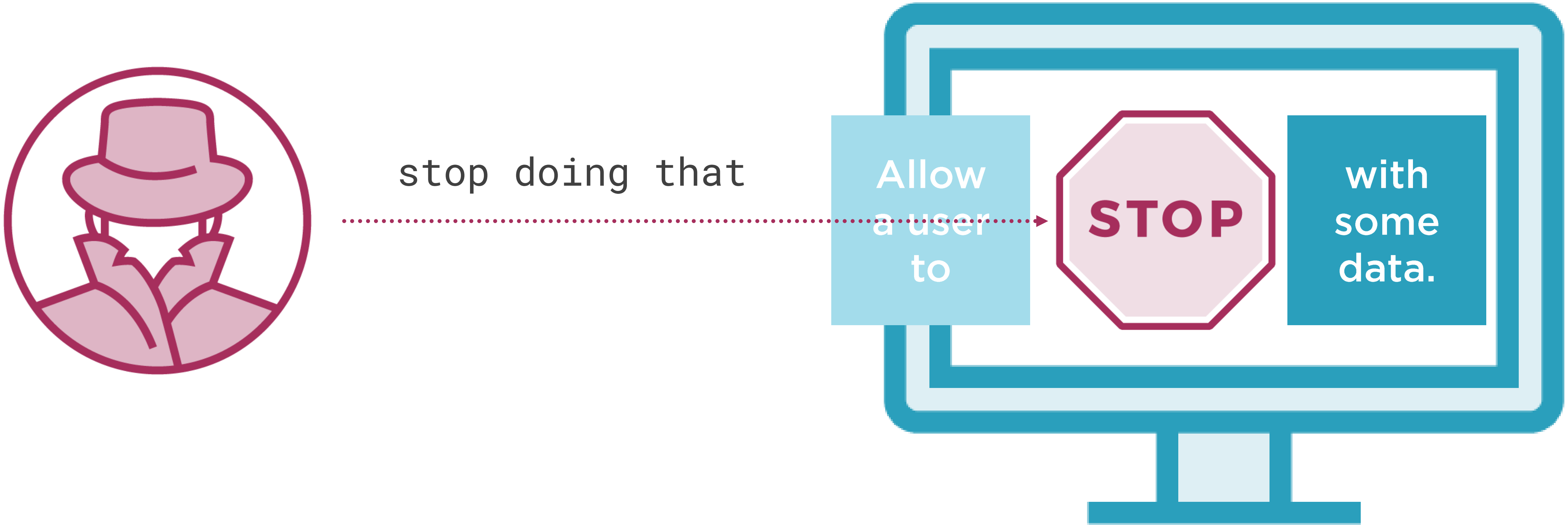


Allow a user to

do some thing

with some data.


stop doing that
Allow a user to
do some thing
with some data.

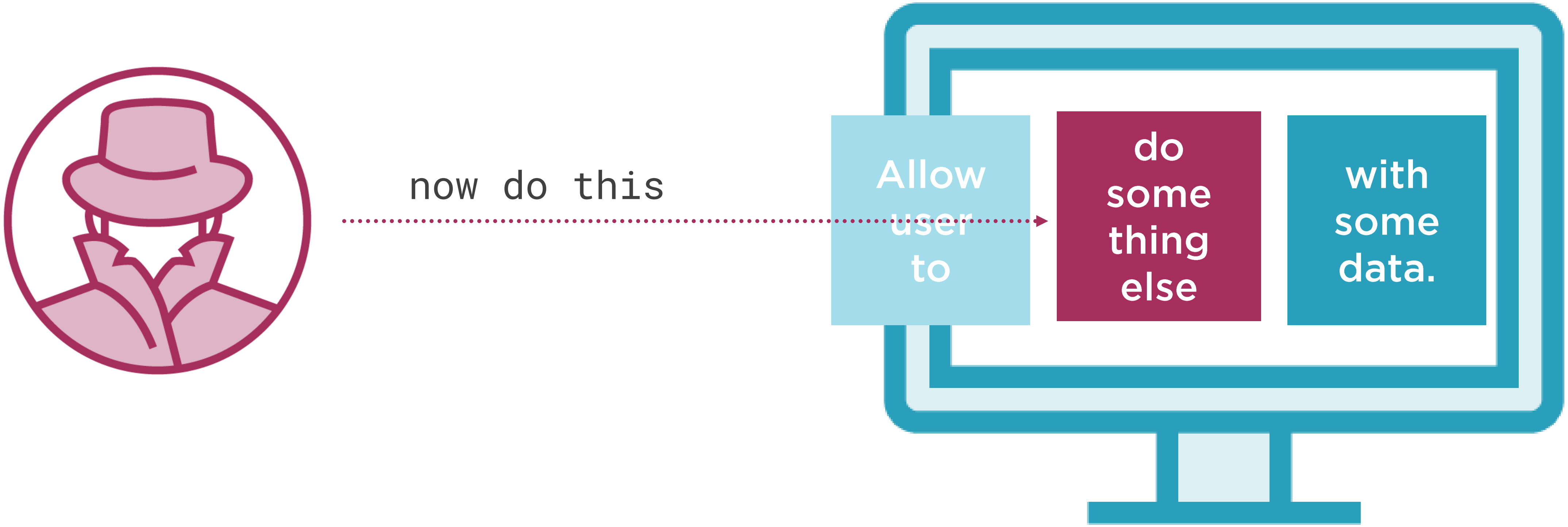


stop doing that

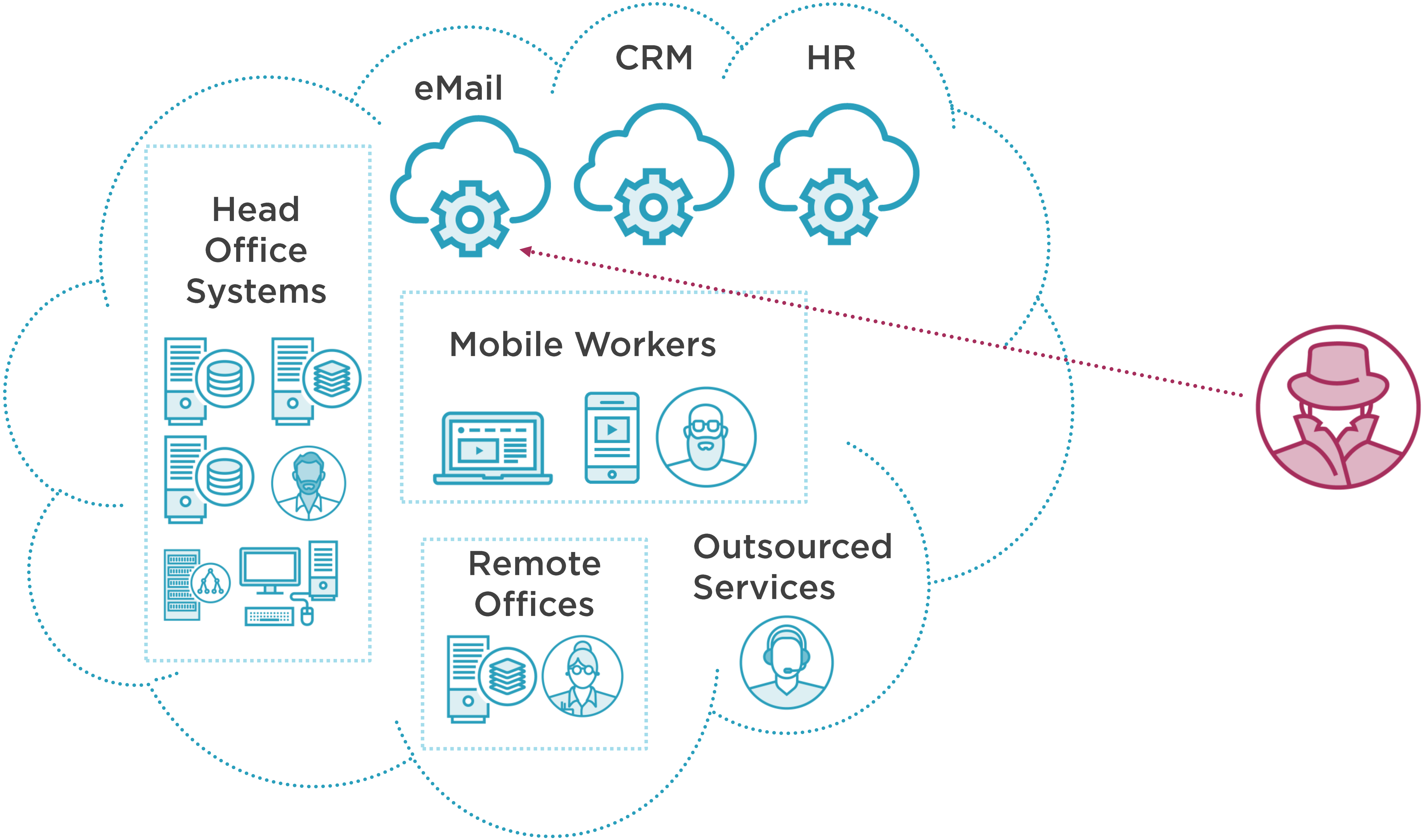
Allow a user to

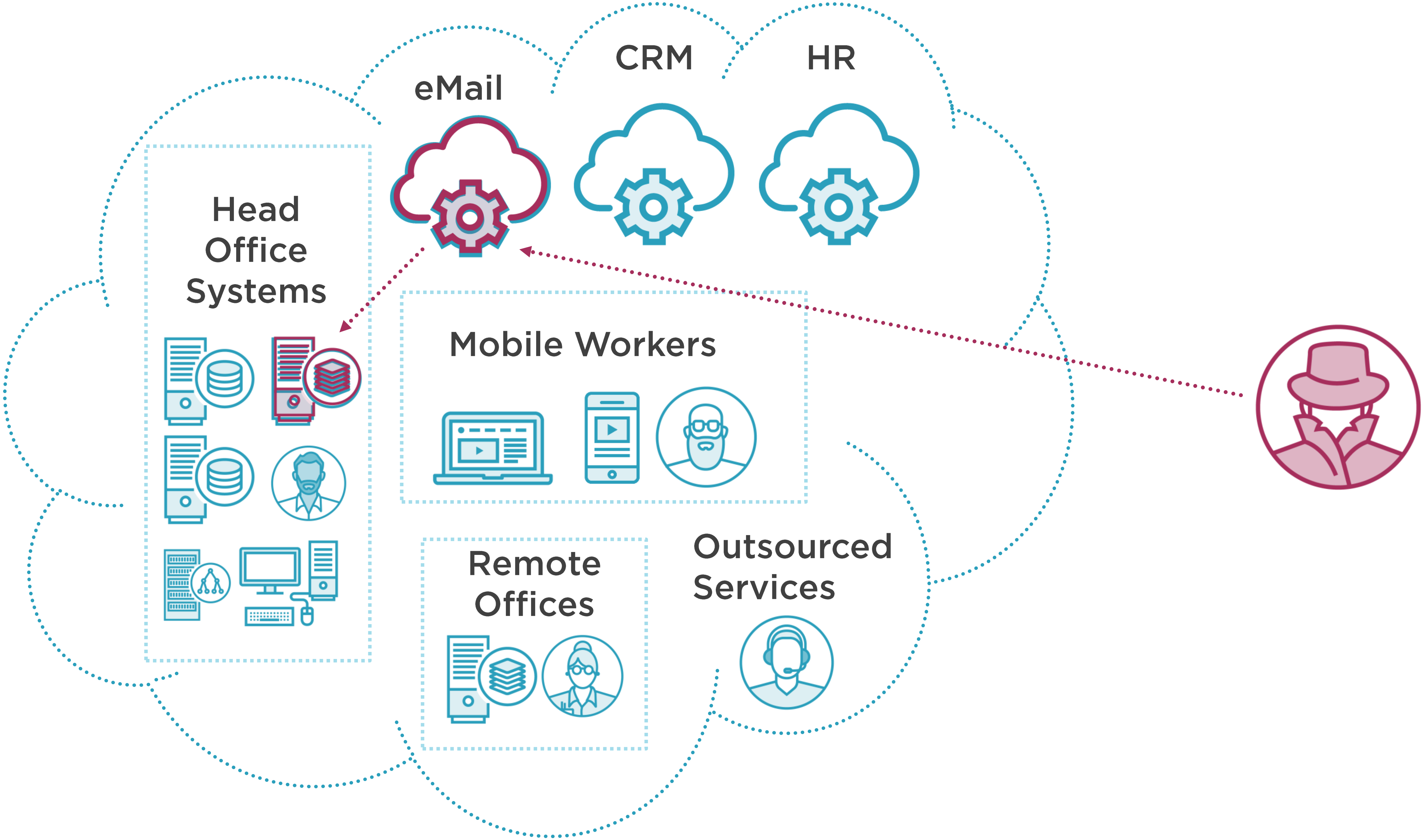
STOP

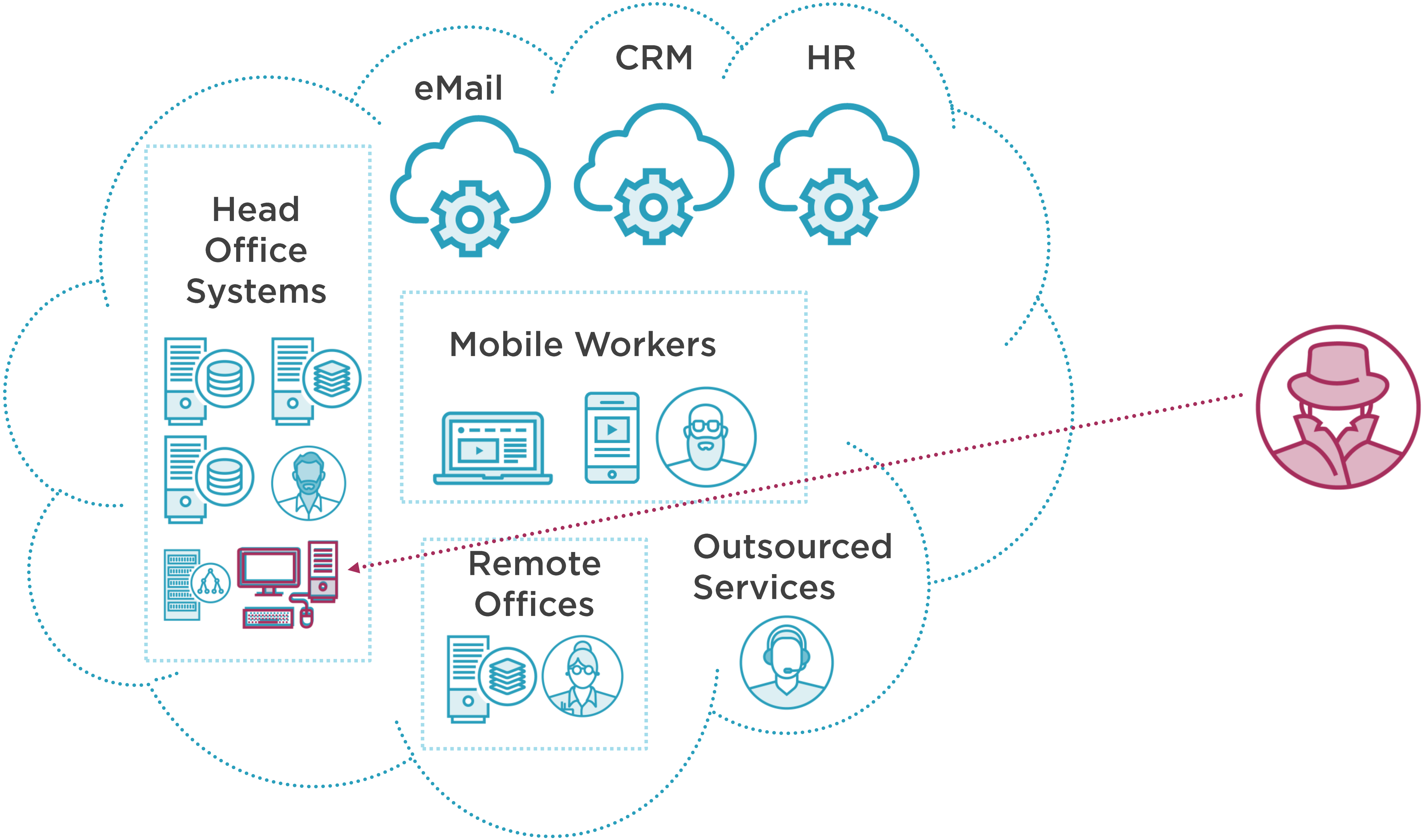
with some data.


now do this
Allow user to
do some thing else
with some data.

DoS: Denial of Service attack


eMail
CRM
HR
Head Office Systems
Mobile Workers
Remote Offices
Outsourced Services


eMail
CRM
HR
Head Office Systems
Mobile Workers
Remote Offices
Outsourced Services


eMail
CRM
HR
Head Office Systems
Mobile Workers
Remote Offices
Outsourced Services

Phishing: Tricking users into divulging their credentials to an attacker