Forcepoint

Data Security Everywhere

Empowering people to work anywhere, with data everywhere

Altan Yarar

Sr. Named Account Manager

Türkiye & Azerbaycan & Kazakhstan & Özbekistan

Ours is a world of rapid transformation

Ours is a world of rapid transformation

You'll never have less data than you have today

348TB Amount of data managed by the average enterprise

That data is used in more remote locations

75% Of workers will be full- or part-time remote

And exposed between more remote applications

70% Of workloads are executed in the cloud

Open to attacks from a huge enemy

86% Of businesses admit to being compromised

New technologies are making data easier to breach than ever

Help Net Security
December 5, 2023

2024 brings changes in data security strategies

2024 will be a revolutionary year for the data security landscape as Data Security Posture Management (DSPM) technology rapidly evolves to keep pace with the colossal amount of data being and across business sectors, a

NEWS 2 NOV 2023

Forrester: GenAI Will Lead to Breaches and Fines in 2024

Phil Muncaster
UK / EMEA News Reporter, Infosecurity Magazine
Email Phil   Follo

Rampant ger
breaches and
leading analy

Forrester mac
and trust.

Senior analys
assistants tha
vulnerabilities

Looking to 2024: Data, AI and security will be top priorities for businesses

By Nathan Vega | Published 6 days ago

No Comments

FORTUNE

Home   News   Tech   Finance   Leadership   Well   Recommends   Fortune 500

CONFERENCES · BRAINSTORM TECH

As A.I. spreads through the office, companies are rethinking how they deal with data

BY STEPHEN PASTIS
July 14, 2023 at 5:54 PM CDT

FORTUNE BRAINSTORM TECH

Why data, AI, and regulations top the threat list for 2024

The new year finds us confronted by a landscape characterized by political uncertainty, social fragmentation, escalating geopolitical tensions, and a turbulent macro-economic backdrop, making it crucial for security leaders to strategically prepare for the forthcoming challenges.

FORBES > INNOVATION

Ensuring Data Privacy: 20 Best Practices For Businesses In The AI Age

Expert Panel® Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

Nov 28, 2023, 01:15pm EST

Security doesn't need to be complex

---> Embrace zero trust

---> Manage policies in one place

---> Push enforcement to the edge

---> Make data uniform and fast everywhere — even from BYOD

Forcepoint's mission is to enable Data Security Everywhere

so that people can safely work anywhere with data everywhere

Increase Productivity

Have people work anywhere with data everywhere—seamlessly, faster, easier—even from BYOD

Cut Costs

Replace fragmented infrastructure with more efficient, easier cloud service that cuts helpdesk calls too

Immediate Economic Impact

Reduce Risk

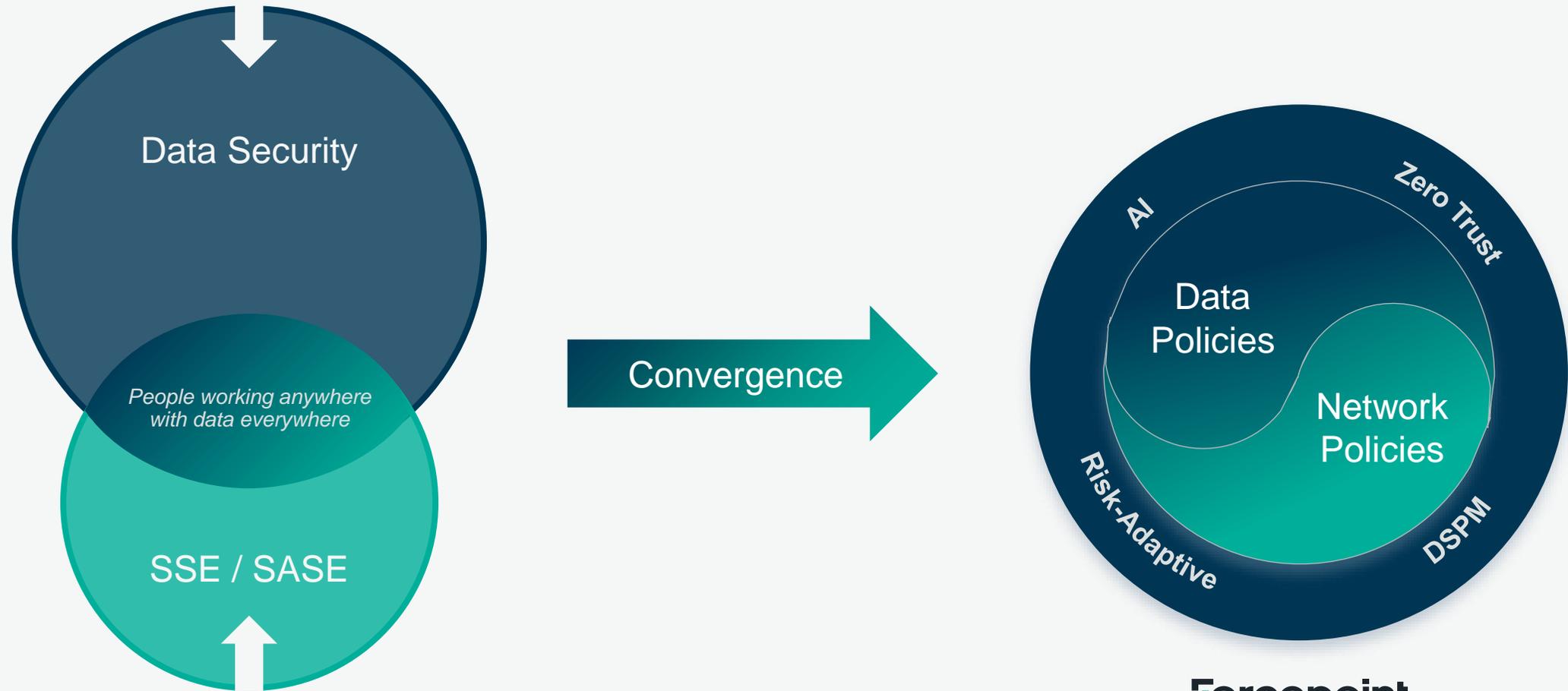Use Zero Trust and enterprise-class security to continuously protect sensitive data wherever it is used

Streamline Compliance

Have consistent visibility & control everywhere
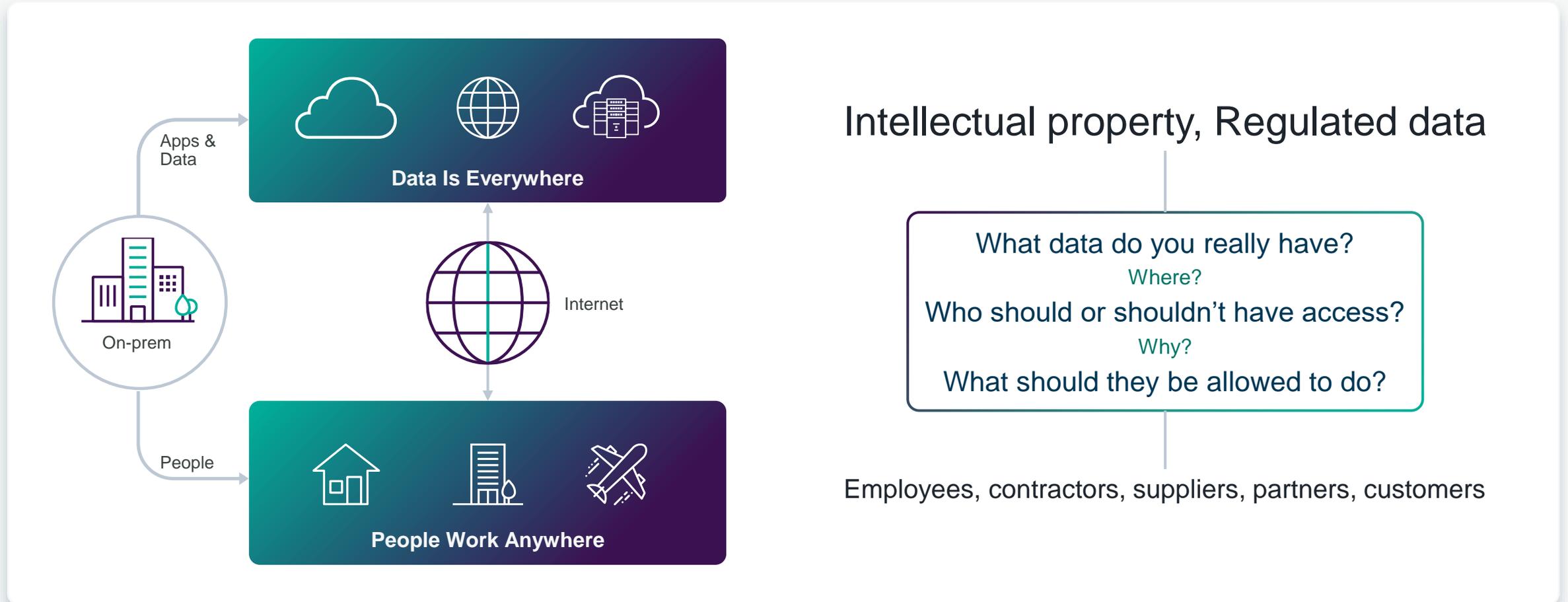
Cybersecurity *is* data security now

We bring data security & network security together for better visibility & control

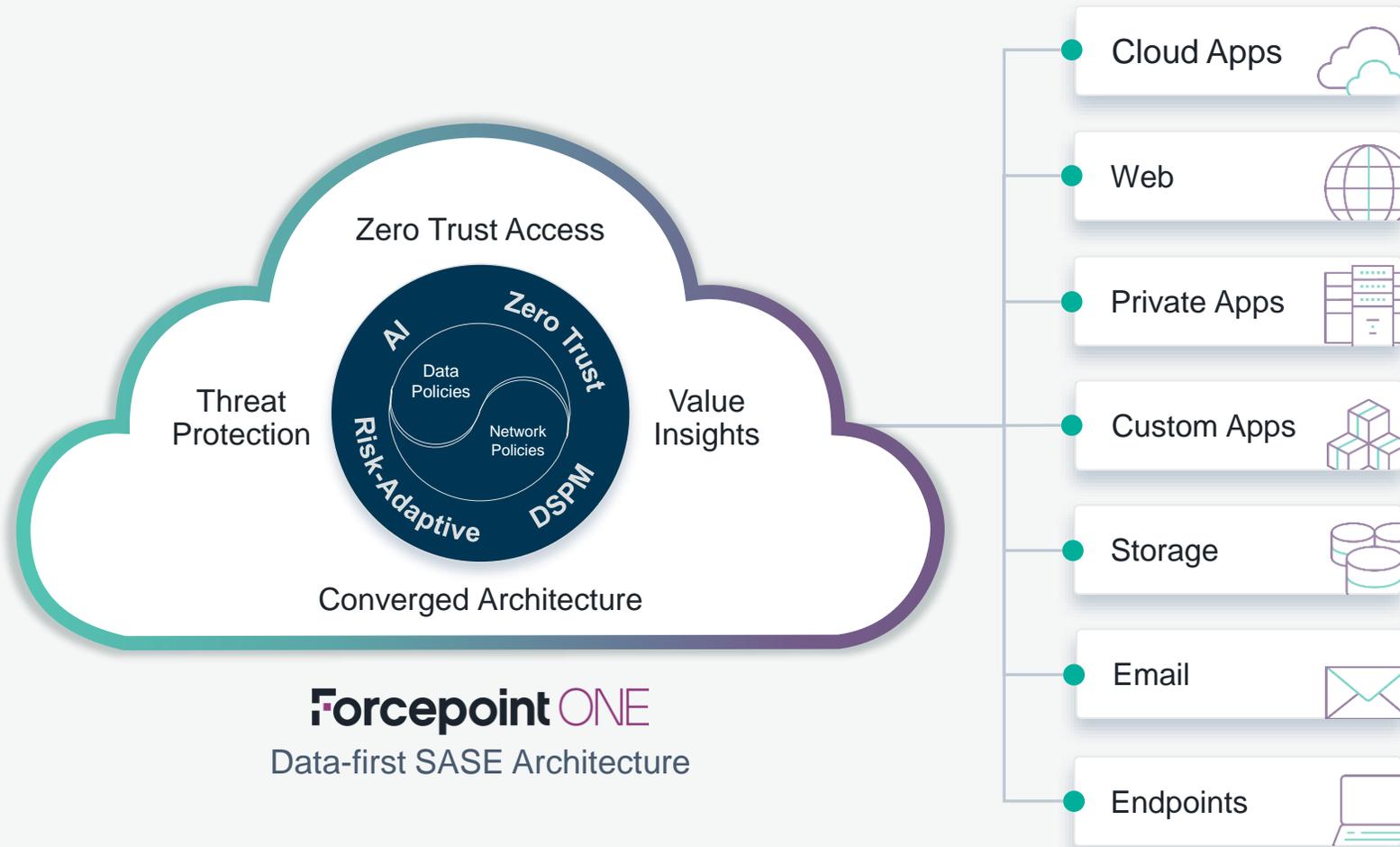# Data is now the key to competitiveness and business transformation

Apps & Data

On-prem

Data Is Everywhere

Internet

People

People Work Anywhere

Intellectual property, Regulated data

What data do you really have?
Where?
Who should or shouldn't have access?
Why?
What should they be allowed to do?

Employees, contractors, suppliers, partners, customers

Today, people work anywhere with data everywhere

Delivered from a modern architecture, powered by AI and Zero Trust

Zero Trust Access

AI · Zero Trust

Data Policies

Network Policies

Risk-Adaptive · DSPM

Threat Protection

Value Insights

Converged Architecture

Forcepoint ONE

Data-first SASE Architecture

- Cloud Apps
- Web
- Private Apps
- Custom Apps
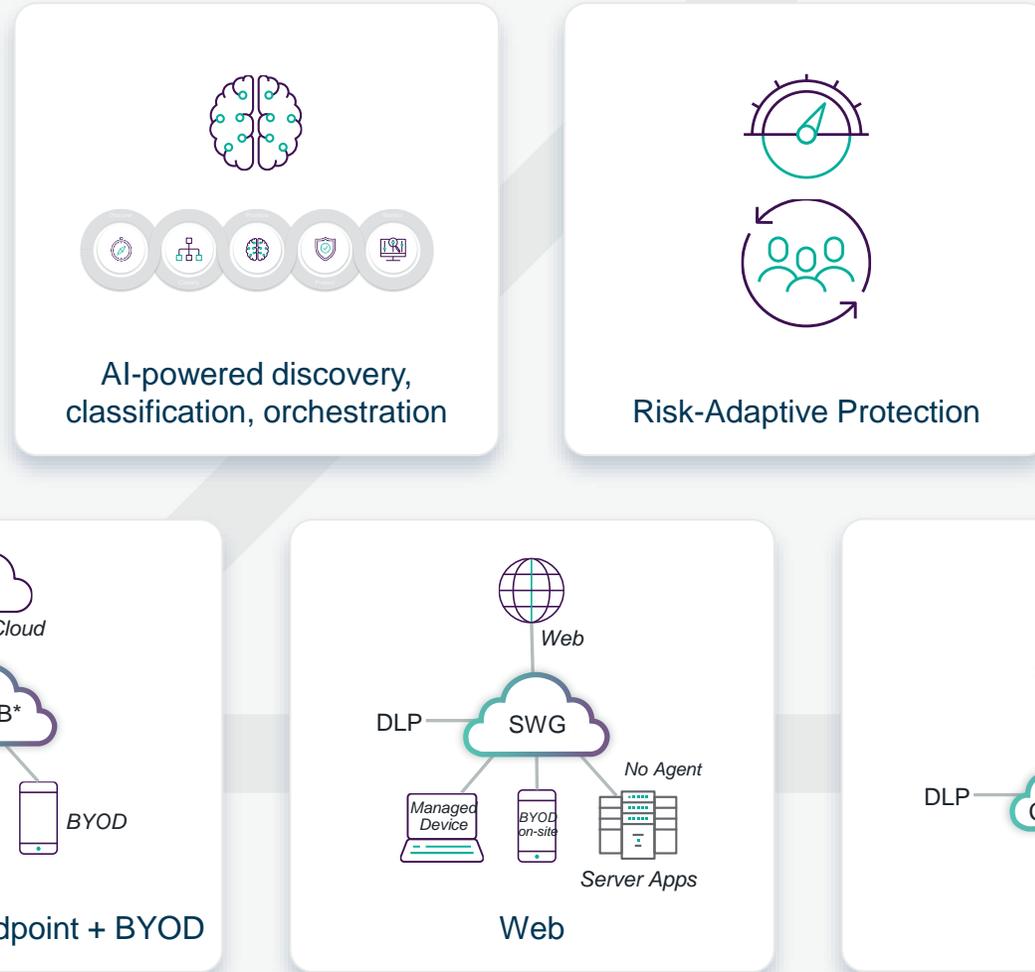- Storage
- Email
- Endpoints

Forcepoint

Data Security Everywhere

Empowering people to work anywhere, with data everywhere

Security doesn't have to be difficult
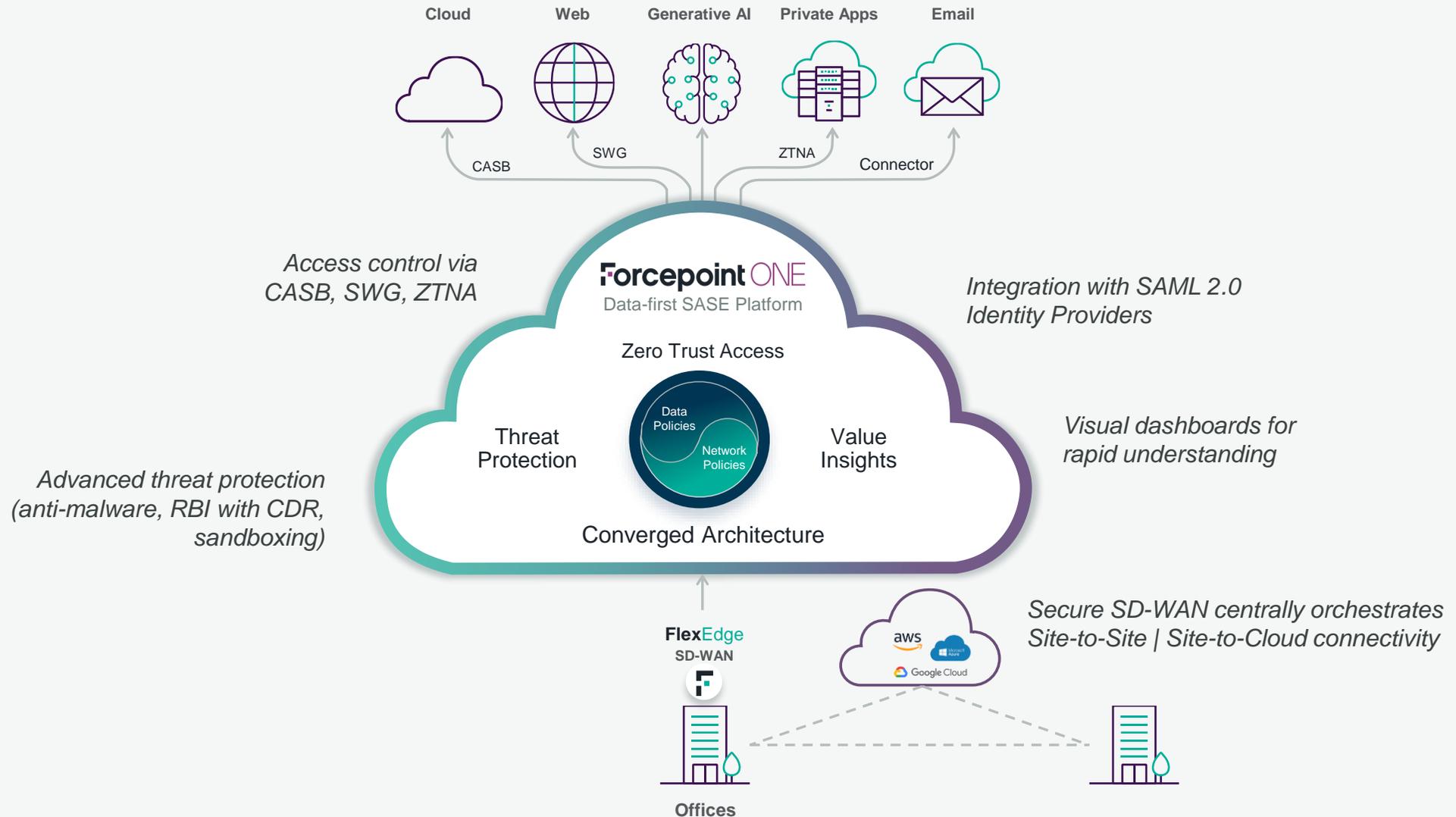
5 Steps to Data Security Everywhere

Forcepoint

Security. Simplified.

AI-powered discovery, classification, orchestration

Risk-Adaptive Protection

Cloud Apps + Endpoint + BYOD

Web

Email

*Add ZTNA to replace VPNs for accessing private 'cloud' apps

Data-first SASE architecture simplifies other security and networking, too

Extensible, efficient, reliable

# Simplify data security across cloud apps and endpoint devices

One set of policies, one console

Real enterprise-class DLP (1700+ built-in templates) wherever needed

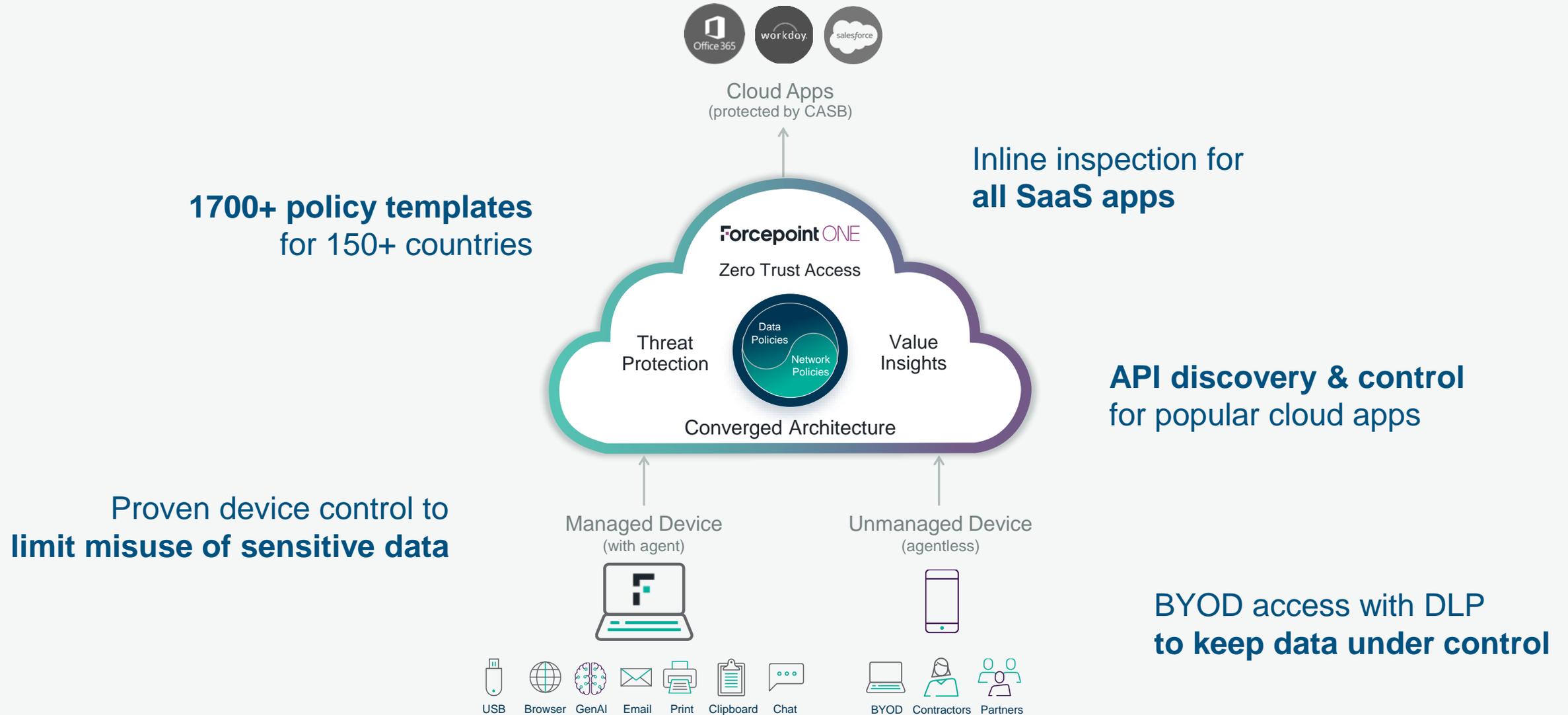Remove the largest hurdles to cloud adoption—esp. with BYOD

Extend modern cloud-first data security to the endpoint, or traditional endpoint DLP to the cloud

Eliminate need for multiple systems, manual syncing
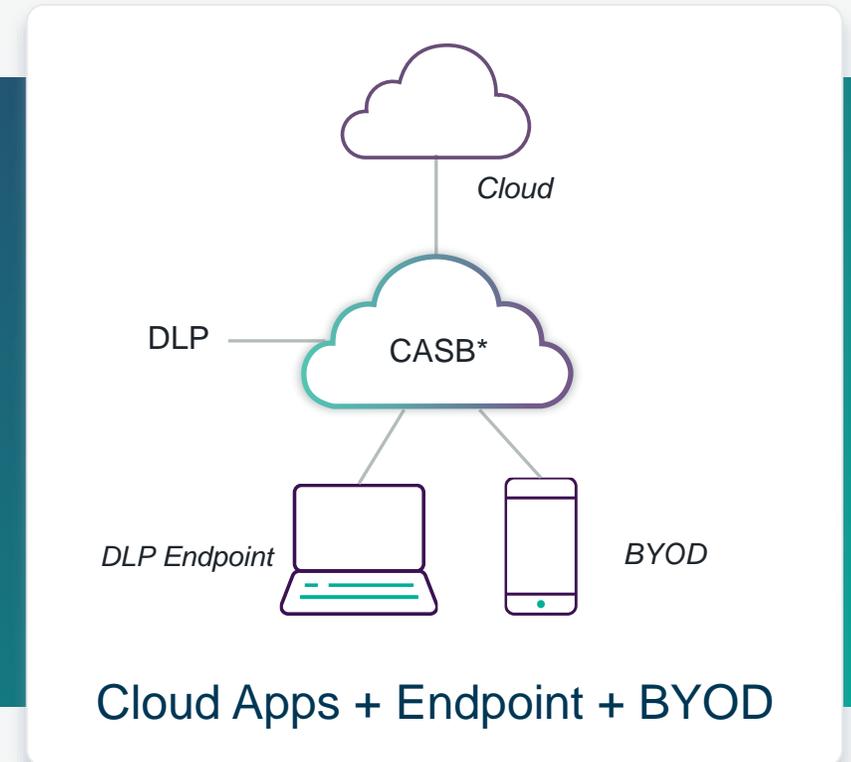
Cloud

DLP —— CASB*

DLP Endpoint

BYOD

Cloud Apps + Endpoint + BYOD

*Add ZTNA to replace VPNs for accessing private 'cloud' apps

Forcepoint

Deliver consistent data security for Unmanaged & Managed devices
from cloud to endpoint

Cloud Apps
(protected by CASB)

Forcepoint ONE

Zero Trust Access

Data Policies

Network Policies

Threat Protection

Value Insights

Converged Architecture

1700+ policy templates for 150+ countries

Inline inspection for **all SaaS apps**

API discovery & control for popular cloud apps

Proven device control to **limit misuse of sensitive data**

Managed Device
(with agent)

Unmanaged Device
(agentless)

BYOD access with DLP **to keep data under control**

USB   Browser   GenAI   Email   Print   Clipboard   Chat

BYOD   Contractors   Partners

Control access with a full, industry-leading CASB

Data-first SASE architecture

Identity-based access control using SAML 2.0

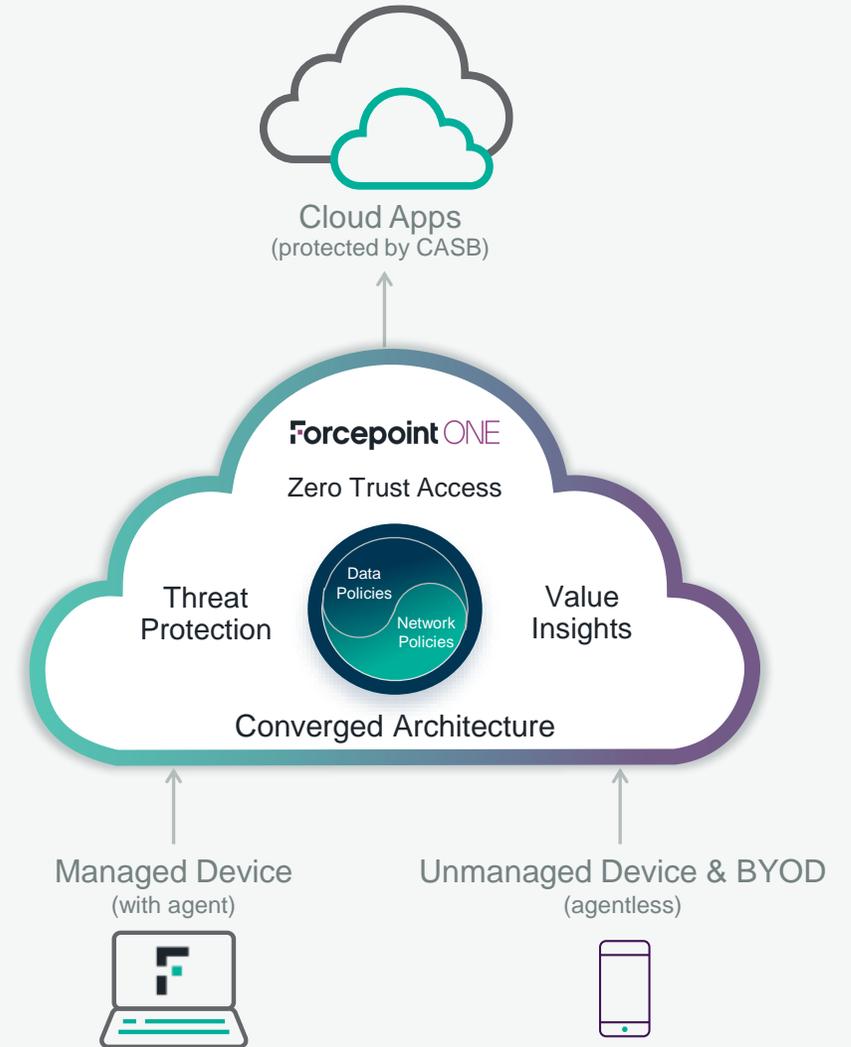800,000+ known apps with risk assessments

Extensible controls via easy scripting

Malware scanning for data-in-motion & data-at-rest

BYOD, Linux, Chromebook access via reverse proxy

API control over sharing and permissions
- Protect Microsoft O365, AWS, Salesforce and more

Cloud Apps
(protected by CASB)

Forcepoint ONE

Zero Trust Access

Threat Protection

Data Policies

Network Policies

Value Insights

Converged Architecture

Managed Device
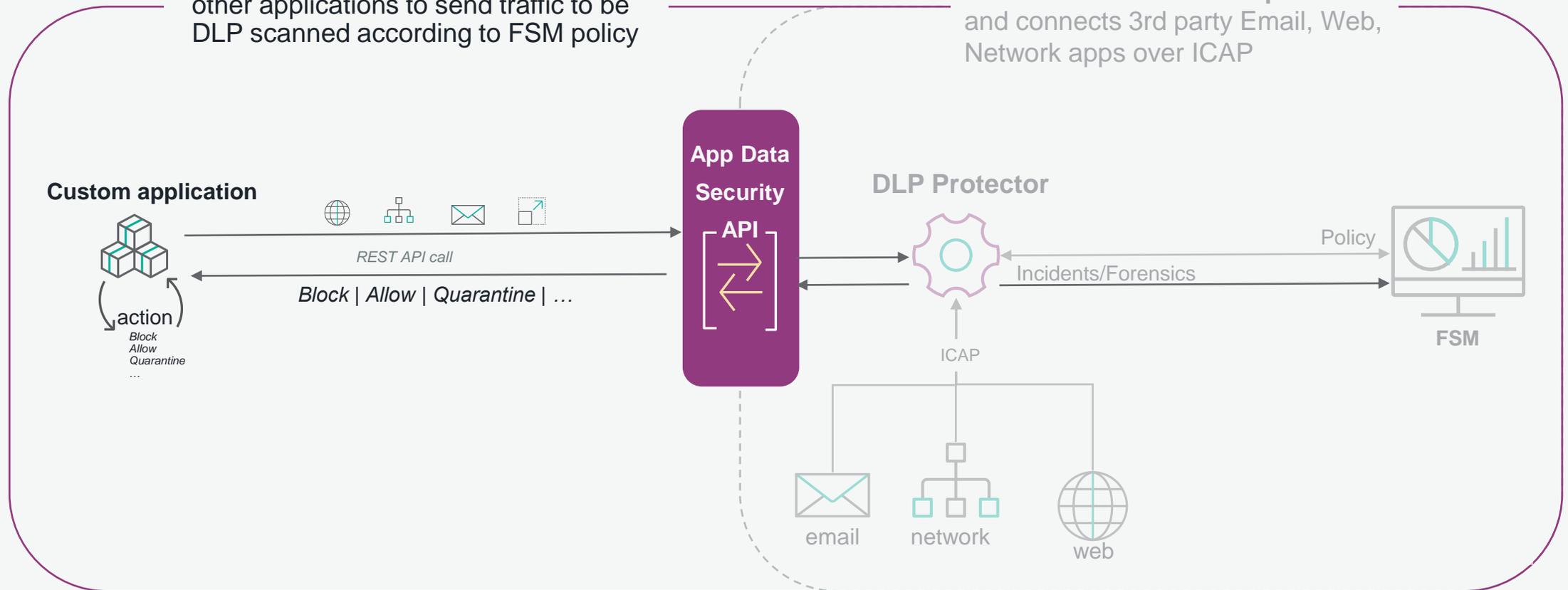(with agent)

Unmanaged Device & BYOD
(agentless)

DLP v10.1

New Product: App Data Security API

The **App Data Security API** enables other applications to send traffic to be DLP scanned according to FSM policy
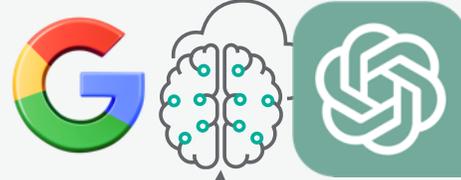
The **Protector** is a component of **DLP Network.** It runs **on-premise** and connects 3rd party Email, Web, Network apps over ICAP

Custom application

REST API call

Block | Allow | Quarantine | …

action

Block
Allow
Quarantine
…

App Data Security

API

DLP Protector

Policy

Incidents/Forensics

FSM

ICAP

email

network

web

REST API is a more modern, performant, secure interface than ICAP
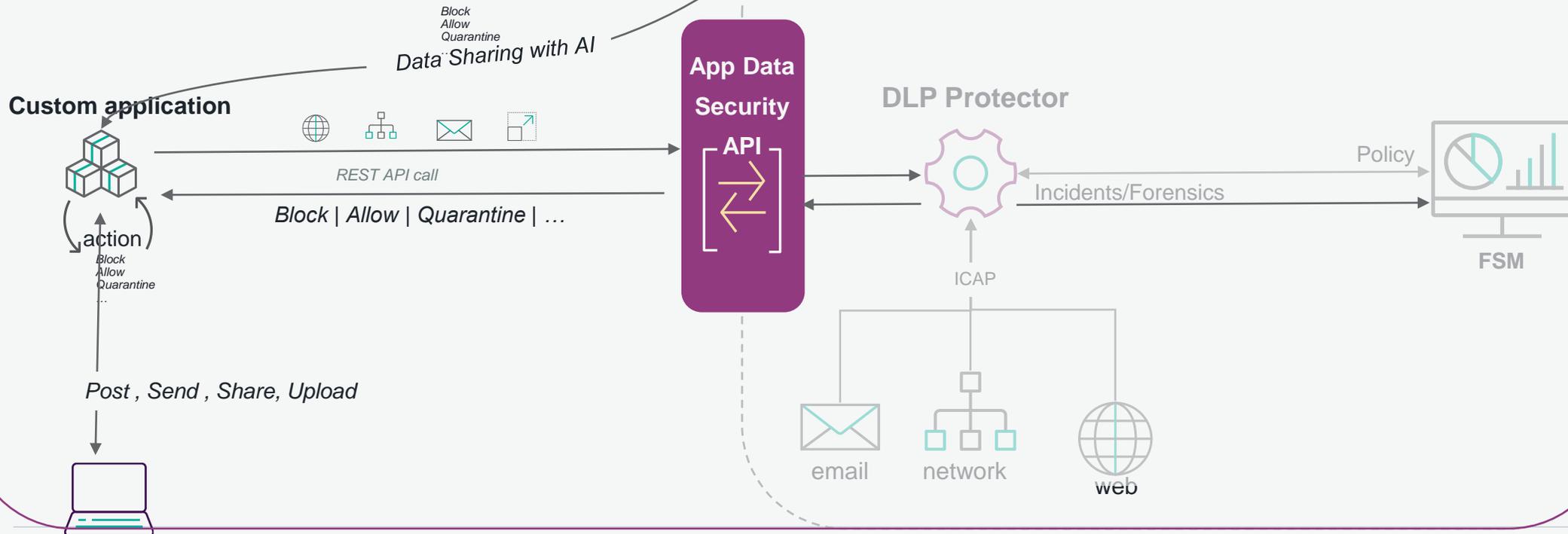
Forcepoint

© 2024 Forcepoint 16

Use Case 1

Mobile or desktop app supported by Gen AI tools

The **App Data Security API** enables other applications to send traffic to be DLP scanned according to FSM policy

The **Protector** is a component of **DLP Network.** It runs **on-premise** and connects 3rd party Email, Web, Network apps over ICAP

Block
Allow
Quarantine
...

Data Sharing with AI

App Data Security
API

DLP Protector

Custom application

REST API call

Block | Allow | Quarantine | …

Policy

Incidents/Forensics

FSM

action

Block
Allow
Quarantine
...

ICAP

Post , Send , Share, Upload
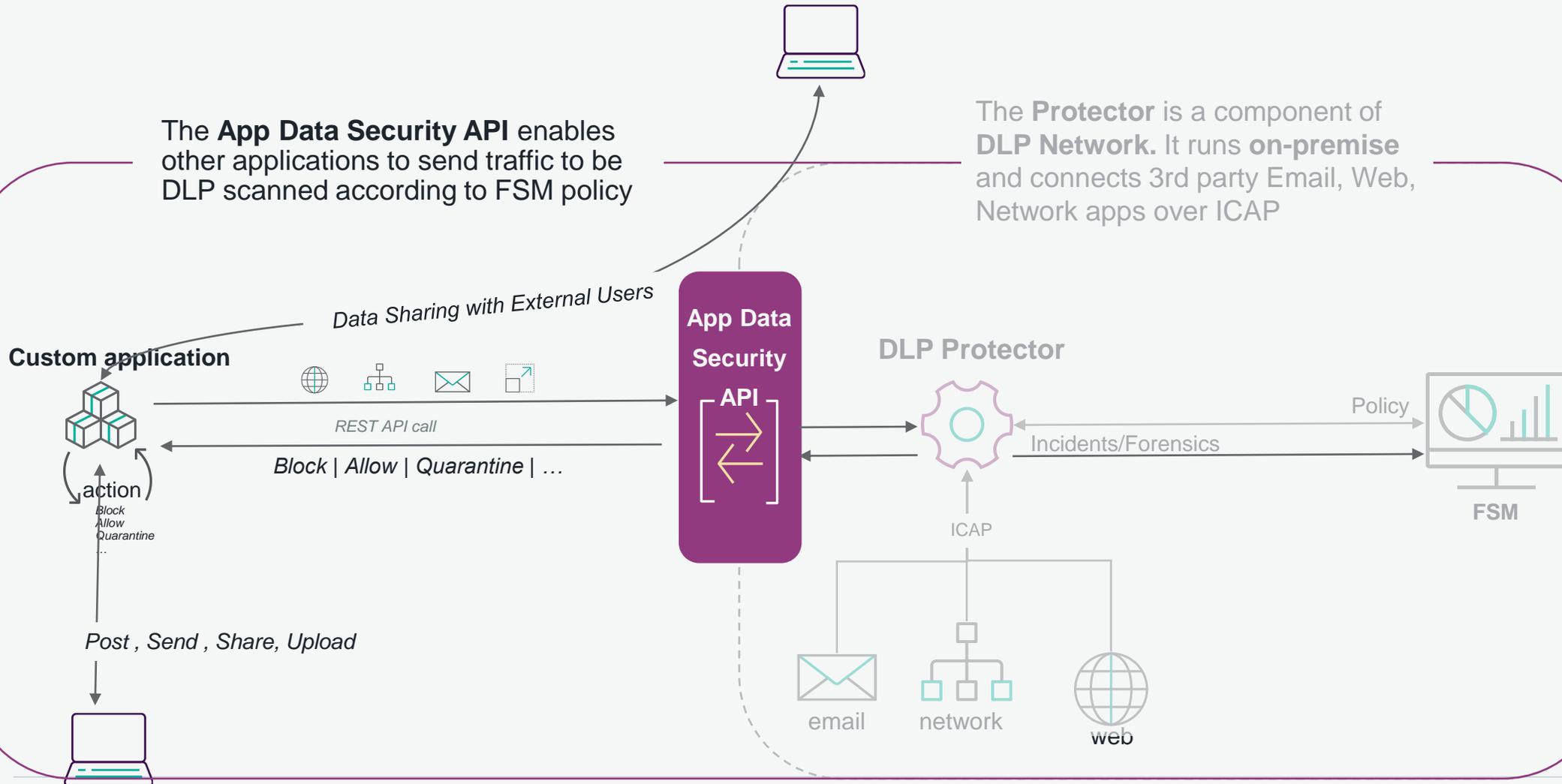
email   network   web

Use Case 2

File Transfer Application

The **App Data Security API** enables other applications to send traffic to be DLP scanned according to FSM policy

The **Protector** is a component of **DLP Network.** It runs **on-premise** and connects 3rd party Email, Web, Network apps over ICAP

Custom application

Data Sharing with External Users

REST API call

Block | Allow | Quarantine | …

action

Block
Allow
Quarantine
…

Post , Send , Share, Upload

App Data Security

API

DLP Protector

Policy

Incidents/Forensics

FSM

ICAP

email   network   web

Deliver consistent data security from the Cloud to the Endpoint

Increase Productivity

Remove obstacles to cloud adoption from managed devices & BYOD

Cut Costs

Eliminate redundant, fragmented solutions—unify policies & incident management

Reduce Risk

Prevent data loss in cloud apps, laptops, BYOD; protect customer data & brand reputation

Streamline Compliance

Show that data security policies are enforced consistently wherever the data is used

Control website uploads/downloads by people, programs, and more

Web security that's close to people and data: cloud | network | endpoint

Keep sensitive data in, malware out

Safeguard managed & agentless devices (Wi-Fi, BYOD, IoT)
- Enforce in cloud or at network edge

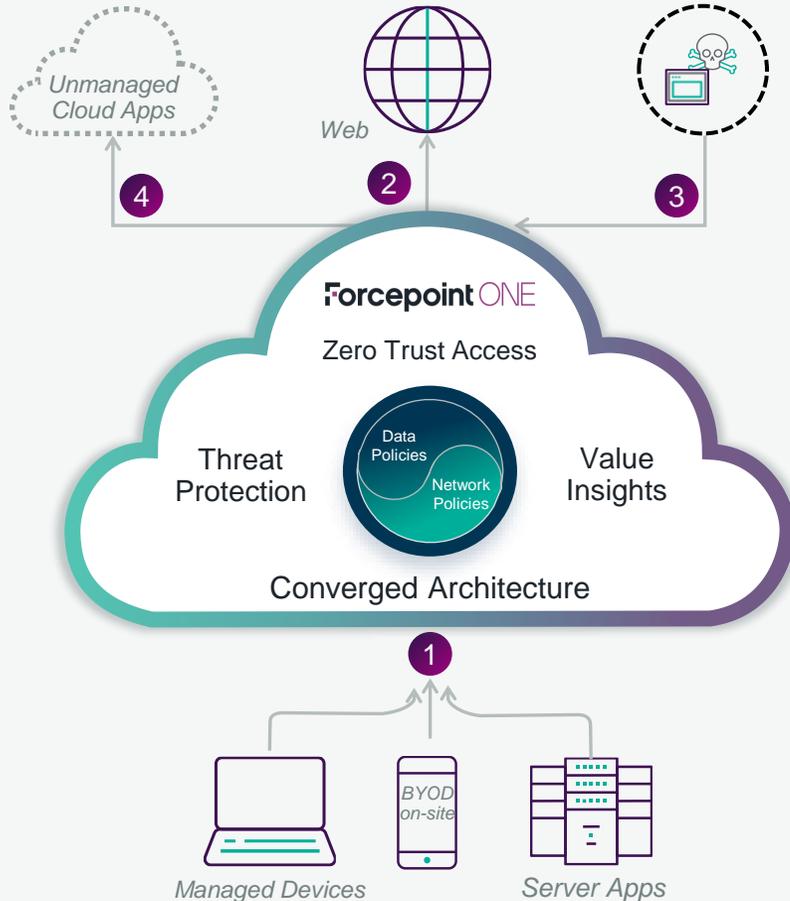Provide a better browsing experience, use bandwidth more efficiently
- Enforce on endpoint (up to 2X faster) or at network edge
- Have location-aware apps work properly

Inspect data uploaded from server apps, IoT, etc. to web storage

Web

DLP — SWG

No Agent

Managed Device

BYOD on-site

Server Apps

Web
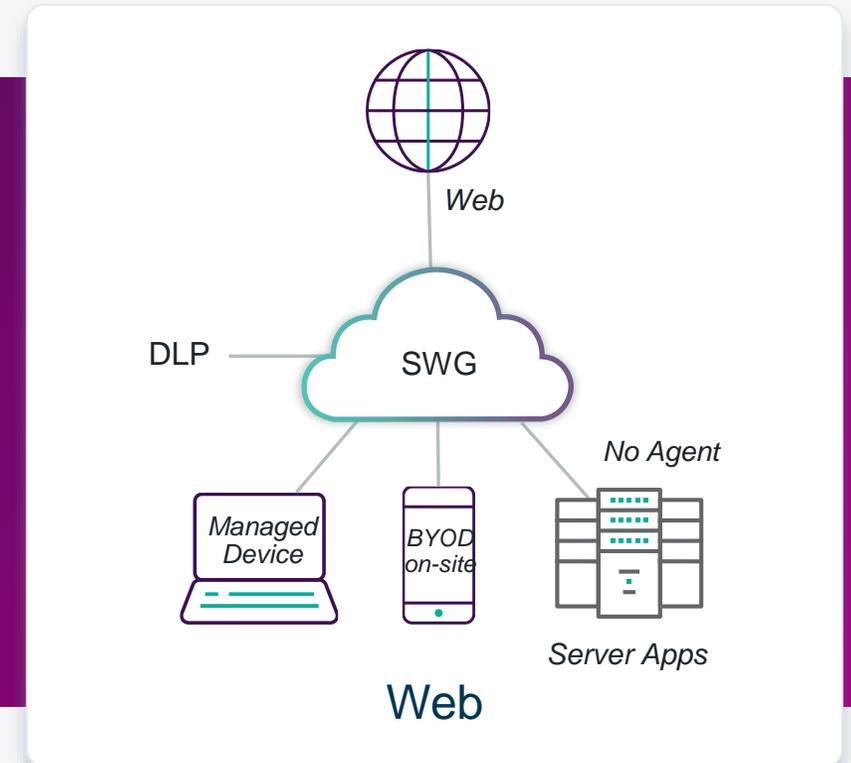
Secure data—and access—on the web with consistent policies everywhere

Data-first SASE architecture

Forcepoint ONE

Zero Trust Access

Threat Protection

Data Policies

Network Policies

Value Insights

Converged Architecture

Unmanaged Cloud Apps

Web

Managed Devices

BYOD on-site

Server Apps

1 **Scan** uploads for sensitive data with DLP policies
- Extensive customization for inline DLP controls without app integrations

2 **Enforce** granular controls over user web activities
- Ensure compliance with Acceptable Use Policies

3 **Prevent** web threats and malware downloads
- Data-in-motion malware scanning
- Safe use of any website or download document via RBI/CDR (complete with DLP enforcement)

4 **Detect** and manage Shadow IT—prevent data loss

Put security close to users/data with multi-tier Distributed Enforcement

Same policies/dashboards across cloud, network, endpoint

Make web security available anywhere
- Agentless enforcement with GRE and IPSEC support
- Over 300 PoPs

Use bandwidth more effectively
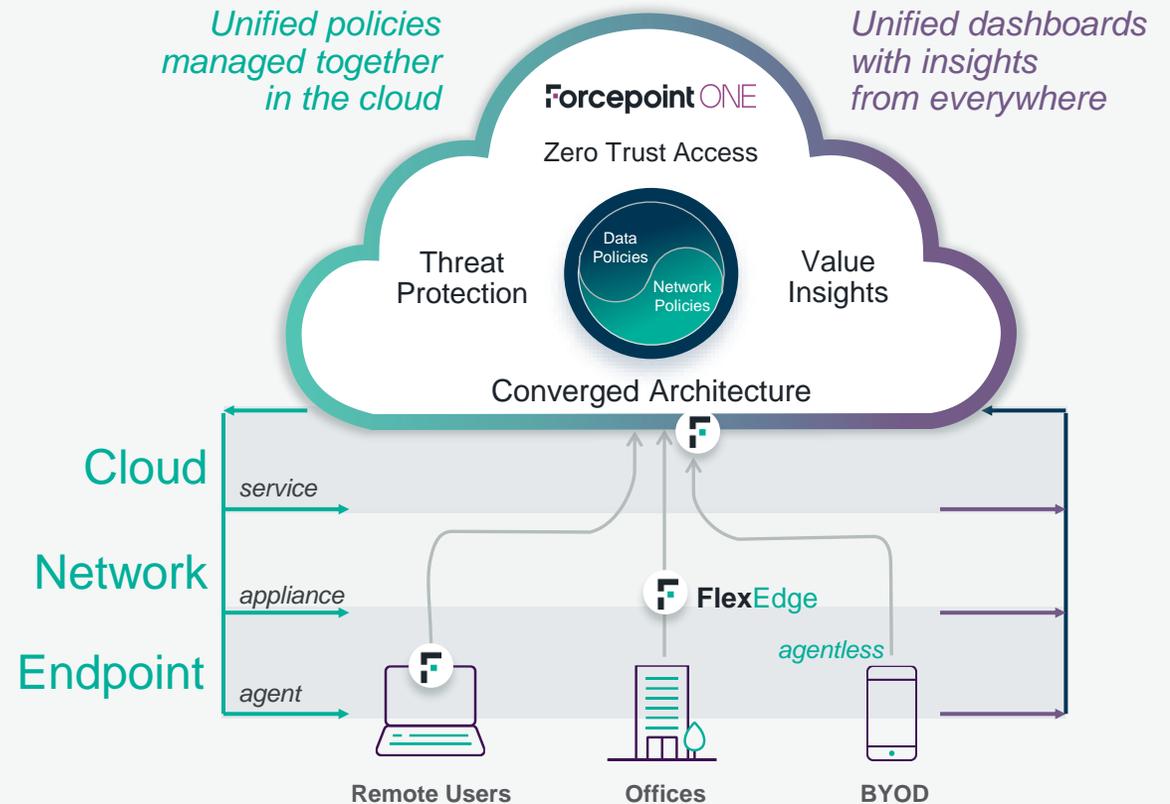- Enforce locally for low-bandwidth environments

Accelerate web performance
- Up to 2X faster
- Native experience, with location & localization

Connect Safely
- Apply Zero-Trust framework
- Make BYOD safe to use with business apps

Keep sensitive data where it belongs

Unified policies managed together in the cloud

Unified dashboards with insights from everywhere

Forcepoint ONE

Zero Trust Access

Threat Protection

Data Policies

Network Policies

Value Insights

Converged Architecture

F

Cloud — *service*

Network — *appliance*

F FlexEdge

Endpoint — *agent*

agentless

F

Remote Users

Offices

BYOD

Extend web security beyond people—safeguard programs and systems

Monitor and manage data uploaded from server apps, IoT, and more
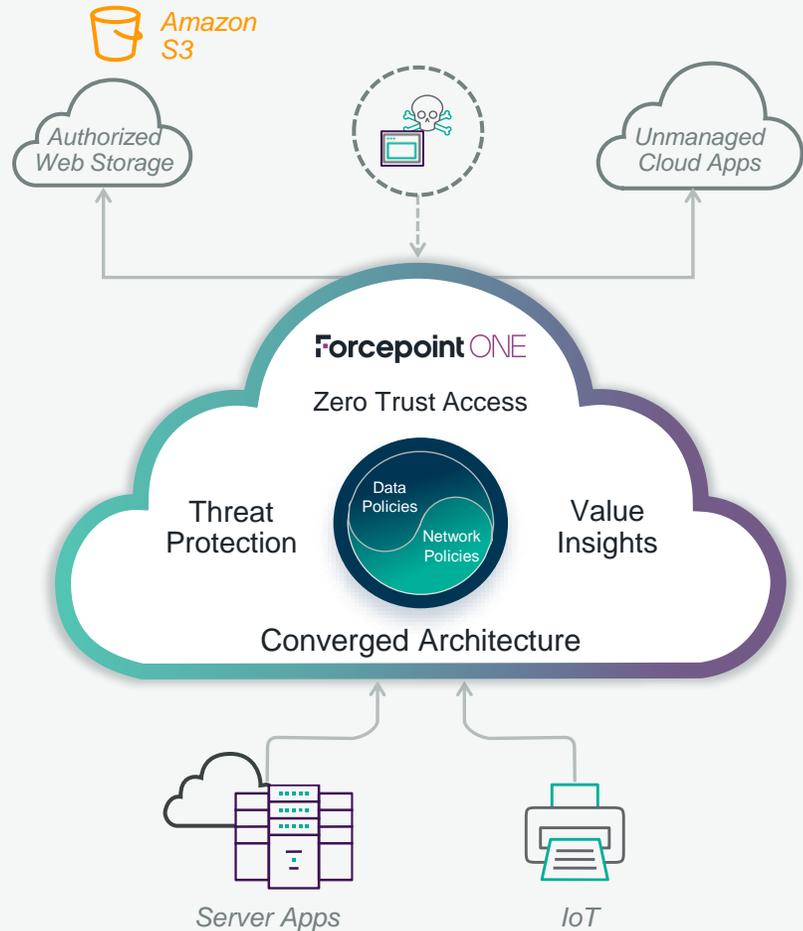
Control uploads of sensitive data to web-based storage
- From physical or virtual data centers

Prevent malware from being downloaded to IoT devices

Guard access to unmanaged cloud apps from automated systems

Extend data security policies to the Web and keep threats out

Increase Productivity
Enable safe usage of any website or downloaded document

Cut Costs
Eliminate redundant, fragmented solutions that have ineffective controls

Reduce Risk
Prevent data loss in web apps or contamination from malware

Streamline Compliance
Make data security consistent across web and other channels for more efficient compliance

Prevent the #1 form of data theft: unauthorized email contents

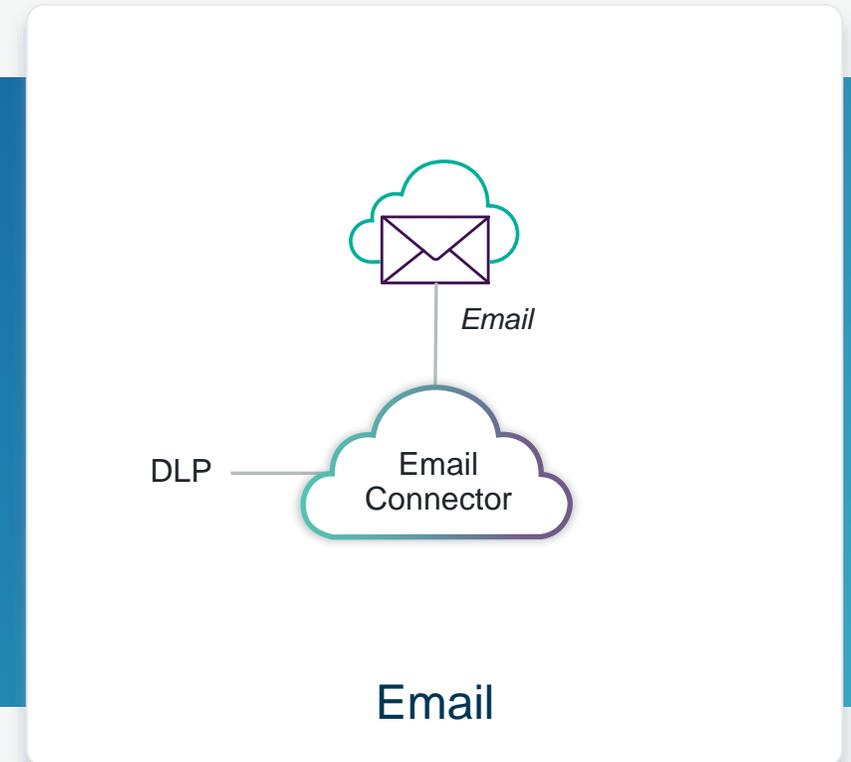Security that's easy to deploy in minutes

Control what can be emailed out of your organization

No agent required—supports all mail clients

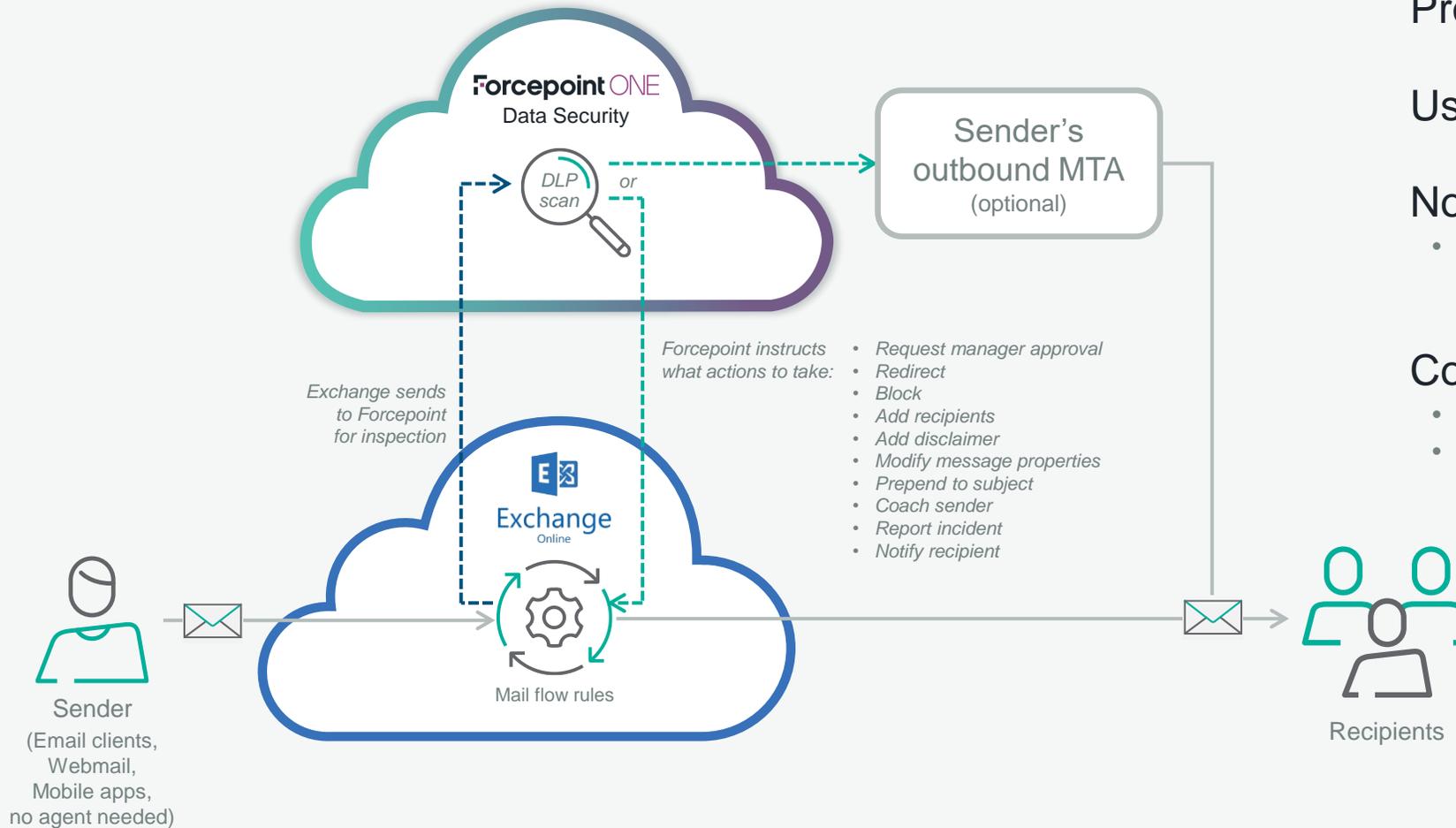Apply same data security policies, dashboards everywhere

Integrated with Exchange for native workflow like 'Manager Approval'

Complement in-bound threat protection solutions

Email

DLP —— Email Connector

Email

Forcepoint DLP for Cloud Email

Visibility and control of what can be emailed out of your organization

Forcepoint ONE
Data Security

DLP scan or

Sender's outbound MTA
(optional)

Exchange sends to Forcepoint for inspection

Exchange
Online

Mail flow rules

Forcepoint instructs what actions to take:
- *Request manager approval*
- *Redirect*
- *Block*
- *Add recipients*
- *Add disclaimer*
- *Modify message properties*
- *Prepend to subject*
- *Coach sender*
- *Report incident*
- *Notify recipient*

Sender
(Email clients, Webmail, Mobile apps, no agent needed)

Recipients

Provides enhanced control over email

Use any email app—no agent needed

No new consoles to learn
- Incidents and policies managed in same console as other channels

Complements other email solutions
- Inbound threat protection
- Outbound MTAs

Prevent data loss over Email

Increase Productivity
Enable people to work with sensitive data without the risk of losing control of it

Cut Costs
Eliminate need for additional consoles, duplicate policies, specialized agents

Reduce Risk
Stop #1 way that data is stolen

Streamline Compliance
Provide consistent visibility and control over data that leaves the organization

# Take security to the next level with Risk-Adaptive Protection

Automation that use Zero Trust to make digital security work more like the real world

Give people access to the data you trust them to use, with 'guardrails'

Continuously monitor for risky behavior

If people make mistakes or show poor judgement, dynamically coach, increase logging, adapt

Focus harshest actions (blocking) on people who pose the most risk—without causing problems for everyone else
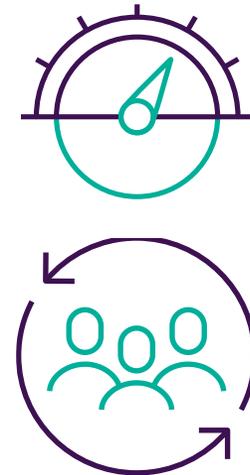
Risk-Adaptive Protection

Pioneered by Forcepoint

Risky user behavior creates problems for data security

Static solutions lack visibility and impede business due to false positives

50% of all data breaches due to insider risky behavior

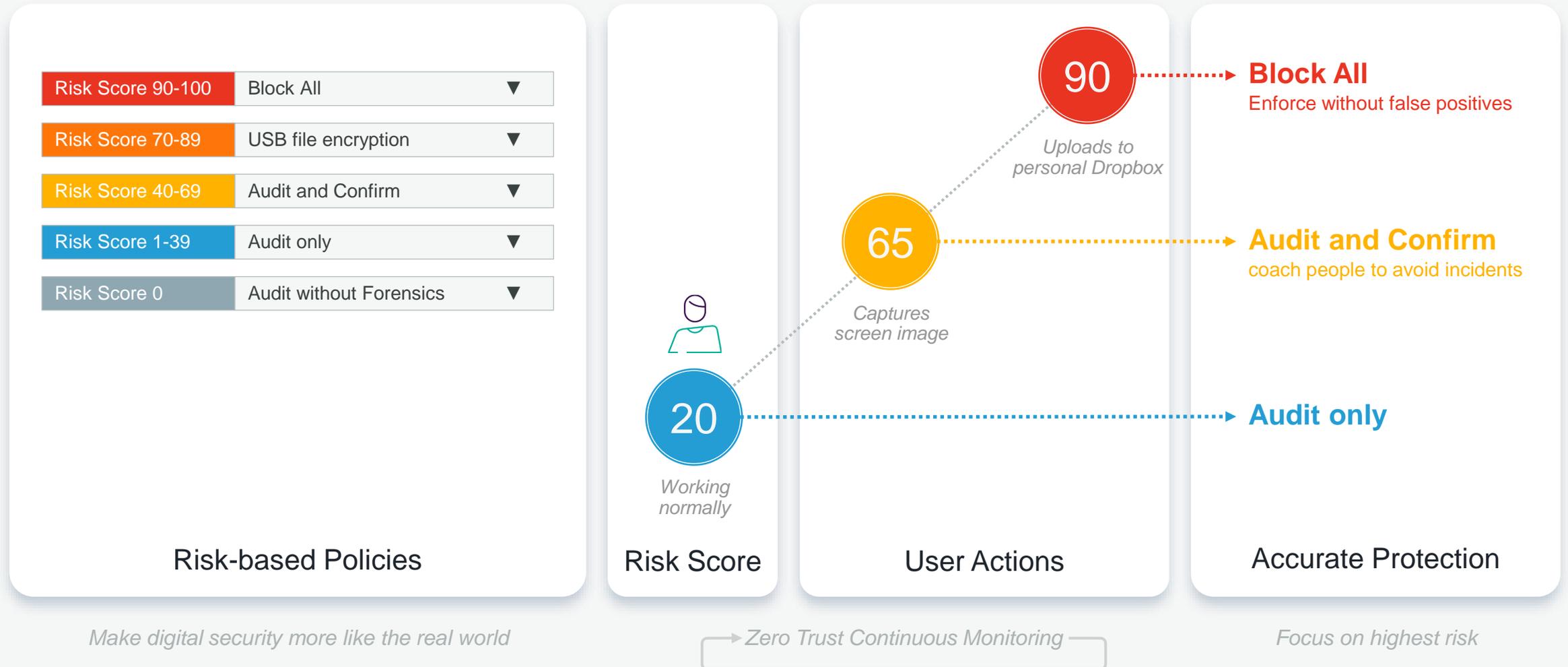Strong data security often conflicts with business productivity

DLP incident alert overload increasing security admin fatigue

Most user risk programs only monitor behavior—without fixing the problem of false positives
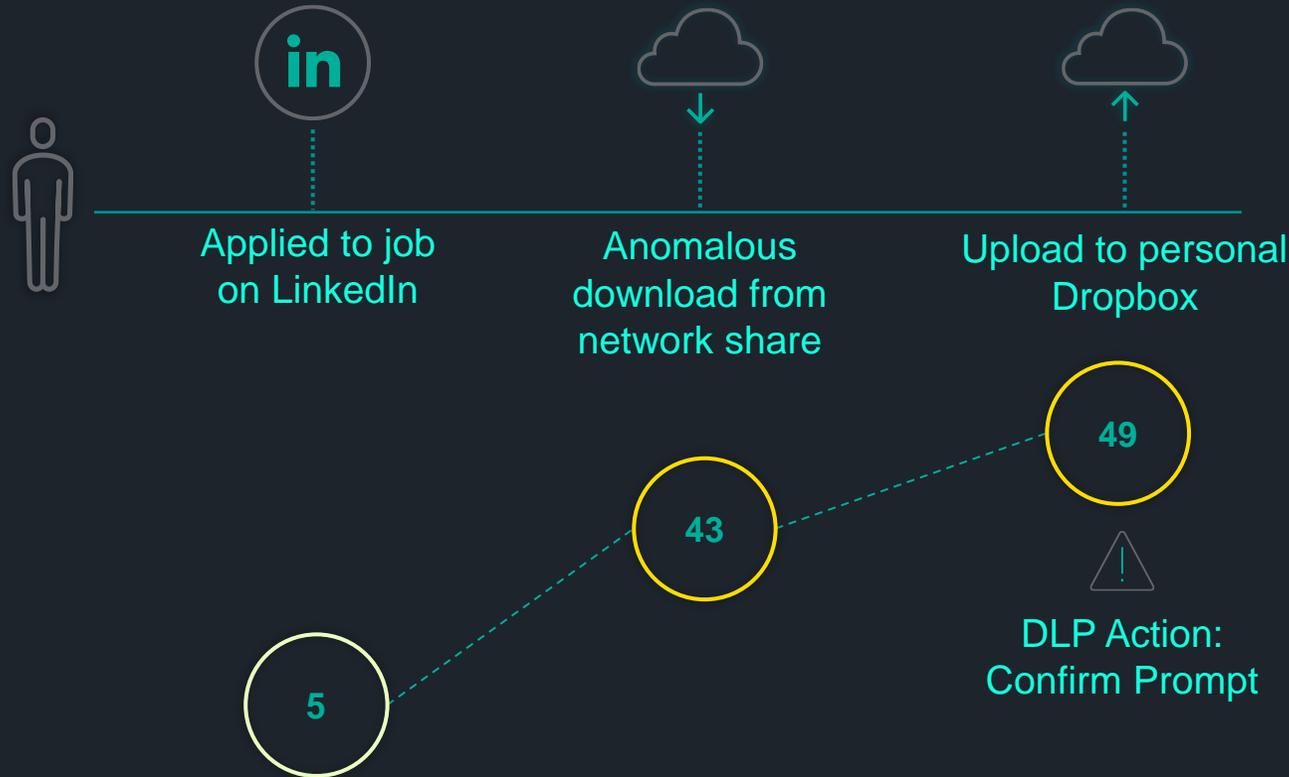
Risk-Adaptive Protection

Automate insights/enforcement and simplify operations with contextual security

Risk-based Policies

Risk Score 90-100	Block All ▼
Risk Score 70-89	USB file encryption ▼
Risk Score 40-69	Audit and Confirm ▼
Risk Score 1-39	Audit only ▼
Risk Score 0	Audit without Forensics ▼

Risk Score

90 Uploads to personal Dropbox

65 Captures screen image

20 Working normally

User Actions

Accurate Protection

Block All
Enforce without false positives

Audit and Confirm
coach people to avoid incidents

Audit only

Make digital security more like the real world

Zero Trust Continuous Monitoring

Focus on highest risk

Getting DLP Policies based on user risk scoring

☑ For Risk-Adaptive Protection users, determine actions according to the source's risk level:

Risk level 1	Risk level 2	Risk level 3	Risk level 4	Risk level 5
Action plan: Audit Only ▾	Audit Only ▾	EP Confirm ▾	Encrypt ▾	BLOCK ALL ▾

in

Applied to job
on LinkedIn

Anomalous
download from
network share

Upload to personal
Dropbox

49

43

5

⚠
DLP Action:
Confirm Prompt

❑ Risk Level 1 = Score 0

❑ Risk Level 2 = Score 1-39

❑ Risk Level 3 = Score 40-69

❑ Risk Level 4 = Score 70-89

❑ Risk Level 5 = Score 90-100

Forcepoint

Automate and simplify data security with Risk-Adaptive Protection

Increase Productivity

Eliminate data security friction that gets in the way of business

Cut Costs

Simplify incident management and eliminate false positives that chew up everyone's time

Reduce Risk

Automate enforcement to progressively adapt based on the risk each user presents

Streamline Compliance

Strengthen compliance with privacy regulations through more-accurate policy enforcement

Modernize with Data Security Posture Management (DSPM)

AI-powered automation for discovery, classification, orchestration

Discover where your sensitive data resides

Classify data to make policies and reporting consistent

**Prioritize** where to focus data security efforts the most

Protect intellectual property and regulated data everywhere

Monitor risk to data to dynamically adapt policies
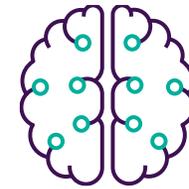
AI-powered discovery, classification, orchestration

Data security begins with having good your visibility into data

Discover — **Classify** — **Prioritize** — **Protect** — **Monitor**

20% Visible

DARK DATA

80% Hidden
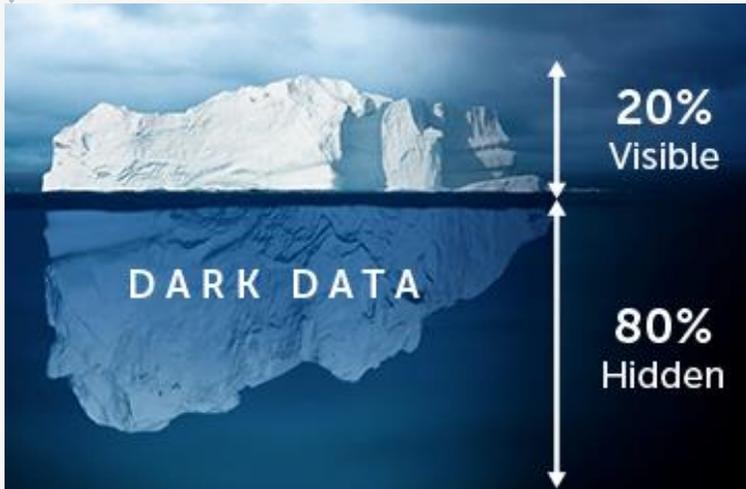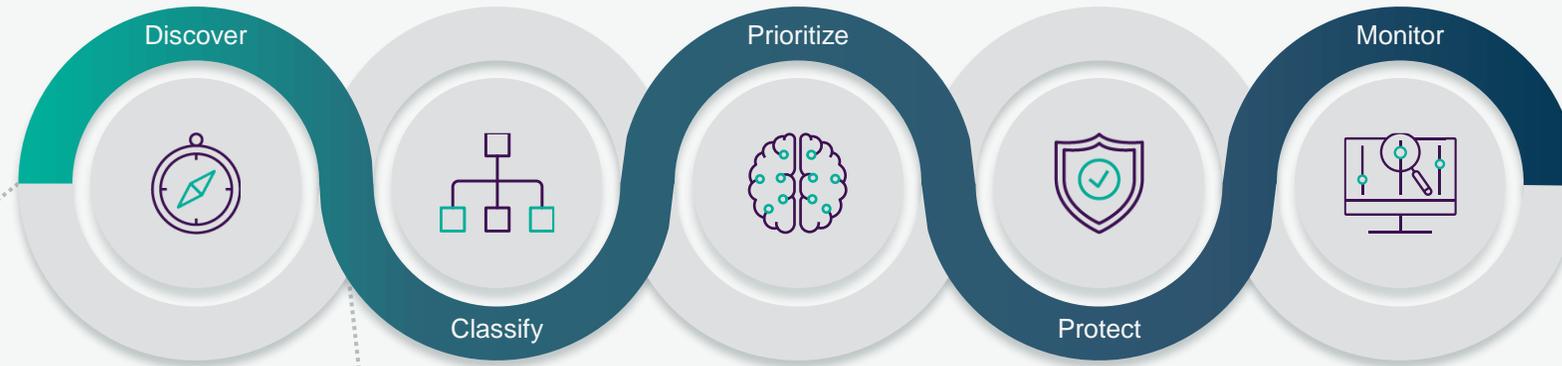
Visibility into unknown/unused data is key to reducing risk

Accurate classification simplifies policy definition & automation

Understanding data & permissions is first step to preventing breaches

Policy enforcement automation greatly reduces gaps & false positives
- Typical DSPM remediation workflows are too manual

Data security is continuous—monitoring & adapting to change

Forcepoint DSPM

AI powered discovery and classification with real-time risk reporting and remediation orchestration
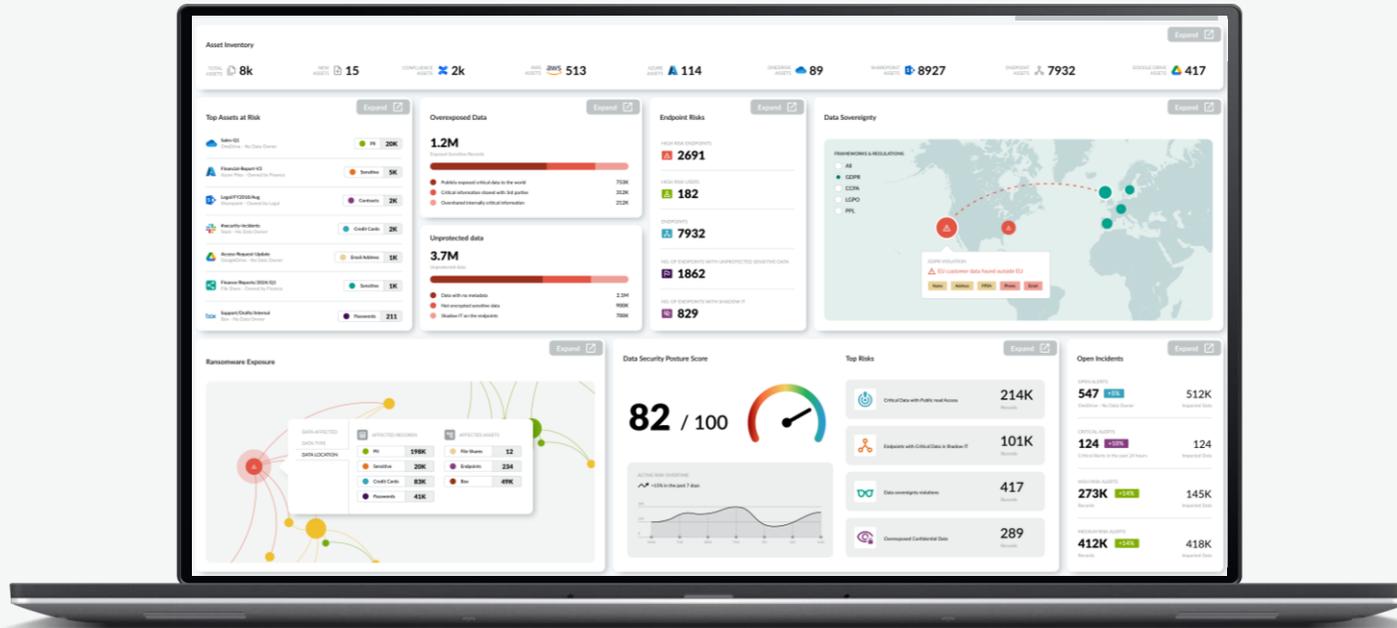
High-speed, comprehensive discovery

(in the cloud and on-prem; unstructured data now, structured data soon)

AI-powered data classification

(powered by a highly trained 50-dimensional model)

Real-time monitoring and risk assessment

(checks access permissions and other data risks)

Powerful remediation and workflow orchestration

(implements business priorities for stakeholder groups; helps automate fixing of data risks)

Modernize and automate the data security lifecycle with AI-powered DSPM technologies

Increase Productivity
Enable faster, safer data access and sharing for better innovation and collaboration

Cut Costs
Automate to reduce time and resources spent on data security investigations & remediation

Reduce Risk
Prevent breaches by uncovering and taking care of sensitive data not being used properly


Streamline Compliance
Gain true visibility and control over sensitive data throughout your organization

DSPM- DRA Introduction

Free tool

By running a DRA a customer gains insight into a sample subset of their data,

exposing the risks and vulnerabilities in the organization which they likely have no insight into.

Utilizing the DSPM product, the report can be produced in a matter of days
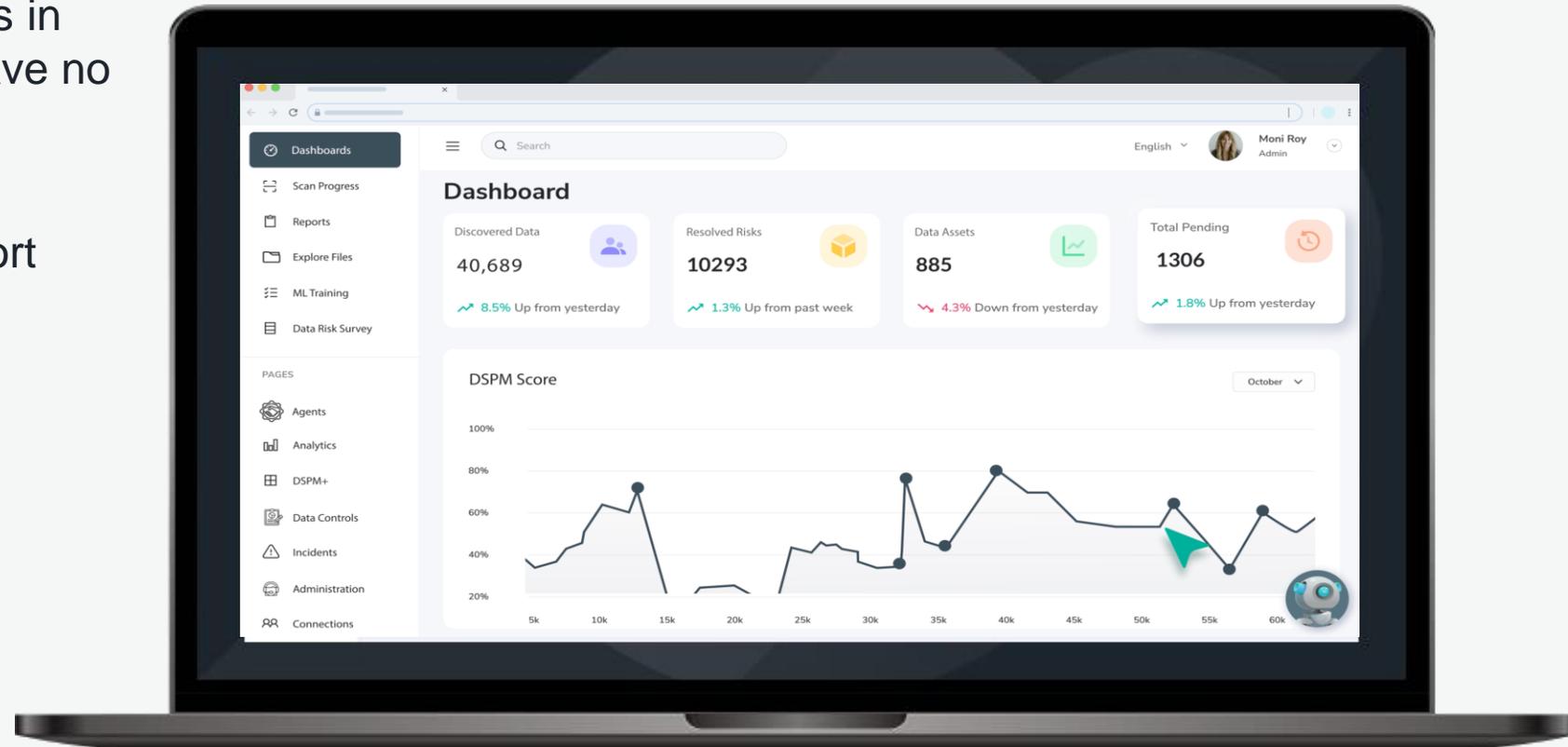
Empower your people and your business with Forcepoint

Forcepoint
FREE
DRA
Data Risk Assessment

Forcepoint
Security. Simplified.

Security that enables today's global business

IBM

CDW · TOYOTA

accenture

Qualcomm

"Probably the **easiest deployment I've seen in my entire IT career,…it's like an easy button for CIOs.**"

– CIO, US Agency

~12,000	14,000+	20M+	700+	300+	~21B	2.1B	5M
Customers	Transactions, LTM	Licensed Seats	F|ONE Customers	Global PoPs	Web transactions processed per day (3.9T per year)	Policy violations prevented per day	Security incidents prevented per day

Industry Awards

Corporate Awards

Product Leadership Awards

Empower your people and your business with Forcepoint

Forcepoint

Data Security Everywhere

AI | Zero Trust | DSPM | Risk-Adaptive | DLP | Email | CASB | ZTNA | SWG | RBI | CDR | SD-WAN

Increase Productivity

Cut Costs

Reduce Risk

Streamline Compliance

Teşekkür ederim.

altan.yarar@forcepoint.com

Forcepoint