Last update: March 2020

imperva

PRODUCT ROADMAP

Runtime Application Self-Protection

RASP

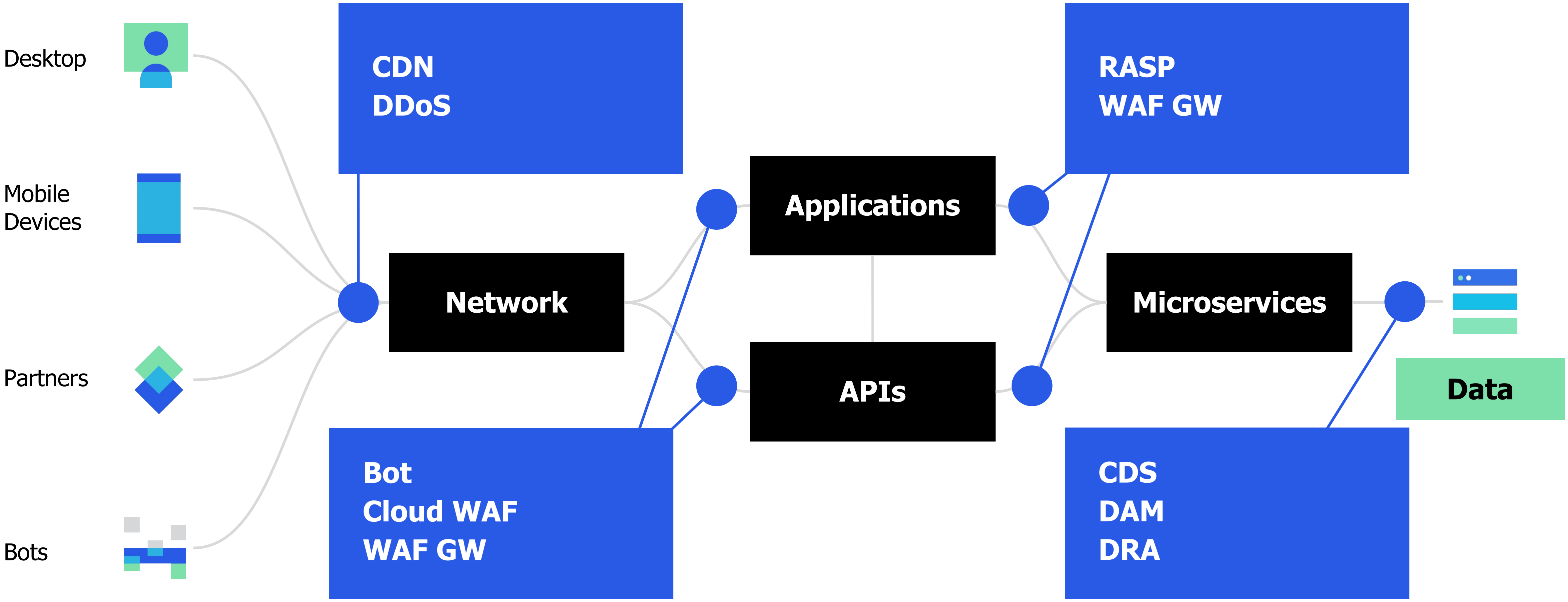
Disclaimer

This presentation is being provided for INFORMATIONAL PURPOSES ONLY. The information provided represents Imperva’s expectations as of the date the presentation was prepared. Imperva undertakes no obligation to update or revise this information. The information should not be construed as a commitment to deliver any specific upgrade or feature or functionality.

Imperva may change the contents of the presentation in its sole discretion at any time. You should not rely on the anticipated timelines or potential upgrades, features or functionality described in the presentation when making a decision to purchase products from Imperva.

Imperva protects data and all paths to it

The imperva Products Portfolio



Desktop

Mobile Devices

Partners

Bots

CDN
DDoS

Bot
Cloud WAF
WAF GW

Network

Applications

APIs

RASP
WAF GW

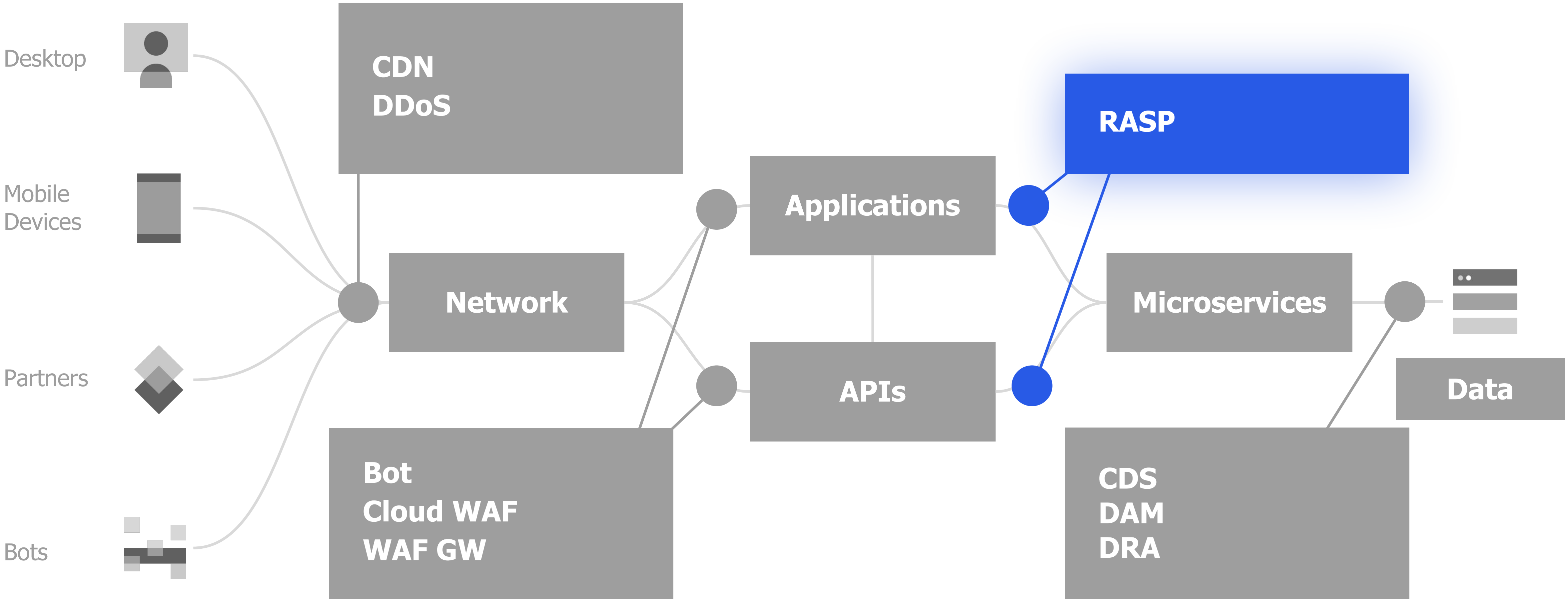
Microservices

CDS
DAM
DRA

Data

Proprietary and confidential. Do not distribute.

Runtime Application Self-Protection



Desktop

Mobile Devices

Partners

Bots

CDN
DDoS

Network

Bot
Cloud WAF
WAF GW

Applications

APIs

RASP

Microservices

Data

CDS
DAM
DRA

Proprietary and confidential. Do not distribute.

RASP - Recently Delivered

Scale

Added Dot.net Core

Redesign Manager in v3

Data & Forensics

Provided insights in SIEMs in real time

Policy alignment between languages

Agent Enhancements

RASP.lib core engine

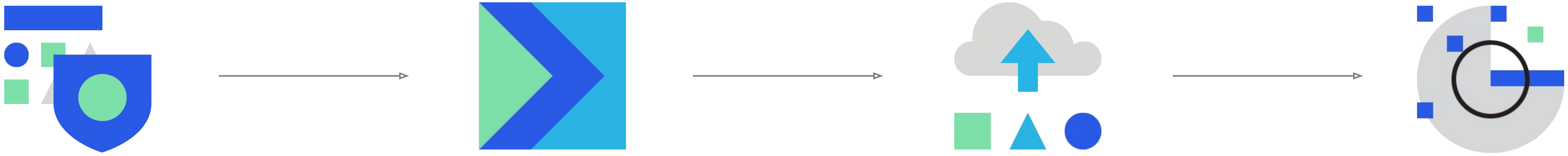
Ability to run along other agents

RASP Looking Forward

Insights	Attack Analytics Integration	Imperva One UDT Enhancements		
Advance Controls		License consumption	Centralized Configuration Signed Configuration	Managed by SaaS platform
Innovation			Work out of the box	Deeper In-App Protections
Coverage	Run alongside with others (APM)	Node.js		
	Node.js Beta	Java 11		Additional Language
	Q1	**Q2**	**+6 months**	

RASP + Attack Analytics

Architecture



App with RASP

RASP engine protects your applications and produces alerts in case of attacks

Event Forwarder

Central engine to forward RASP alerts to Attack Analytics

Uploader

- Authentication
- Masking
- Forwarding to the cloud

Attack Analytics in UMC

Attack Analytics distils RASP jointly with other AppSec alerts to provide an account level attack landscape

Languages Support

Node.js

Java11 support

TBD

Pending customers' feedback

Central Management

Control RASP policy changes from central management with signed configuration

Phase 1

Policies are maintained in one central location (Customer environment)

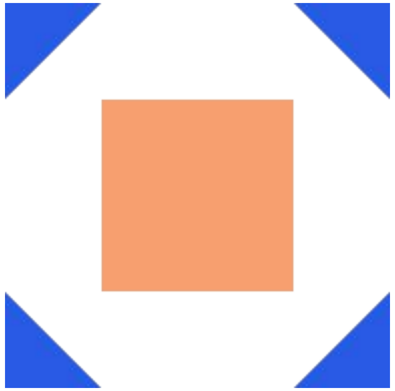
Phase 2

Connect RASP Manager with Imperva SaaS Management (aka UMC)

UMC gives RASP advanced features

Work out of the box

Create a vanila policy to support quick, zero-touch set up



Deep In-App protection

Leverage In-app knowledge to provide advanced security

Thank You!