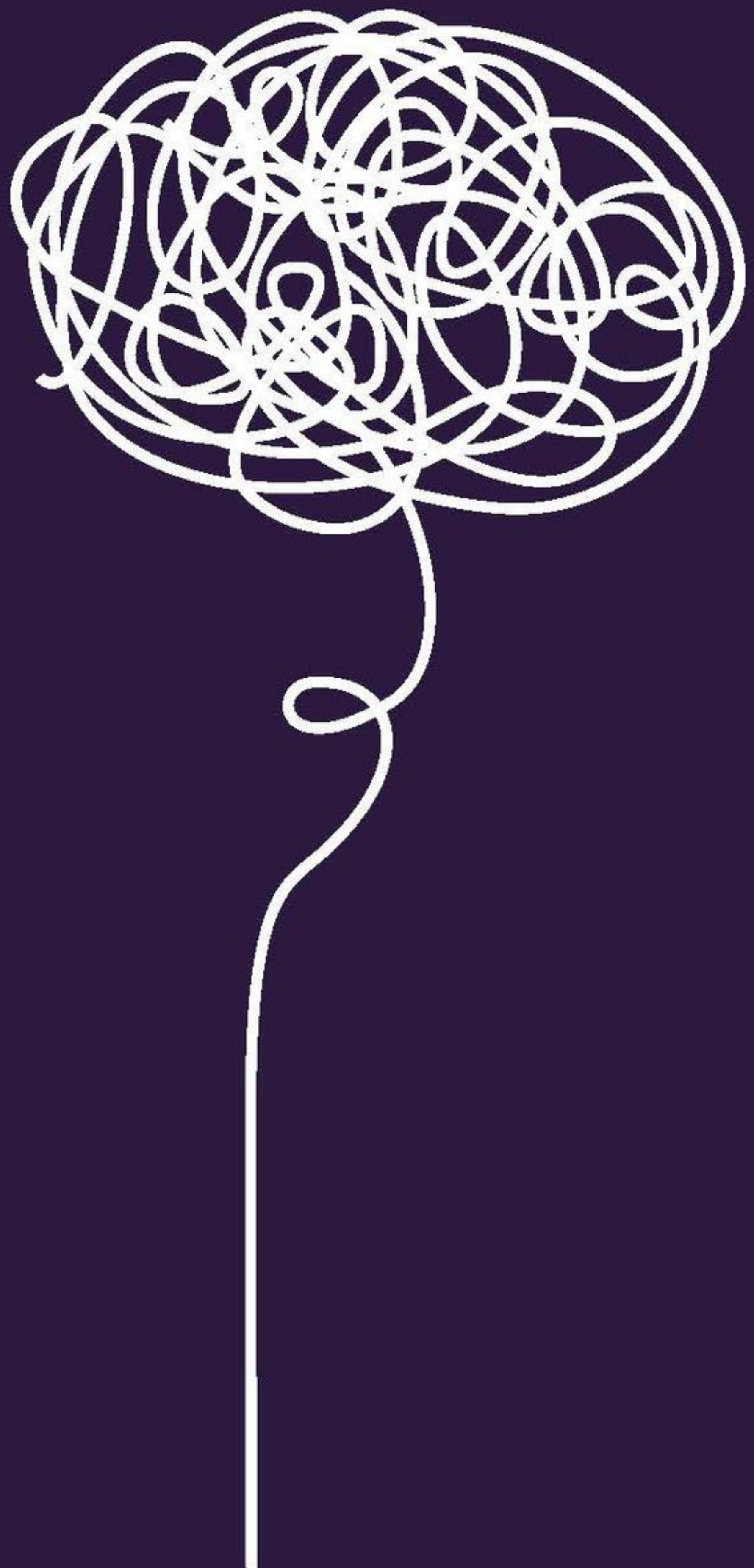


pylones*

*Simplifying
Digital Challenges

*Pylones at a glance

Turnover: >12.1m Euros (steadily increasing for the past 10 years)

Focuses +90% in Private Sector (Corporate & Enterprise ICT Market)

>50 Full Time Employees (25% more than 10 years with the company)

ISO
9001 | 27001 | 27701
20000-1 | 22301 | 14000

CYBERSECURITY™
MADE IN EUROPE

>11 International Projects

50+ vendor certifications (F5, HPE, IBM, AWS, Okta, Palo Alto, Microsoft etc.)

Long term partnership with leading companies in the private sector

13+ International Vendor partnerships

Founded in 1997

Owned by Cyprus based P.M. Tseriotis Group

Activities in Greece, Cyprus, Central & Southern Europe with numerous projects internationally

Pylones a Technology Partner of Choice

To make an **online/mobile banking** transaction or preview your **insurance** identity & contract we gave our best!

85% Banks - 60% Insurance trusting us

with **>100 projects delivered** the past 10 years

When you pick up your mobile phone to call someone or open your **4/5G to surf** be sure that Pylones has put its hands on it**!**

100% Telcos rely on us

with **>150 projects delivered** the past 10

We are in favor from **Large Enterprise Sector** for lots of reasons…

80 different organizations choose us

with **>500 projects delivered** the past 10

Guess who trust Pylones

Public sector trust us too, taking the GOV **digital experience** to the next level

with **>30 projects delivered** the past 3

Companies wants to pick up their phone and help them solve their daily problems

making us their IT support partner of choice

rise of 20% in **Support Contracts** every single

Customer’s **feedback** reflect if **we deliver what we promised**, and every year customers rate us

with up to 95%

8 in 10 customers rate us with **100%**

*NIS2 Directives

*Key Directives

Risk Assessment and Management:

- Conduct regular risk assessments.
- Implement appropriate security measures.
- Develop incident response plans.

Incident Reporting and Notification:

- Establish procedures for reporting and notifying relevant authorities of cybersecurity incidents.
- Cooperate with competent authorities in investigations.

Security Measures:

- Implement appropriate technical and organizational security measures.
- Protect sensitive data and systems.
- Ensure business continuity.

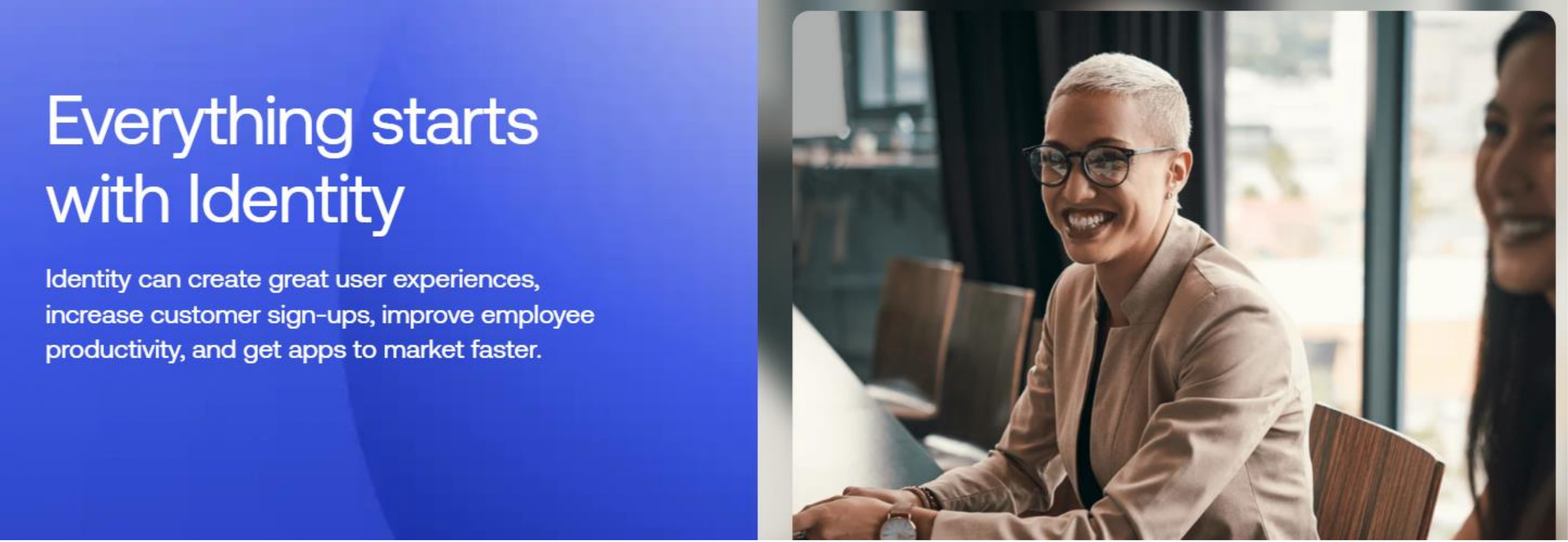
Business Continuity Management:

- Develop and maintain business continuity plans.
- Test and update plans regularly.
- Ensure rapid recovery from incidents.

Key Directives

Risk assessment Directive	Incident Reporting Directive	Security Measures Directive	Business Continuity & DR Directive
F5/Mazebolt (DDoS assessment and protection)	SecurityHQ (SOC services)	Okta (Identity Access Management) Sailpoint (Identity Governance)	Veeam (Backup / Restore / DR for on prem, cloud, hybrid models)
Palo Alto (Firewalls protection - EDR)	Sailpoint (IGA)	F5 – Aruba/HPE (networks security for cloud or on prem or hybrid models)	AWS (Backup for Cloud Infra)
Okta (Identity Access Management) Sailpoint (Identity Governance)	AWS (Cloud)	Palo Alto (Firewalls – Endpoints security)	Aruba/HPE (Networks Backup)
AWS (Cloud infrastructure assessment) Aruba/HPE (Networks assessment)	Palo Alto (Firewalls protection - EDR)	Mazebolt (DDoS assessment and mitigation)	
AEG Swift (Transactions security)		AWS (Cloud security)	
Veeam (Backup security)		Veeam (Immutability and Backup security)	
		AEG Swift (Transactions security)	

Solutions Overview

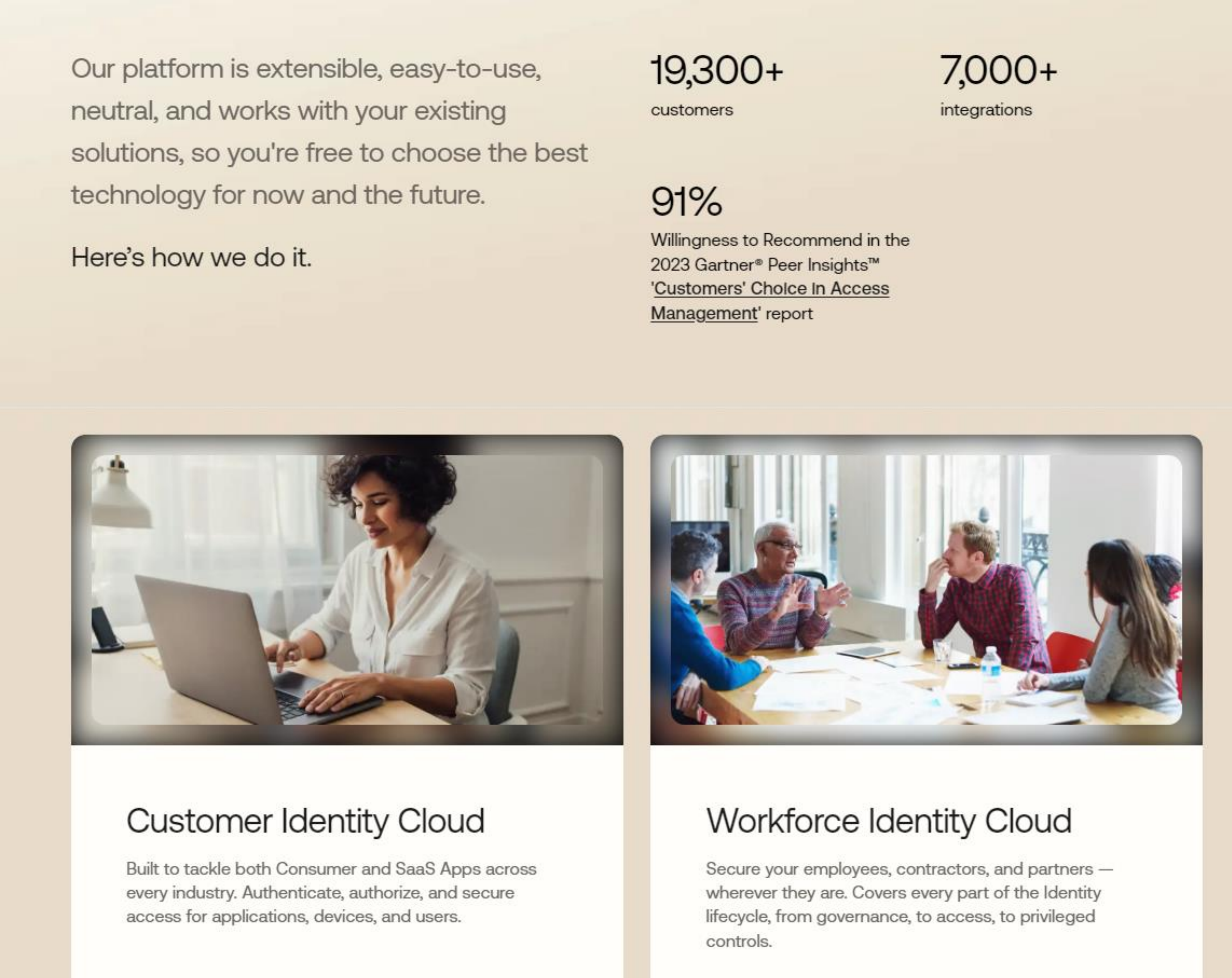


Everything starts with Identity

Identity can create great user experiences, increase customer sign-ups, improve employee productivity, and get apps to market faster.

Identity Access Management

okta



Our platform is extensible, easy-to-use, neutral, and works with your existing solutions, so you're free to choose the best technology for now and the future.

Here's how we do it.

19,300+ customers	7,000+ integrations
91% Willingness to Recommend in the 2023 Gartner® Peer Insights™ 'Customers' Choice In Access Management' report	

Customer Identity Cloud

Built to tackle both Consumer and SaaS Apps across every industry. Authenticate, authorize, and secure access for applications, devices, and users.

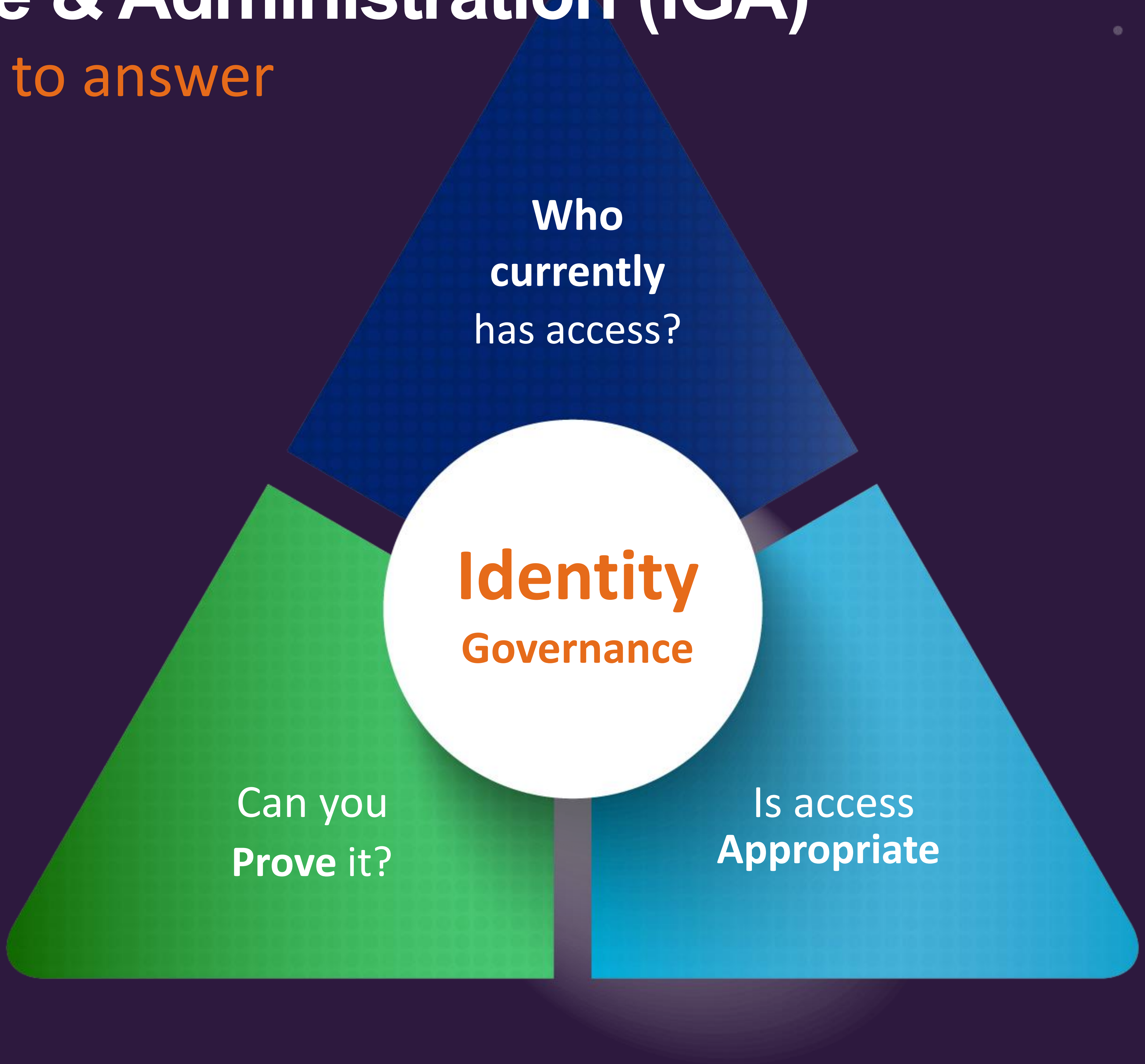
Workforce Identity Cloud

Secure your employees, contractors, and partners — wherever they are. Covers every part of the Identity lifecycle, from governance, to access, to privileged controls.

* Identity Governance & Administration (IGA)

SailPoint enables organizations to answer

3 CRITICAL QUESTIONS



Who currently has access?

Identity Governance

Can you **Prove** it?

Is access **Appropriate**

SailPoint Identity Platform

Lifecycle Management

Provisioning

Access Request

Compliance Management

Access Certification

Separation of Duty

Data Access Governance

File Access Management

Cloud Governance

SaaS Management

Password Management

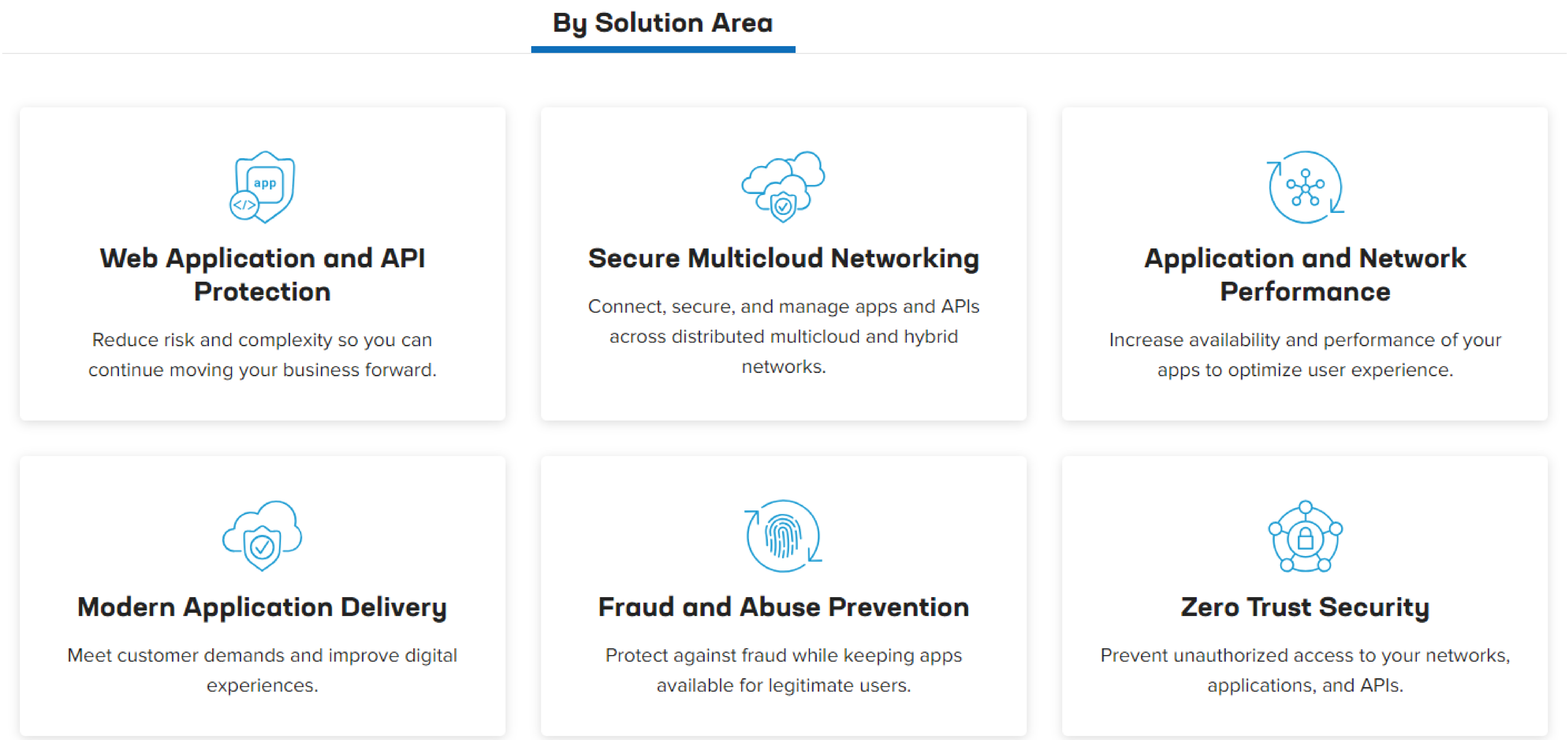
Access Risk Management

Access Modeling

Access Insights

Recommendations

Secure Every App



By Solution Area

Web Application and API Protection

Reduce risk and complexity so you can continue moving your business forward.

Secure Multicloud Networking

Connect, secure, and manage apps and APIs across distributed multicloud and hybrid networks.

Application and Network Performance

Increase availability and performance of your apps to optimize user experience.

Modern Application Delivery

Meet customer demands and improve digital experiences.

Fraud and Abuse Prevention

Protect against fraud while keeping apps available for legitimate users.

Zero Trust Security

Prevent unauthorized access to your networks, applications, and APIs.

Continuous Defense

F5 mitigates risk and improves digital resiliency by continuously defending critical business logic behind apps and APIs.

Consistent Security

F5 dramatically simplifies operations to reduce tool sprawl and complexity by providing end-to-end observability and uniformly protecting the entire digital fabric.

Confident Innovation

F5 solutions allow customers to grow with confidence by aligning security to digital strategy and removing the burden of manual policy tuning and remediation fire drills that distract your teams from their core mission.

API Protection

F5 secures your APIs across a complex hybrid and multi-cloud fabric with F5® Distributed Cloud WAAP—reducing risk and complexity while improving operational efficiencies—so you maintain visibility and control across your entire digital ecosystem.

Get App Security Without Compromise

Explore Web App and API Protection Solutions

Mitigate Application Vulnerabilities

Protecting your apps against critical risks—such as the threats listed in the OWASP Top 10—requires comprehensive and consistent security.

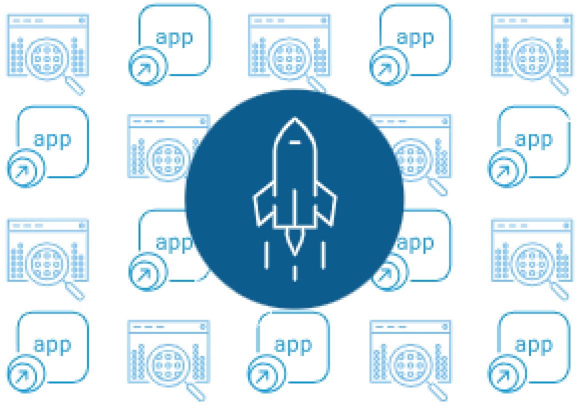
F5 solutions protect apps and APIs everywhere with comprehensive security controls and uniform observability and enforcement—including virtual patching of risks discovered through penetration testing, and simplified lifecycle management of security policies across hybrid and multicloud environments for all application architectures.

Protect Against DDoS Attacks

Organizations of all sizes run the risk of being hit with denial-of-service attacks. The common goal of these attacks is to disrupt performance and availability, but the attacks themselves vary. F5 solutions connect into any architecture to combat blended, multi-vector DoS and DDoS attacks in the deployment model that makes sense for your business.

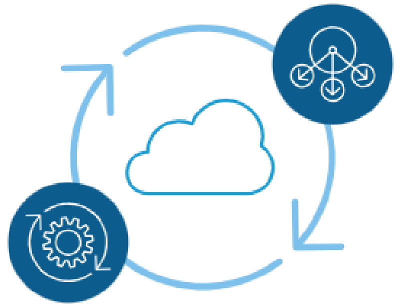
Integrated multi-layer security

Advanced protection keeps threats from reaching applications, including DDoS, network and web app firewalls, and static and dynamic API security to protect services regardless of origin and documentation, leveraging cross-site orchestrated origin and destination identity.



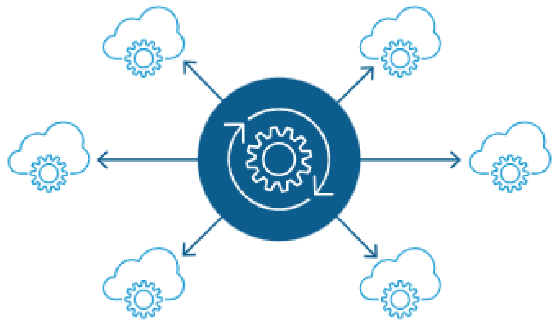
Improved app deployment and observability

Flexible and scalable deployment of modern apps and legacy VMs brings the workload to the data or to the user, with end-to-end network visibility, API mapping and security, and app analytics and observability.



Cross-cloud agility

Unified management of infrastructure and workloads across multiple compute environments creates flexible deployment, simple and secure app-to-app interconnection, and consistent policy enforcement across cloud, data center, and edge.



Operational simplicity

An integrated, automated, and consistent set of SaaS-based services in every environment reduces management effort and misconfigurations, and improves cross-team coordination and productivity.

Web Application Firewall (AWAF)

BOTs

- Proactive bot defense
- Anti-bot mobile SDK
- Client and server monitoring

Account Takeover

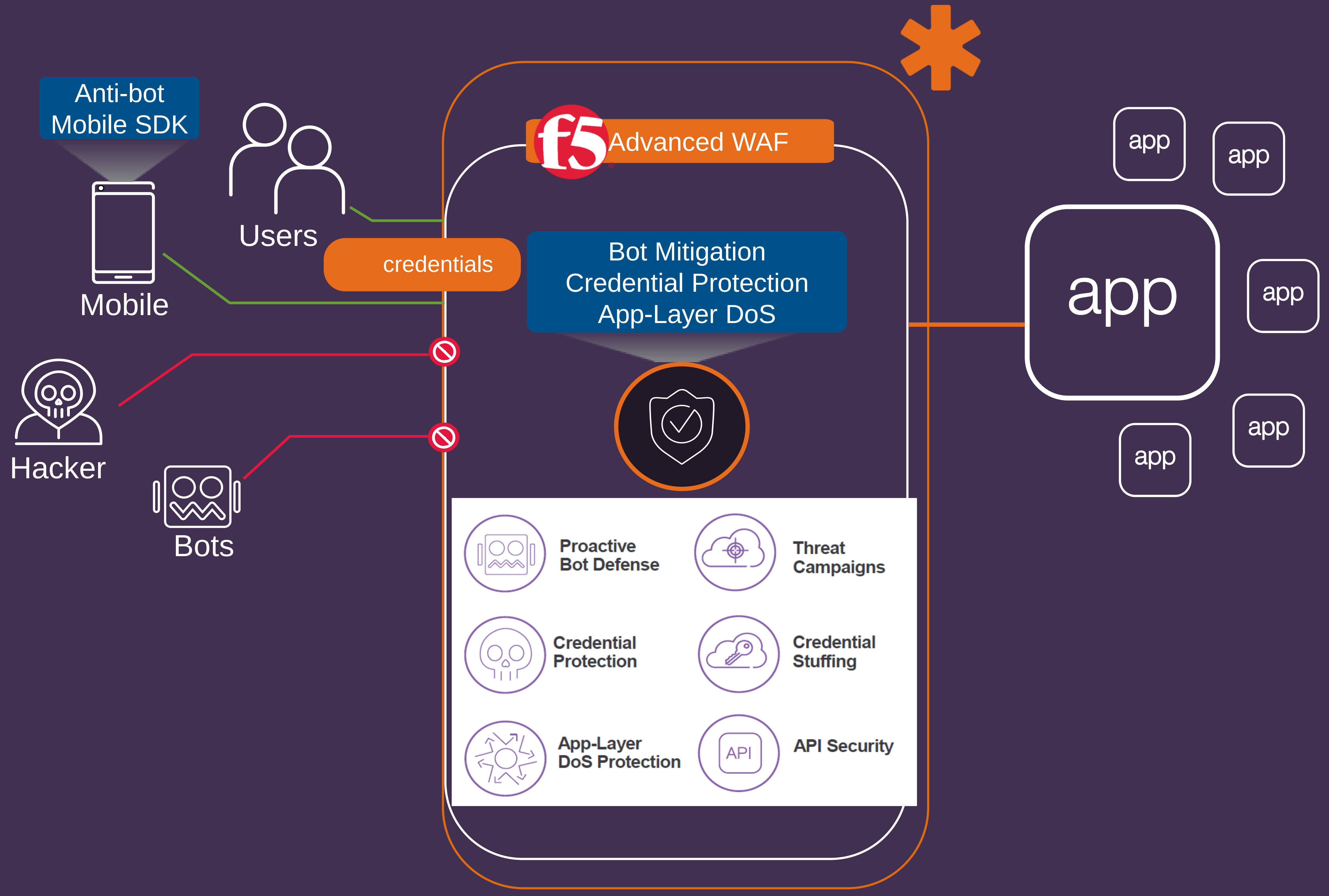
- App-level encryption
- Mobile app tampering
- Brute Force protection

APPs from DoS

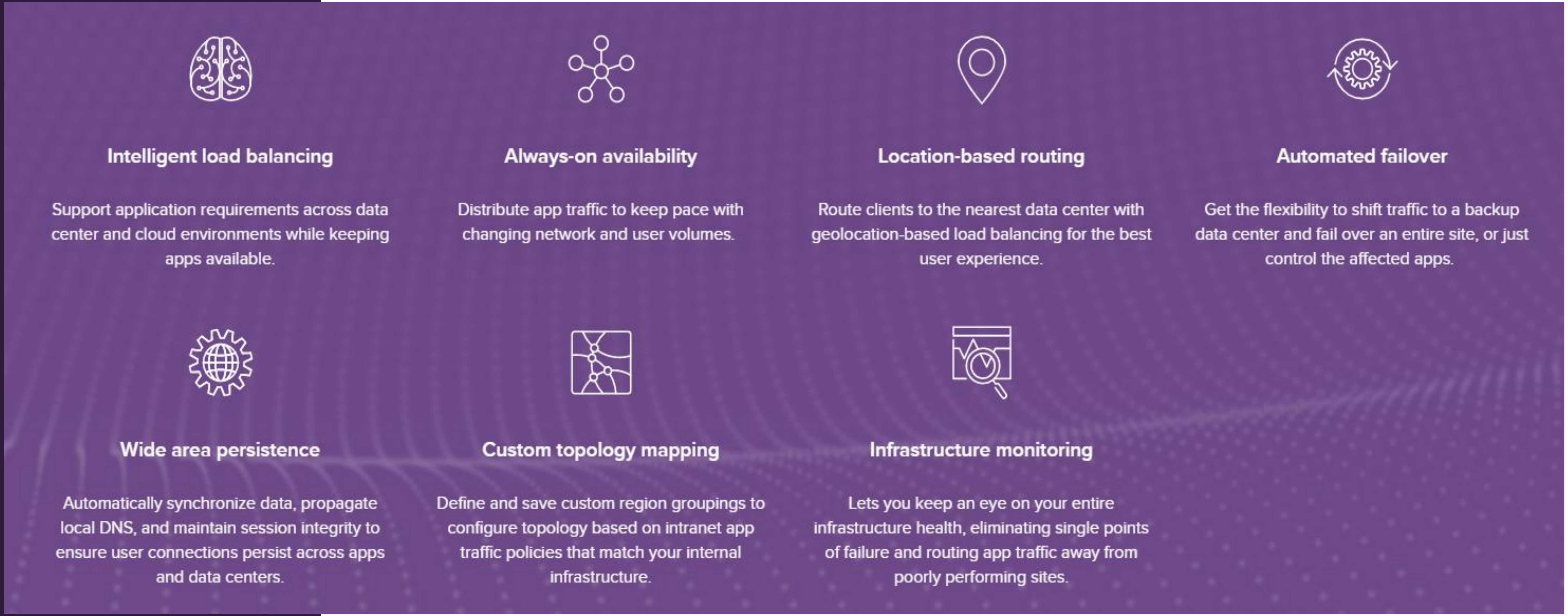
- Auto-tuning
- Behavioral analytics
- Dynamic signatures

APIs from all above

OWASP Compliance Dashboard



LTM – Not so BASIC Load Balancer



Intelligent load balancing

Support application requirements across data center and cloud environments while keeping apps available.

Always-on availability

Distribute app traffic to keep pace with changing network and user volumes.

Location-based routing

Route clients to the nearest data center with geolocation-based load balancing for the best user experience.

Automated failover

Get the flexibility to shift traffic to a backup data center and fail over an entire site, or just control the affected apps.

Wide area persistence

Automatically synchronize data, propagate local DNS, and maintain session integrity to ensure user connections persist across apps and data centers.

Custom topology mapping

Define and save custom region groupings to configure topology based on intranet app traffic policies that match your internal infrastructure.

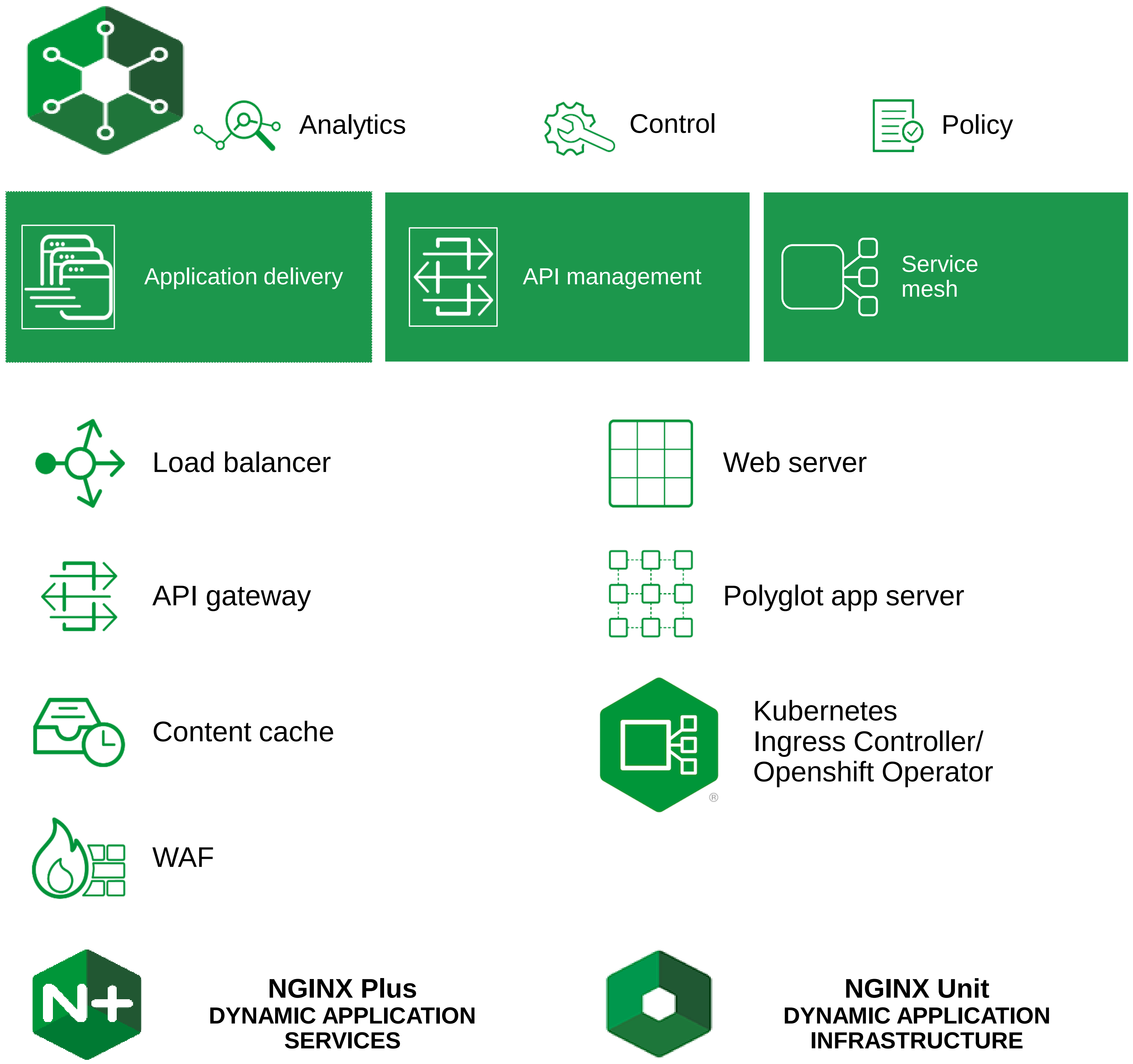
Infrastructure monitoring

Lets you keep an eye on your entire infrastructure health, eliminating single points of failure and routing app traffic away from poorly performing sites.

- Full proxy for protocol/traffic inspection, manipulation and optimisation
- Sophisticated programmability iRules
- Extensive protocol support

High-Performance APP Delivery + API Mgmnt

- Modern, Fast, Scalable
- Lightweight
- Enterprise-grade APP Delivery
- Security onboard
- No sacrifice in performance



Analytics

Control

Policy

Application delivery

API management

Service mesh

Load balancer

Web server

API gateway

Polyglot app server

Content cache

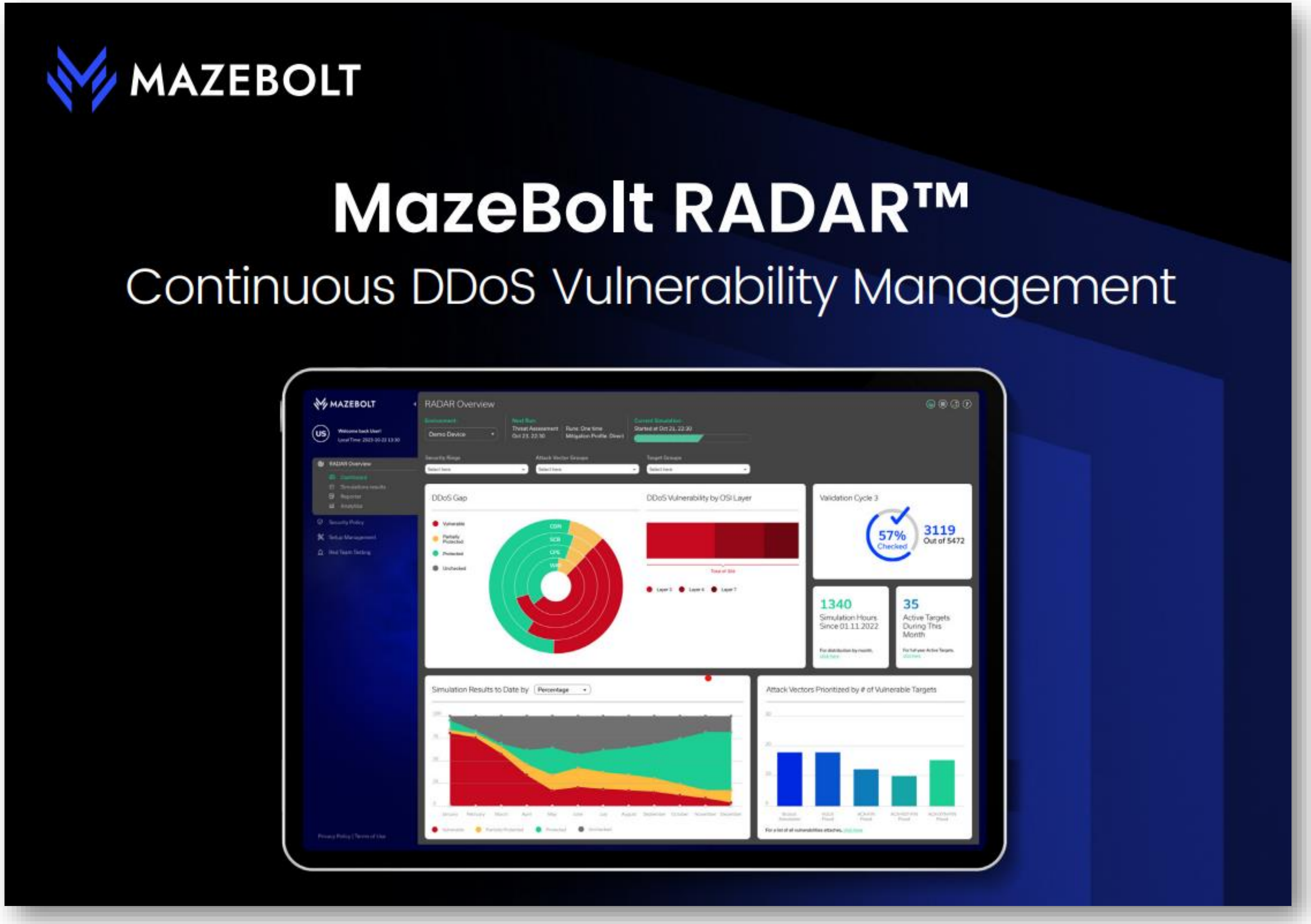
Kubernetes Ingress Controller/ Openshift Operator

WAF

NGINX Plus
DYNAMIC APPLICATION SERVICES

NGINX Unit
DYNAMIC APPLICATION INFRASTRUCTURE

NGINX



MAZEBOLT

MazeBolt RADAR™

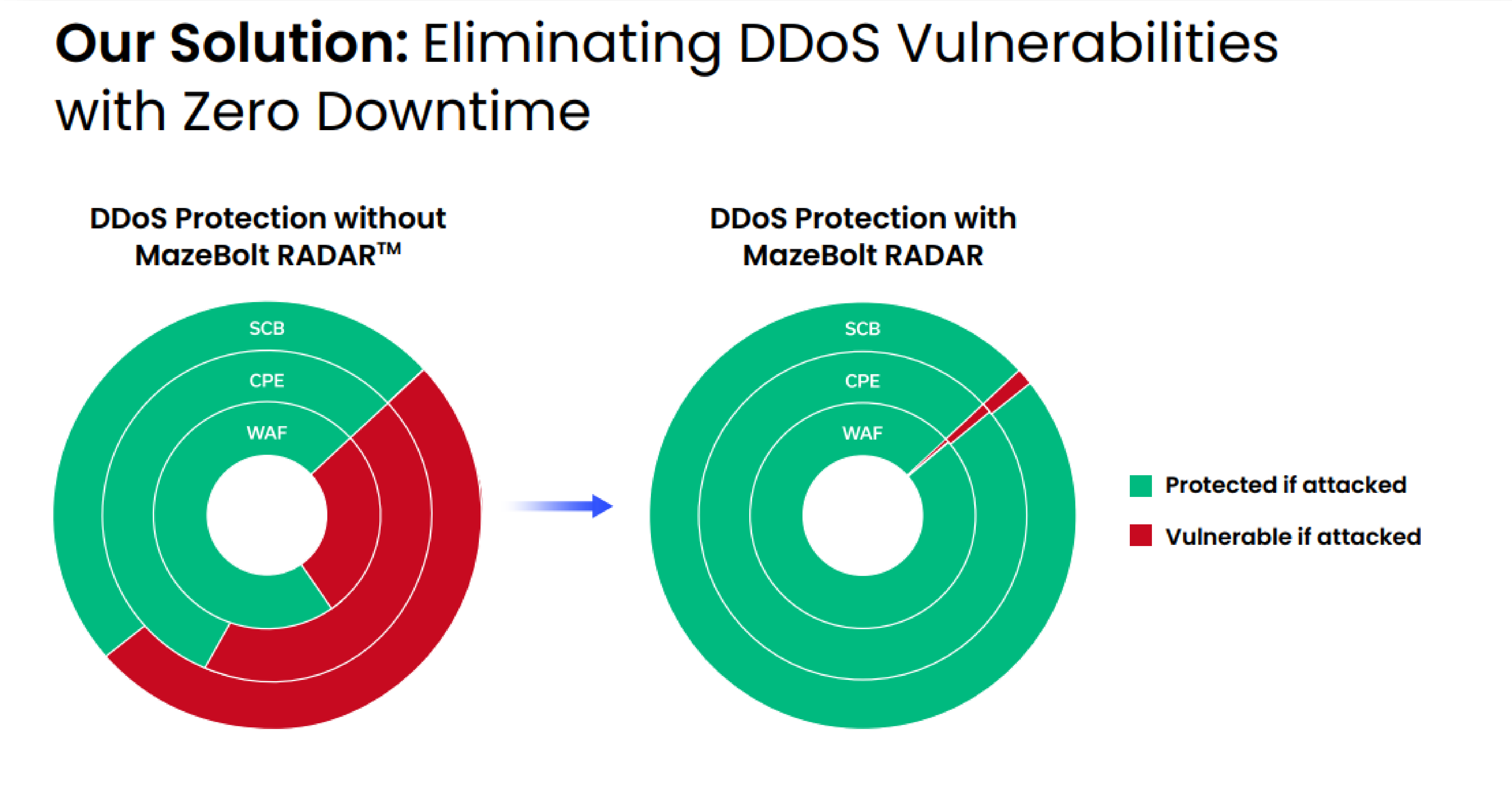
Continuous DDoS Vulnerability Management

RADAR Overview
DDoS Gap
DDoS Vulnerability by OSI Layer
Validation Cycle 3
57% Checked
3119 Out of 5472
1340 Simulation Hours Since 01.11.2022
35 Active Targets During This Month
Simulation Results to Date by
Attack Vectors Prioritized by # of Vulnerable Targets

KEY BENEFITS:

Understanding Your Return on Investment

- Continuous vulnerability identification & remediation
- Extensive reporting for DORA and SEC compliance requirements
- Avoid financial loss and regulatory scrutiny
- Ensures business continuity
- Full attack surface coverage
- Data-driven risk management
- Zero false positives



Our Solution: Eliminating DDoS Vulnerabilities with Zero Downtime

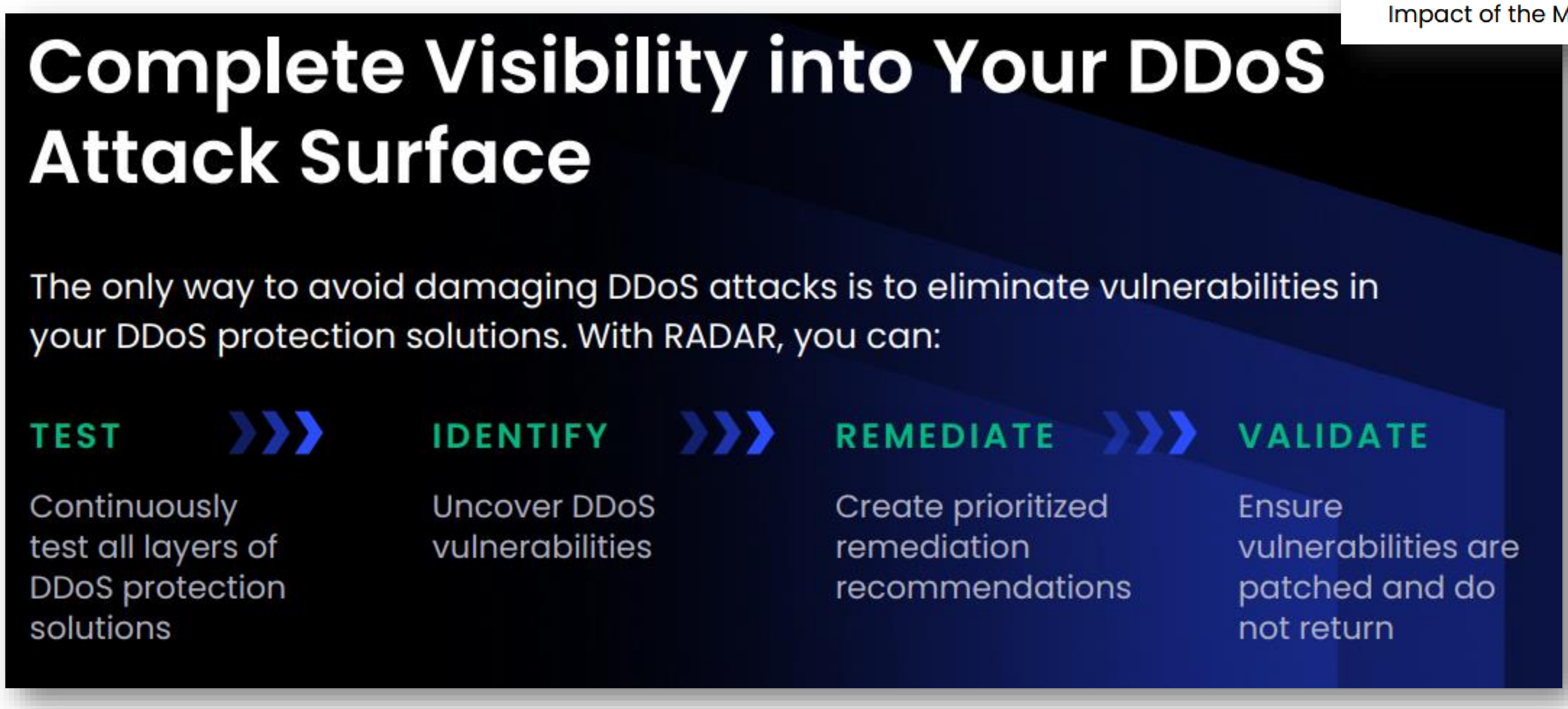
DDoS Protection without MazeBolt RADAR™

DDoS Protection with MazeBolt RADAR

🟩 **Protected if attacked**

🟥 **Vulnerable if attacked**

Impact of the MazeBolt RADAR™ DDoS Vulnerability Management on the Customer's DDoS Protection



Complete Visibility into Your DDoS Attack Surface

The only way to avoid damaging DDoS attacks is to eliminate vulnerabilities in your DDoS protection solutions. With RADAR, you can:

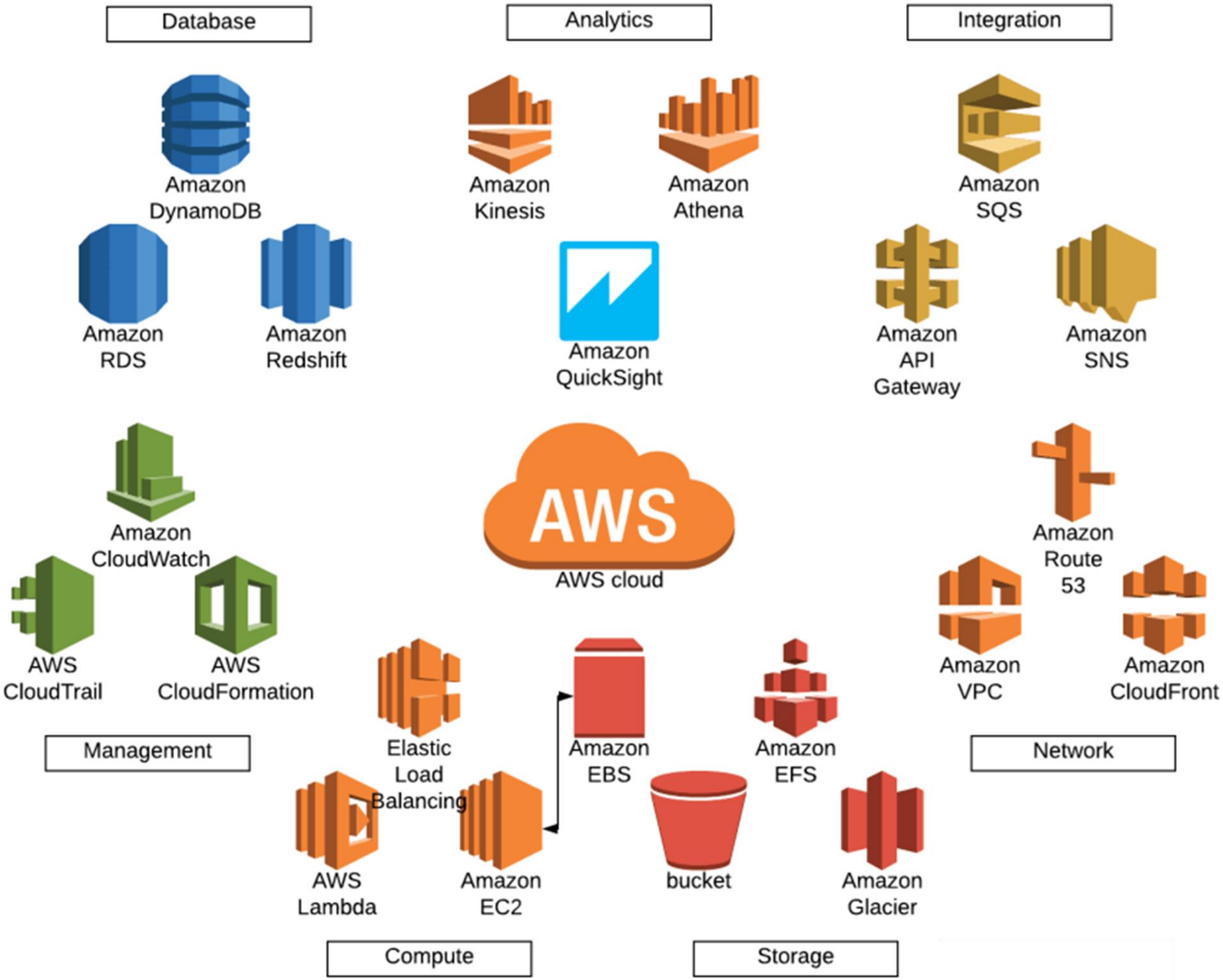
TEST ❯❯❯ **IDENTIFY** ❯❯❯ **REMEDIATE** ❯❯❯ **VALIDATE**

TEST
Continuously test all layers of DDoS protection solutions

IDENTIFY
Uncover DDoS vulnerabilities

REMEDIATE
Create prioritized remediation recommendations

VALIDATE
Ensure vulnerabilities are patched and do not return



Database

Amazon DynamoDB

Amazon RDS

Amazon Redshift

Analytics

Amazon Kinesis

Amazon Athena

Amazon QuickSight

Integration

Amazon SQS

Amazon API Gateway

Amazon SNS

AWS

AWS cloud

Amazon CloudWatch

AWS CloudTrail

AWS CloudFormation

Management

Amazon Route 53

Amazon VPC

Amazon CloudFront

Network

Elastic Load Balancing

AWS Lambda

Amazon EC2

Compute

Amazon EBS

Amazon EFS

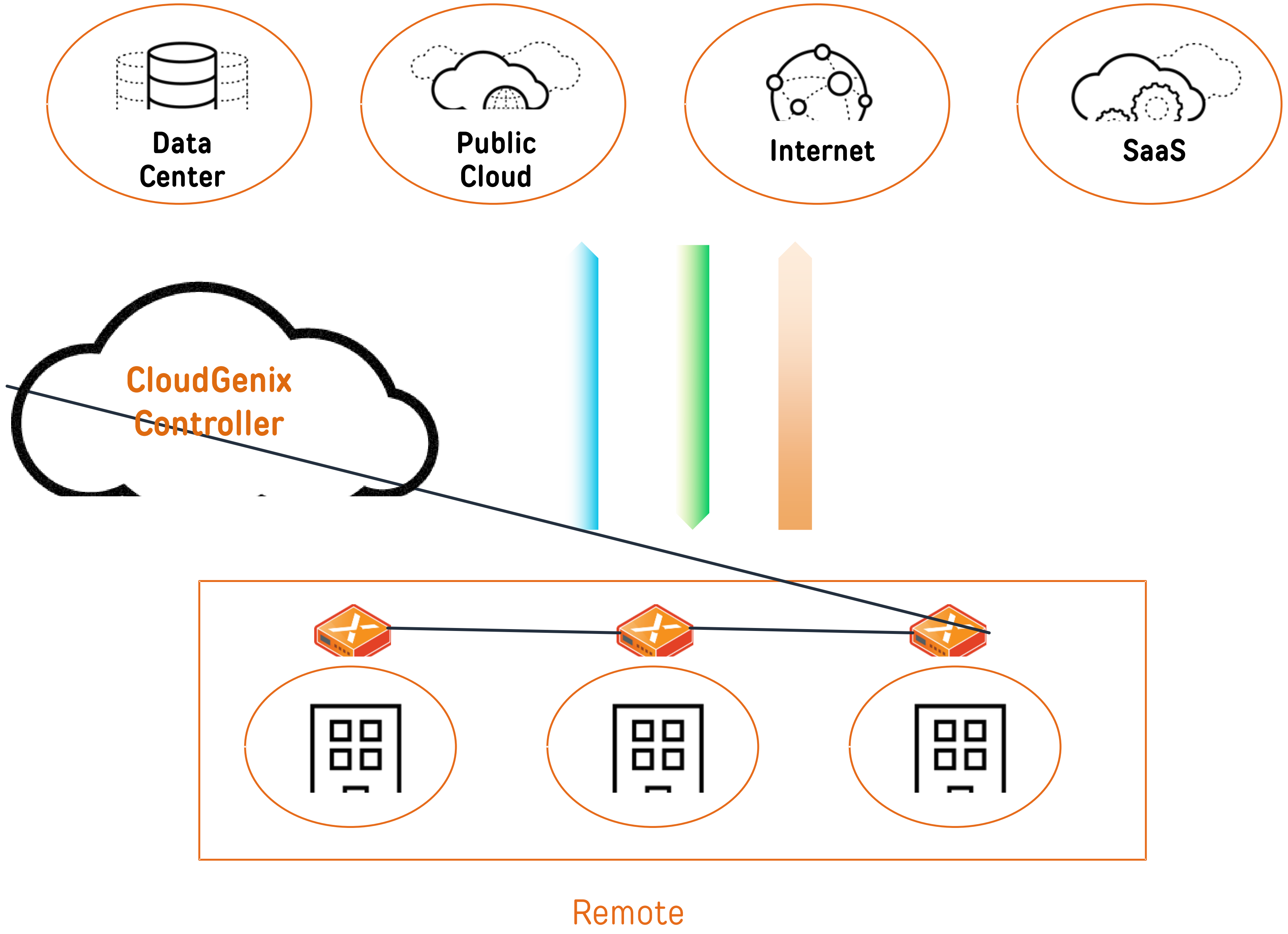
bucket

Amazon Glacier

Storage

Firewalls

SD-WAN - Industry’s 1st Next-Generation SD-WAN



- Deploy Cloud APPs **without** upgrading MPLS , Improve APPs Performance
- Increase branch office **Availability & Capacity** via broadband internet
- Add Internet to branches while **maintain consistent** security perimeter
- **Simplify** networking - Reduce branch HW, support and WAN costs

paloalto NETWORKS CLOUDGENIX

paloalto NETWORKS

Secure Access Service Edge (SASE)

Microsoft Azure AD

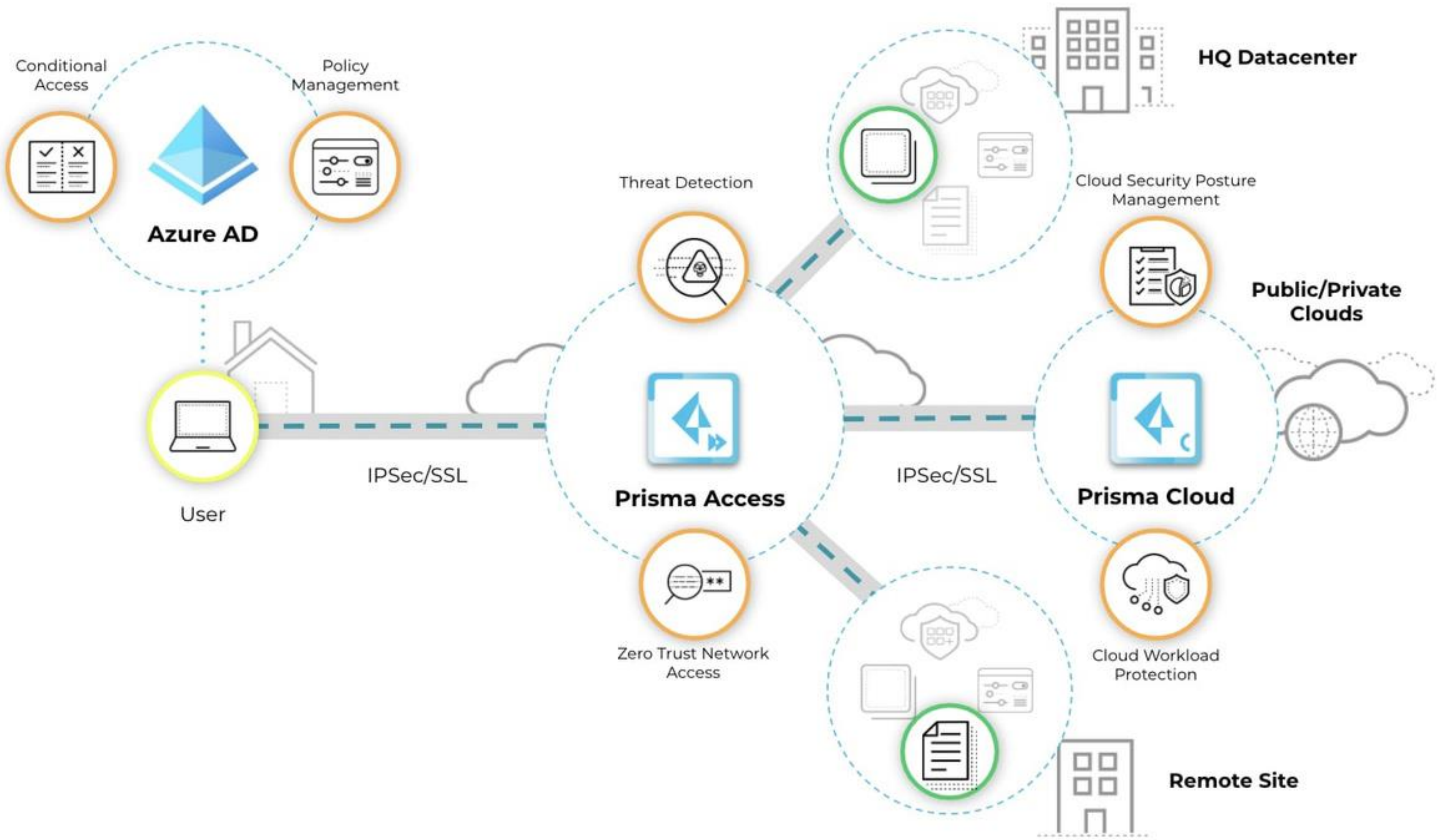
Cloud IAM
on-premises applications
SaaS applications

Prisma Access

NW + Security as a Service
Zero-touch provisioning
VPN Killer: No DC backhauling
Zero Trust Architecture + NGFW
Unmanned mobile Users
Dynamic BW allocation
SLAs: O365, Google G Suite, Slack

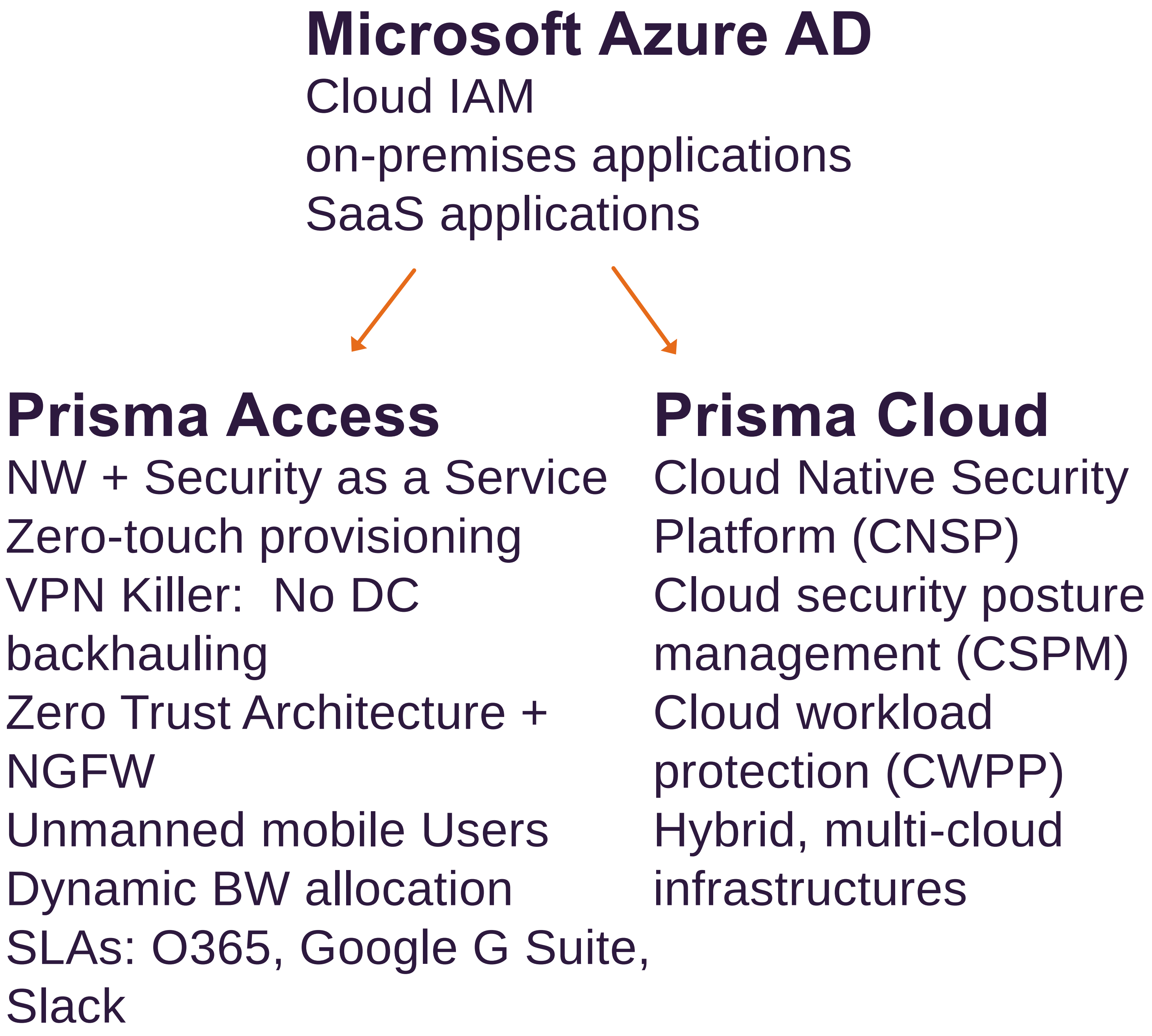
Prisma Cloud

Cloud Native Security Platform (CNSP)
Cloud security posture management (CSPM)
Cloud workload protection (CWPP)
Hybrid, multi-cloud infrastructures



Secure mobile users across hybrid environments

Secure Access Service Edge (SASE)



Microsoft Azure AD
Cloud IAM
on-premises applications
SaaS applications

Prisma Access
NW + Security as a Service
Zero-touch provisioning
VPN Killer: No DC backhauling
Zero Trust Architecture + NGFW
Unmanned mobile Users
Dynamic BW allocation
SLAs: O365, Google G Suite, Slack

Prisma Cloud
Cloud Native Security Platform (CNSP)
Cloud security posture management (CSPM)
Cloud workload protection (CWPP)
Hybrid, multi-cloud infrastructures

NIS2 Directive

- **A plan for handling** security incidents
- **Cybersecurity training** and a practice for basic computer hygiene.
- **A plan for managing** business operations during and after a security incident.

Cortex XDR™

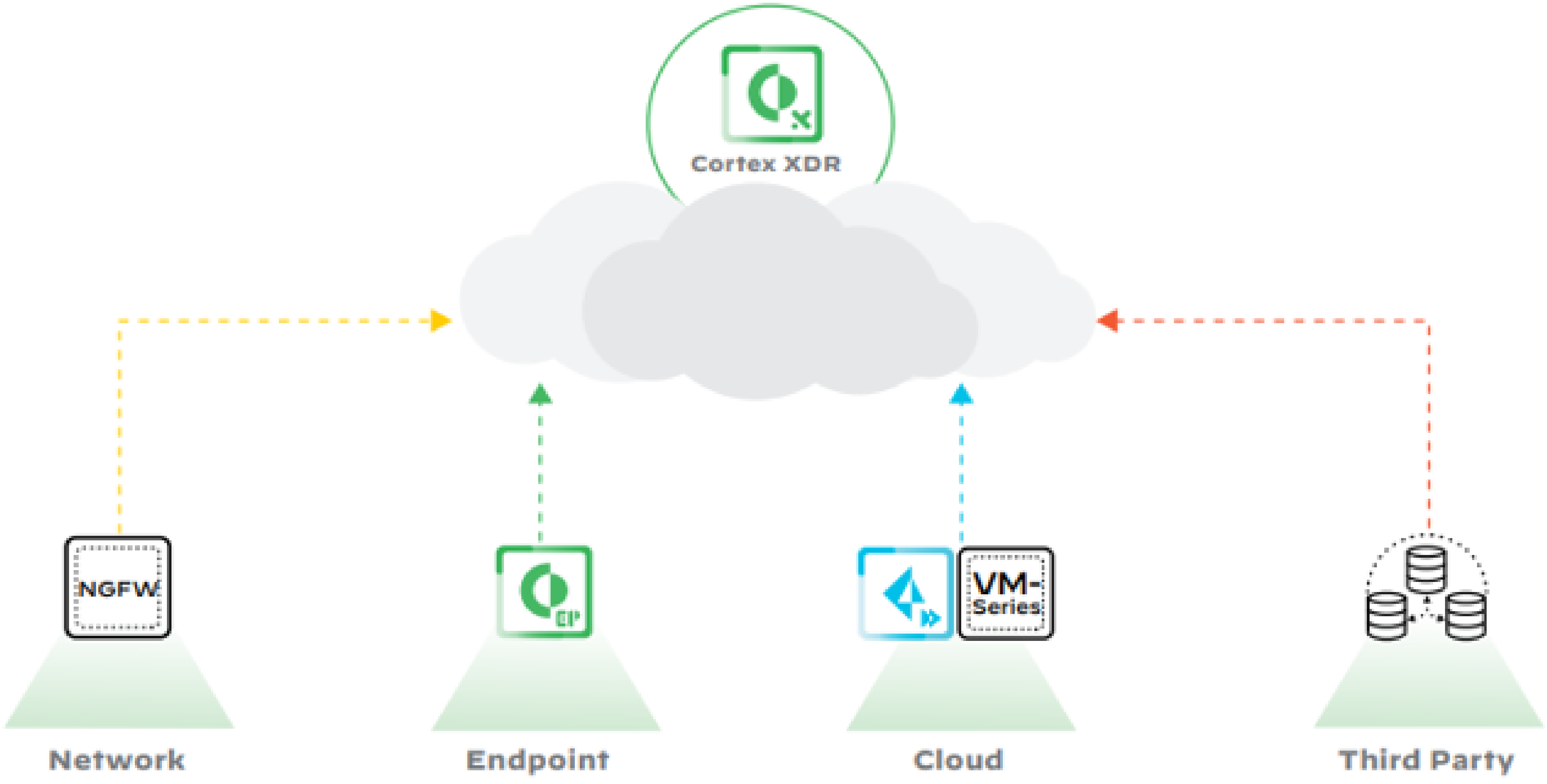
NIS2 Directive

- Risk Assessment

Endpoint Security

*Unified experience for **Prevention, Detection, Investigation, and Response***

- Cloud SIEM
- DATA LAKE
- Forensics
- Incident Response
- Cloud & NTA & ID
- 3rd Party Data Engine
- Host Insights
- Anti-Ransomware
- Behavioral Analysis
- Exploit Isolation
- 0-day protection
- Asset Management
- Compliancy



Network data

- + Palo Alto Networks NGFW
- + Cisco ASA and FirePower
- + Check Point Firewall
- + Fortinet Fortigate

Endpoint data

- + Cortex XDR agent
- + Windows event logs
- + Pathfinder data collector
- + GlobalProtect™ events from NGFW logs

Cloud and identity data

- + Cortex XDR for VM and containers
- + Prisma™ Access
- + VM-Series NGFW
- + Azure Active Directory
- + Okta
- + PingOne
- + Google Cloud Platform logs

AV comparatives Certified EPR 2020 Strategic Leader

AV-Comparatives named Cortex XDR a Strategic Leader in the 2020 Endpoint Protection and Response Test

FORRESTER WAVE LEADER 2021 Endpoint Security Software As A Service

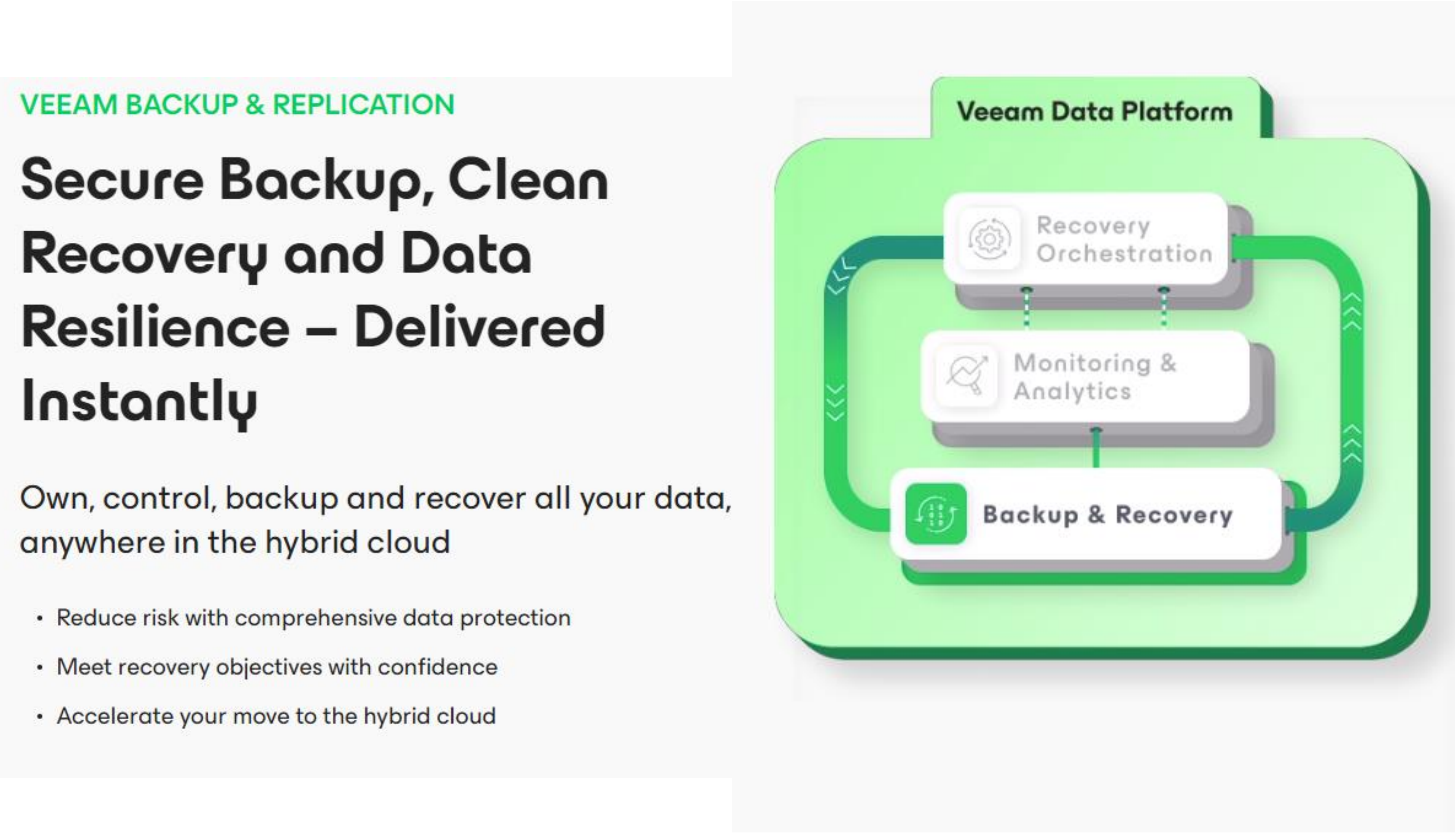
Cortex XDR was named a Leader in the 2021 Forrester Wave: Endpoint Security Software As A Service

MITRE ATT&CK®

Cortex XDR delivers the best combined protection and detection scores, with 100% threat prevention and 97% visibility in the MITRE ATT&CK Round 3 test.

paloalto NETWORKS

✱ Recover - Back up & Restore



VEEAM BACKUP & REPLICATION

Secure Backup, Clean Recovery and Data Resilience – Delivered Instantly

Own, control, backup and recover all your data, anywhere in the hybrid cloud

- Reduce risk with comprehensive data protection
- Meet recovery objectives with confidence
- Accelerate your move to the hybrid cloud

NIS2 Directive

A plan for managing business operations during and after a security incident.

Respond – SOC Services

Managed Security

- Managed Firewall
- Managed Endpoint Protection (EPP)
- Managed Email Gateway
- Managed Data Security
- Digital Risk & Threat Monitoring

Detect and Respond

- Managed Detection & Response (MDR)
- Managed Extended Detection & Response (XDR)
- Managed Network Detection & Response (MNDR)
- Managed Endpoint Detection & Response (EDR)
- Managed Azure Sentinel
- Digital Forensics & Incident Response (DFIR)

Cyber Risk Management

- Penetration Testing
- Vulnerability Management
- CISO as a Service
- Security Controls Assessment

SecurityHQ

WHY SECURITY HQ?

MANAGED SECURITY SERVICES

SOC Team

+300
Certified Security Analysts

6
Data Centers

SLA

20
Years of Experience

Staff Certifications

- PCNSE
- CCIE
- IBM
- JNCIS, JNCIP
- FCNSP
- AWS, Azure Security
- ECIH

- GPEN
- GWPAT
- GCIH
- CISSP

- CCSE, CCSM
- OSCP

*Unique Service Delivery Model

pylones*

Service Delivery Management

- Dedicated SDM
- Dedicated Technical Lead
- Service Assurance Lead

Support 24*7

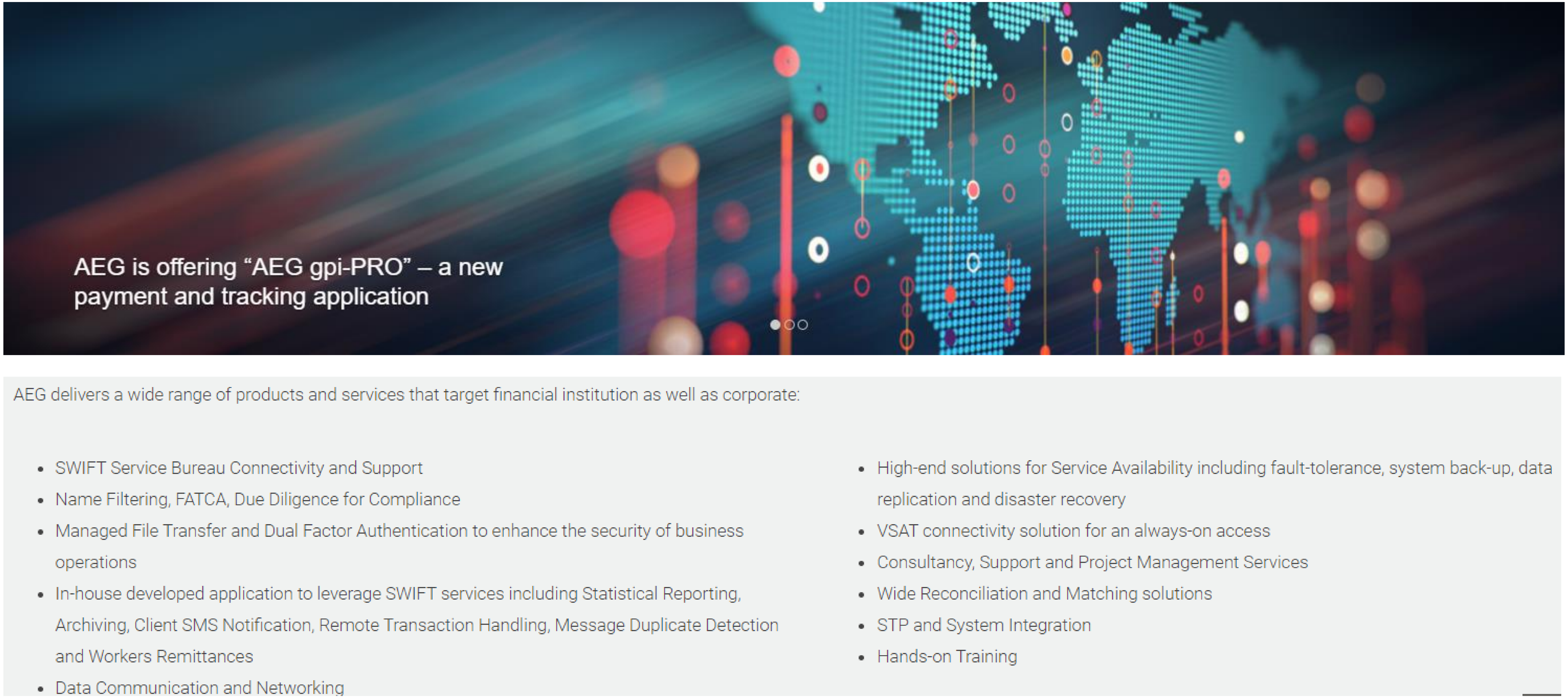
Conduct weekly meetings with the customer

Manage escalations (bi directionally. From SOC to Customer and vice versa)

Ensure all deliverables are met, to quality and on time

Ensure the customer is stratified with the service levels

Coordinate with the customer team and provide coordination between the SOC team and the Customer Security and IT teams.

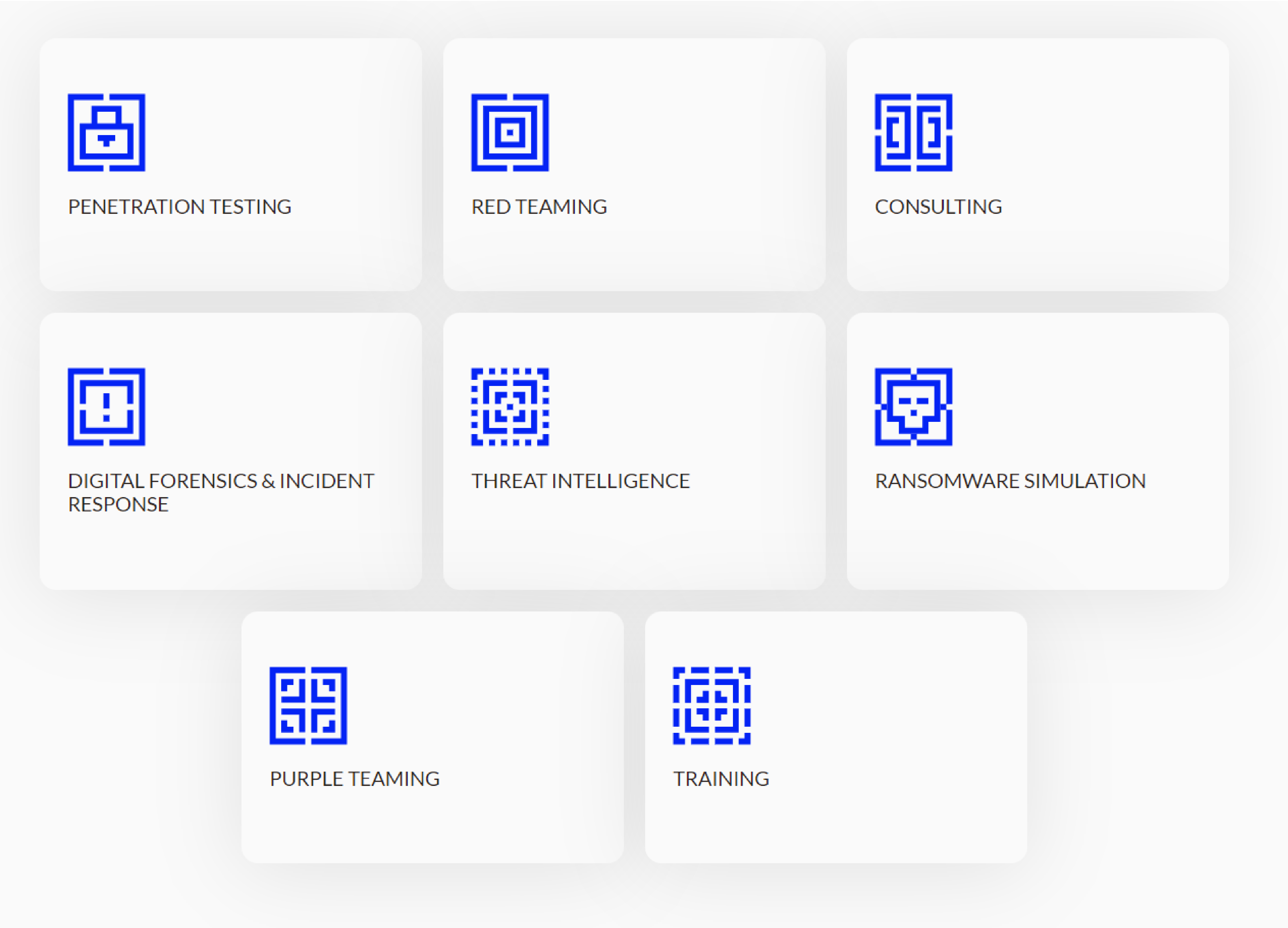


AEG is offering “AEG gpi-PRO” – a new payment and tracking application

AEG delivers a wide range of products and services that target financial institution as well as corporate:

- SWIFT Service Bureau Connectivity and Support
- Name Filtering, FATCA, Due Diligence for Compliance
- Managed File Transfer and Dual Factor Authentication to enhance the security of business operations
- In-house developed application to leverage SWIFT services including Statistical Reporting, Archiving, Client SMS Notification, Remote Transaction Handling, Message Duplicate Detection and Workers Remittances
- Data Communication and Networking
- High-end solutions for Service Availability including fault-tolerance, system back-up, data replication and disaster recovery
- VSAT connectivity solution for an always-on access
- Consultancy, Support and Project Management Services
- Wide Reconciliation and Matching solutions
- STP and System Integration
- Hands-on Training

Advanced Cybersecurity



PENETRATION TESTING

RED TEAMING

CONSULTING

DIGITAL FORENSICS & INCIDENT RESPONSE

THREAT INTELLIGENCE

RANSOMWARE SIMULATION

PURPLE TEAMING

TRAINING

threatscene

pylones*

✱ CYBERSECURITY REVOLUTION

Dive into NIS2

Download the *“Dive into NIS2”* e-Book by Pylones Hellas.

Thank you