Akamai

WORLD INFORMATION TECHNOLOGY

Security Solution Trends


USERS
INTERNET
WEB APPLICATION
API
API IN MOBILE APP
AI CHATBOT
DATA


ORGANIZATION
DATA THEFT
Unauthorized access and data exfiltration
MALICIOUS ACTOR
External threat with malicious intent
REVENUE IMPACT
Financial loss and decreased income
LOSS OF TRUST
Reduced customer confidence and trust
LEGAL DISPUTES
Lawsuits and regulatory penalties
PUBLIC EXPOSURE
Incident becomes publicly known
REPUTATIONAL DAMAGE
Long-term damage to brand reputation

EDGE PROTECTS WHAT MATTERS

Secure Every Connection. Protect Every Experience.

USERS

- Mobile Users
- Web Users
- Employees
- Partners
- IoT / Devices

ATTACKERS

- Hackers
- Malicious Bots
- DDoS / Abuse
- Account Takeover
- Data Exfiltration

INTERNET

EDGE PROTECTION

CDN & ACCELERATION
Deliver fast, available and reliable experiences

DDoS PROTECTION
Absorb and mitigate large-scale attacks

WAF
Block exploits and protect web applications

BOT DETECTION
Detect and stop automated malicious bots

API SECURITY
Discover, secure and protect APIs

FIREWALL FOR AI
Protect AI applications and models from abuse

PROTECTED RESOURCES

WEBSITE
Corporate sites, portals, e-commerce

API
REST / GraphQL APIs, microservices

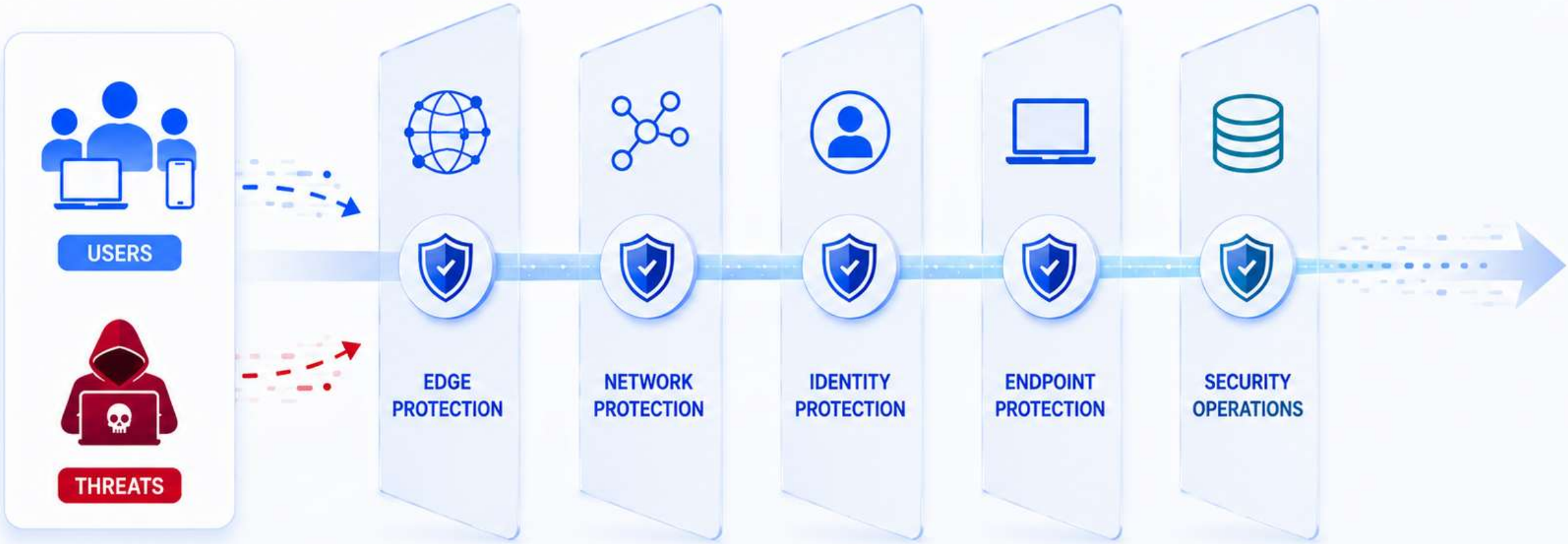
AI CHATBOT
AI assistants, conversational agents

Edge is the first line of defense on the Internet

✓ Protect ✓ Accelerate ✓ Ensure Availability ✓ Deliver Trusted Experiences

CYBER SECURITY PROTECTION LAYERS

Defense in Depth Across the Entire Digital Journey



Every Layer Works Together. Every Layer Protects What Matters.

Prevent | Detect | Respond | Recover

EDGE PROTECTS WHAT MATTERS

Secure Every Connection. Protect Every Experience.

USERS

- Mobile Users
- Web Users
- Employees
- Partners
- IoT / Devices

ATTACKERS

- Hackers
- Malicious Bots
- DDoS / Abuse
- Account Takeover
- Data Exfiltration

INTERNET

EDGE PROTECTION

CDN & ACCELERATION
Deliver fast, available and reliable experiences

DDoS PROTECTION
Absorb and mitigate large-scale attacks

WAF
Block exploits and protect web applications

BOT DETECTION
Detect and stop automated malicious bots

API SECURITY
Discover, secure and protect APIs

FIREWALL FOR AI
Protect AI applications and models from abuse

PROTECTED RESOURCES

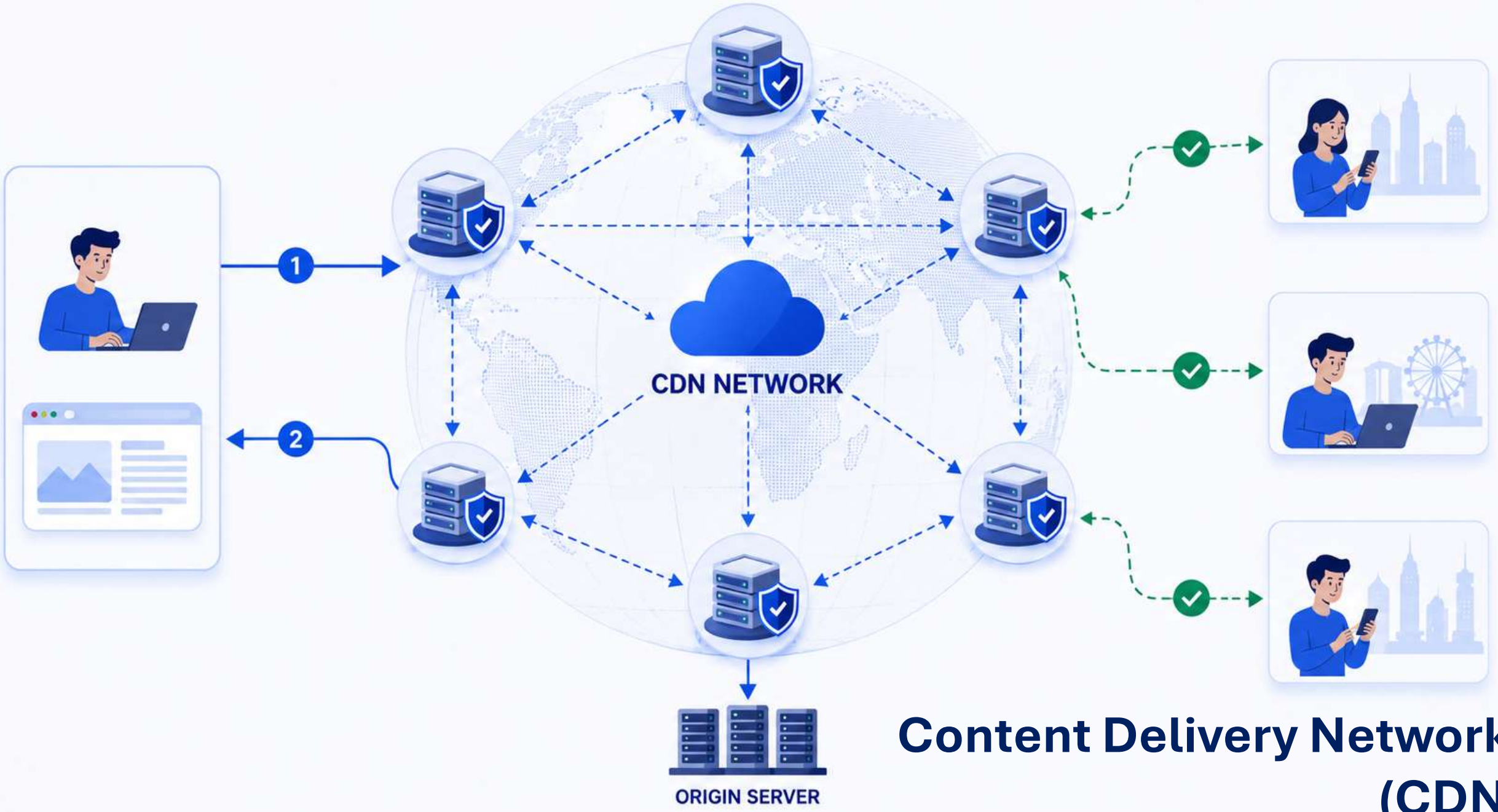
WEBSITE
Corporate sites, portals, e-commerce

API
REST / GraphQL APIs, microservices

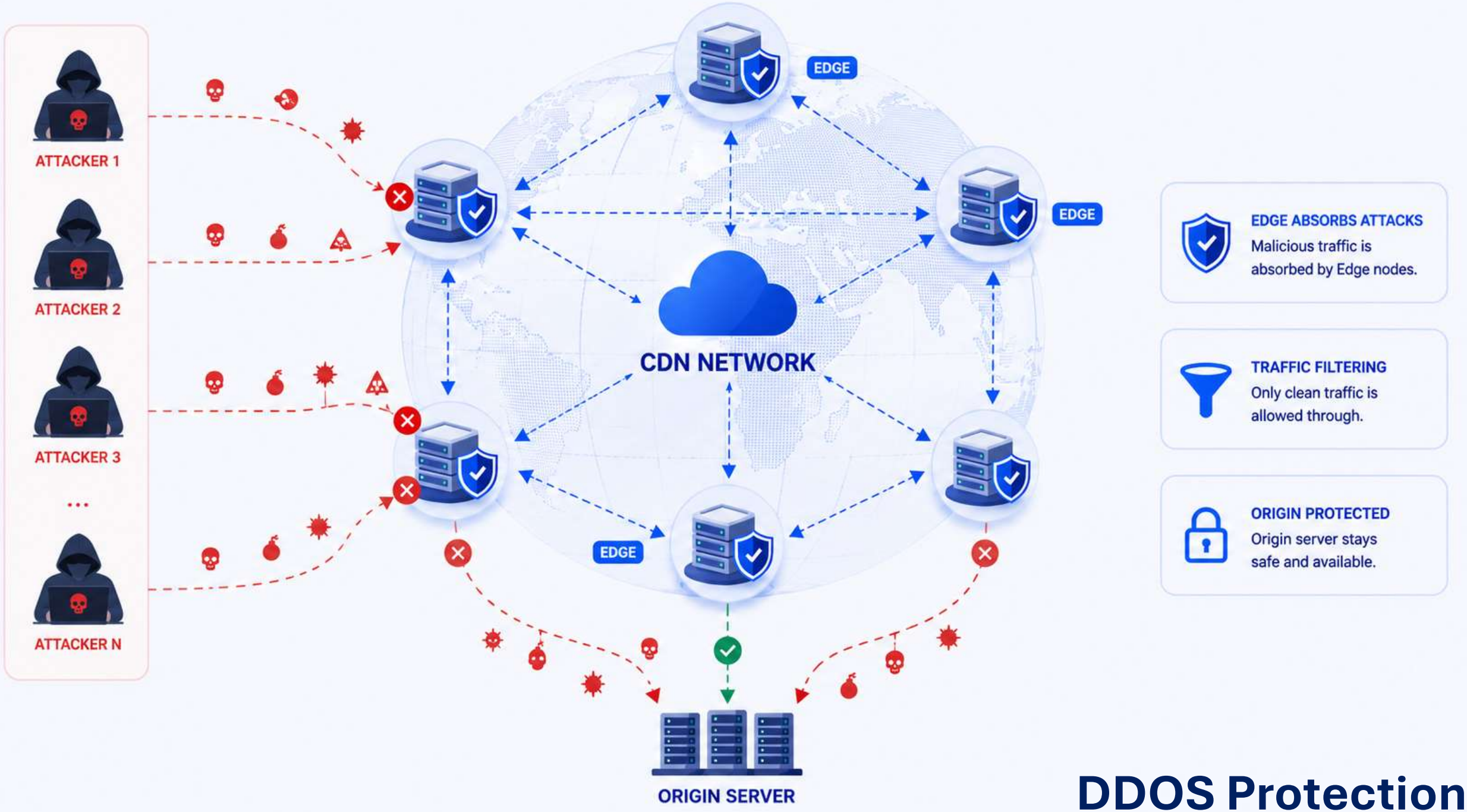
AI CHATBOT
AI assistants, conversational agents

Edge is the first line of defense on the Internet

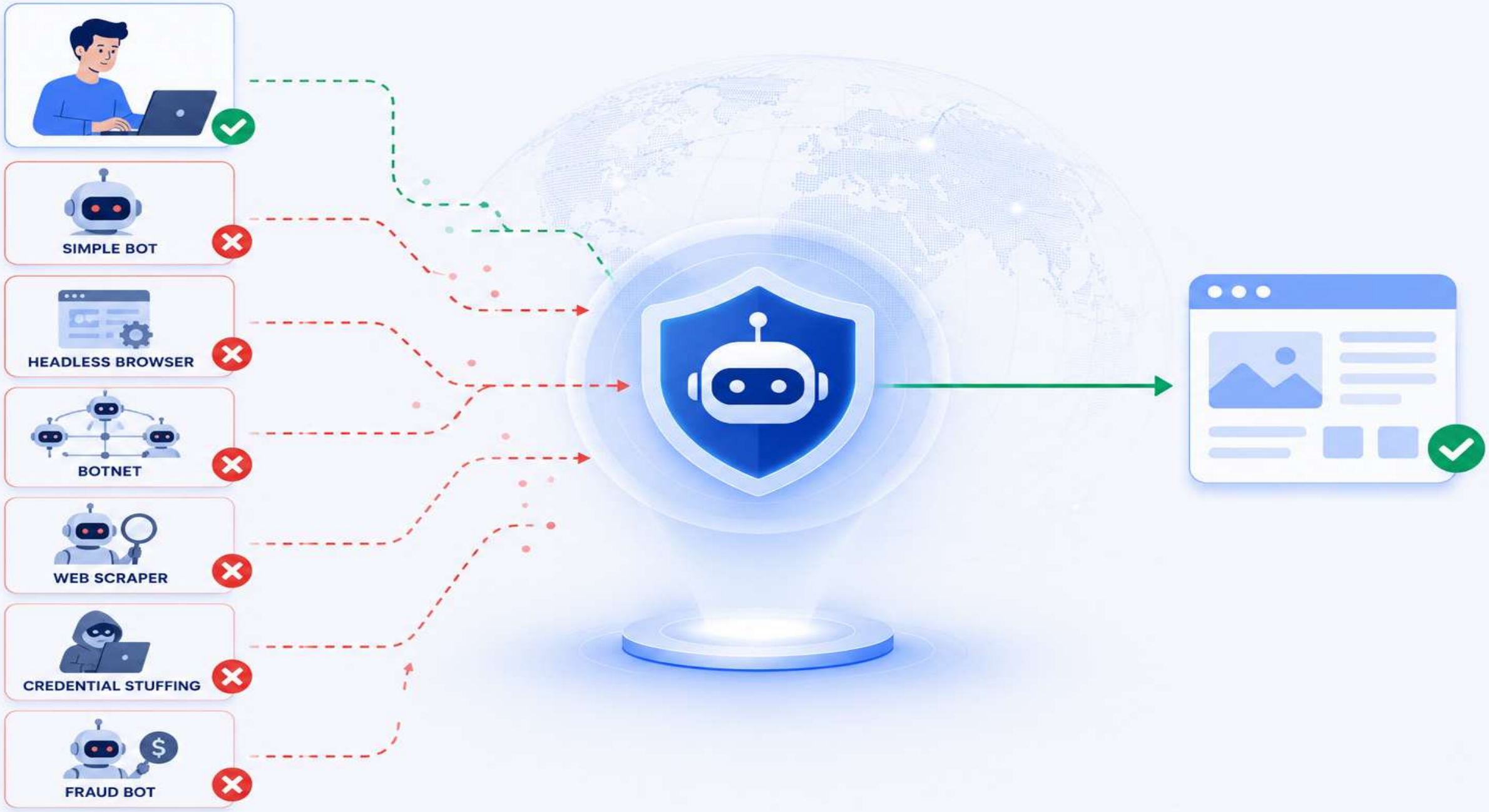
✓ Protect ✓ Accelerate ✓ Ensure Availability ✓ Deliver Trusted Experiences



Content Delivery Network (CDN)



DDOS Protection



BOT DETECTION

WAF

WEB APPLICATION FIREWALL

GOOD USER

ALLOW

ATTACKER

BLOCK

TRAFFIC FILTERING
Block malicious IP, geo, rate limit, anomalous traffic

THREAT DETECTION
Detect known & unknown attacks, signatures, behavior

RULES & POLICIES
OWASP, custom rules, allow/deny rules

LOG & MONITORING
Real-time monitoring, alerting, audit logs

OWASP TOP 10 (2021)

A01	BROKEN ACCESS CONTROL	A06	VULNERABLE AND OUTDATED COMPONENTS
A02	CRYPTOGRAPHIC FAILURES	A07	IDENTIFICATION AND AUTHENTICATION FAILURES
A03	INJECTION	A08	SOFTWARE AND DATA INTEGRITY FAILURES
A04	INSECURE DESIGN	A09	SECURITY LOGGING AND MONITORING FAILURES*
A05	SECURITY MISCONFIGURATION	A10	SERVER-SIDE REQUEST FORGERY (SSRF)*

ALLOW

APPLICATION

WEB / API APPLICATION

DATABASE

THREAT INTELLIGENCE & CVE FEED

Continuous update of threats, vulnerabilities and attack patterns

Auto Update Rules & Signatures

CVE NEW RELEASE

CRITICAL	CVE-2024-3094	Apache Struts RCE Vulnerability	Published: May 21, 2024
HIGH	CVE-2024-24786	PHP CGI Argument Injection	Published: May 15, 2024
MEDIUM	CVE-2024-2361	Next.js Authorization Bypass	Published: May 10, 2024

...

API Security

API

(Application Programming Interface)

A set of rules and protocols that allow systems to communicate with each other.

CLIENTS / APPLICATIONS

- Mobile App
- Web Application
- Cloud Services
- AI / ML Applications
- Partner Integrations

REQUEST
Ask for data or perform a function

RESPONSE
Return data or results

SYSTEMS / DATA

- Database
- Legacy Systems
- Cloud Services
- Third-Party Services
- Internal Services

STANDARDIZED • SECURE • RELIABLE

ENABLES INTEGRATION
Allows different systems and applications to work together seamlessly.

IMPROVES EFFICIENCY
Reduces development time by reusing existing functionalities.

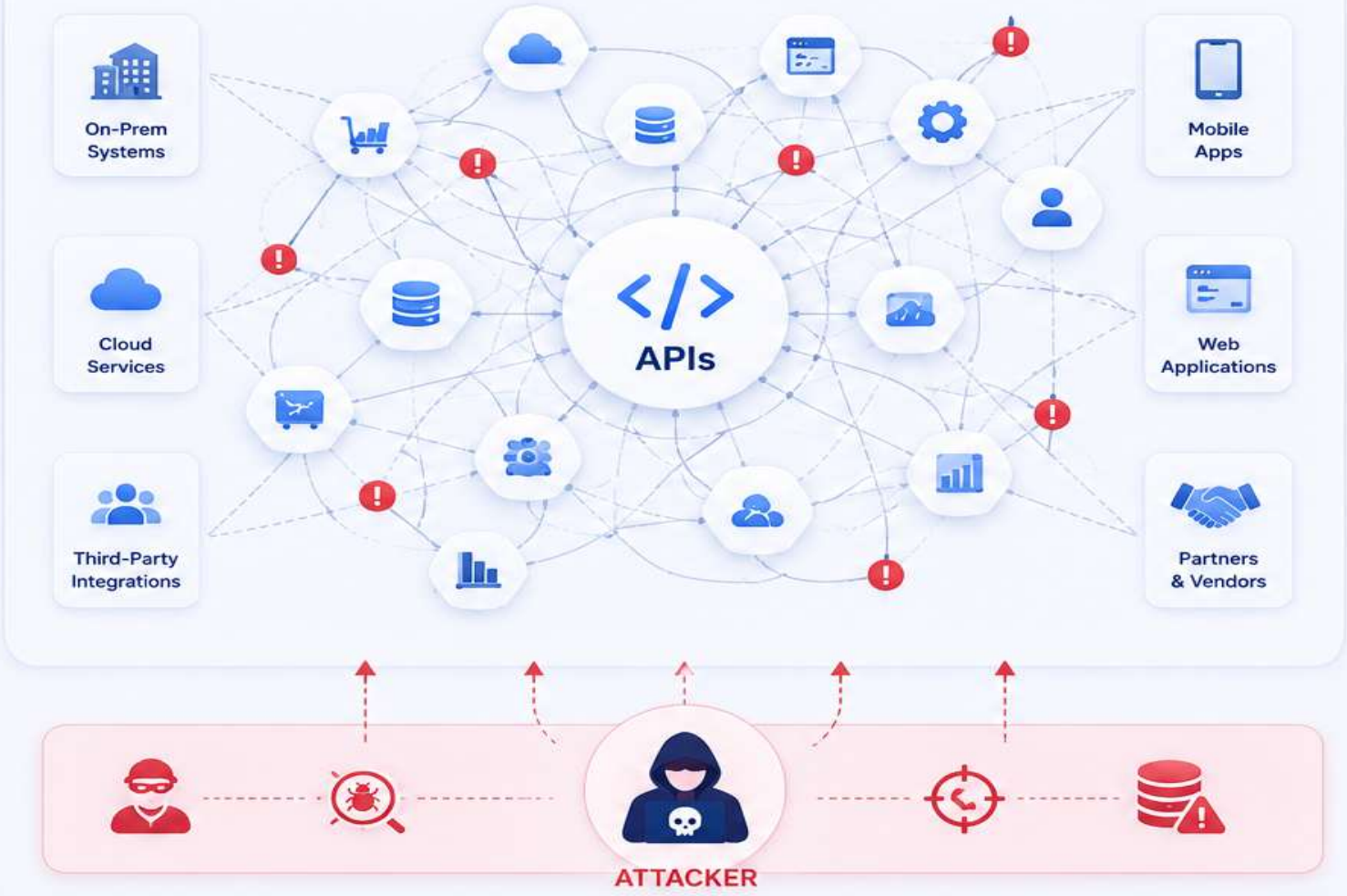
DRIVES INNOVATION
Enables new products, services, and experiences faster.

ENSURES CONTROL
Provides a secure and governed way to access data and services.

PROBLEM: API SPRAWL

API growth expands attack surface and makes security harder to control.

API SPRAWL IN MODERN ORGANIZATIONS



THE IMPACT

OF ORGANIZATIONS EXPERIENCED API SECURITY INCIDENTS

2026 REPORT

3.5 TIMES / YEAR

Average number of API security incidents per organization

2026 REPORT

700K+ USD

Average financial loss per organization

2026 REPORT

ตัวอย่างเหตุการณ์ การลักลอบใช้งาน API

เพราะ API เปิดให้เข้าถึงได้จากอินเทอร์เน็ต โดยไม่มีการยืนยันตัวตนและกำหนดสิทธิ์

ผู้ไม่หวังดี (ใช้ Reverse Engineering)

1. วิเคราะห์แอปพลิเคชัน
   ผู้ไม่หวังดีทำการติดตั้งและวิเคราะห์แอปพลิเคชัน
2. ทำ Reverse Engineering
   สกัดโค้ด ค้นหาการเชื่อมต่อและ Endpoint ของ API
3. ได้ API Endpoint
   ผู้ไม่หวังดีสามารถนำ API Endpoint ออกไปใช้งานได้

ได้ API ออกไปโดยไม่จำเป็นต้องมีสิทธิ์ใช้งานหรือได้รับอนุญาต

เข้าถึง API ได้ผ่านอินเทอร์เน็ต

API ที่เปิดให้เข้าถึง

- ไม่มีการยืนยันตัวตน (Authentication)
- ไม่มีการกำหนดสิทธิ์ (Authorization)

ใครก็สามารถเรียกใช้งาน API ได้โดยไม่ถูกควบคุม

ระบบและข้อมูลของบริษัท

API สามารถเข้าถึงข้อมูลและระบบได้โดยตรง ทำให้ผู้ไม่หวังดีสามารถดึงข้อมูลไปใช้ได้

ข้อมูลที่อาจถูกเข้าถึง

- ข้อมูลลูกค้า
- ข้อมูลธุรกิจ
- ข้อมูลการเงิน
- ข้อมูลสำคัญอื่นๆ

ผลกระทบที่เกิดขึ้น

- ข้อมูลรั่วไหล
- เสียหายต่อชื่อเสียงและความน่าเชื่อถือ
- สูญเสียรายได้และโอกาสทางธุรกิจ
- อาจถูกดำเนินคดีและฟ้องร้อง

ORGANIZATIONS DON'T KNOW ALL THEIR APIS

The Hidden API Problem

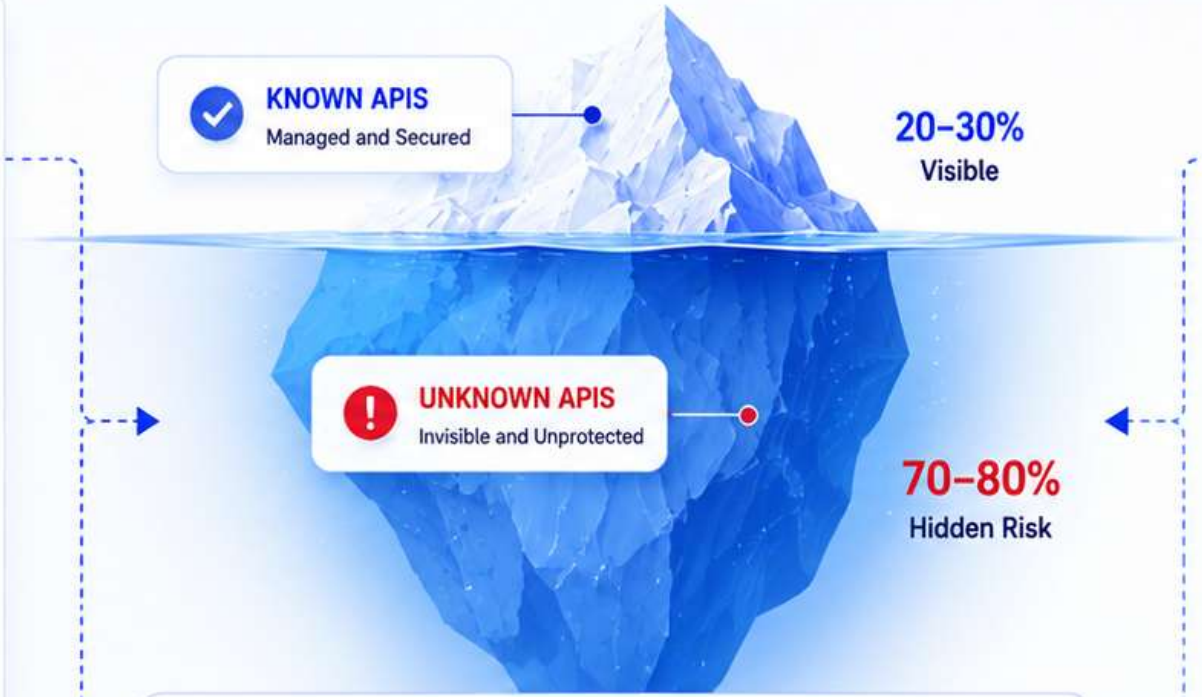
API CREATION HAPPENS EVERYWHERE

Development Teams
Building and deploying APIs rapidly

Cloud & Microservices
APIs across multi-cloud and containers

Partners & Vendors
Third-party integrations and external APIs

SaaS & Business Tools
APIs from SaaS and business applications



They Exist. They're Accessible. They're Unprotected.

THE IMPACT

No Visibility
Cannot see what you don't know

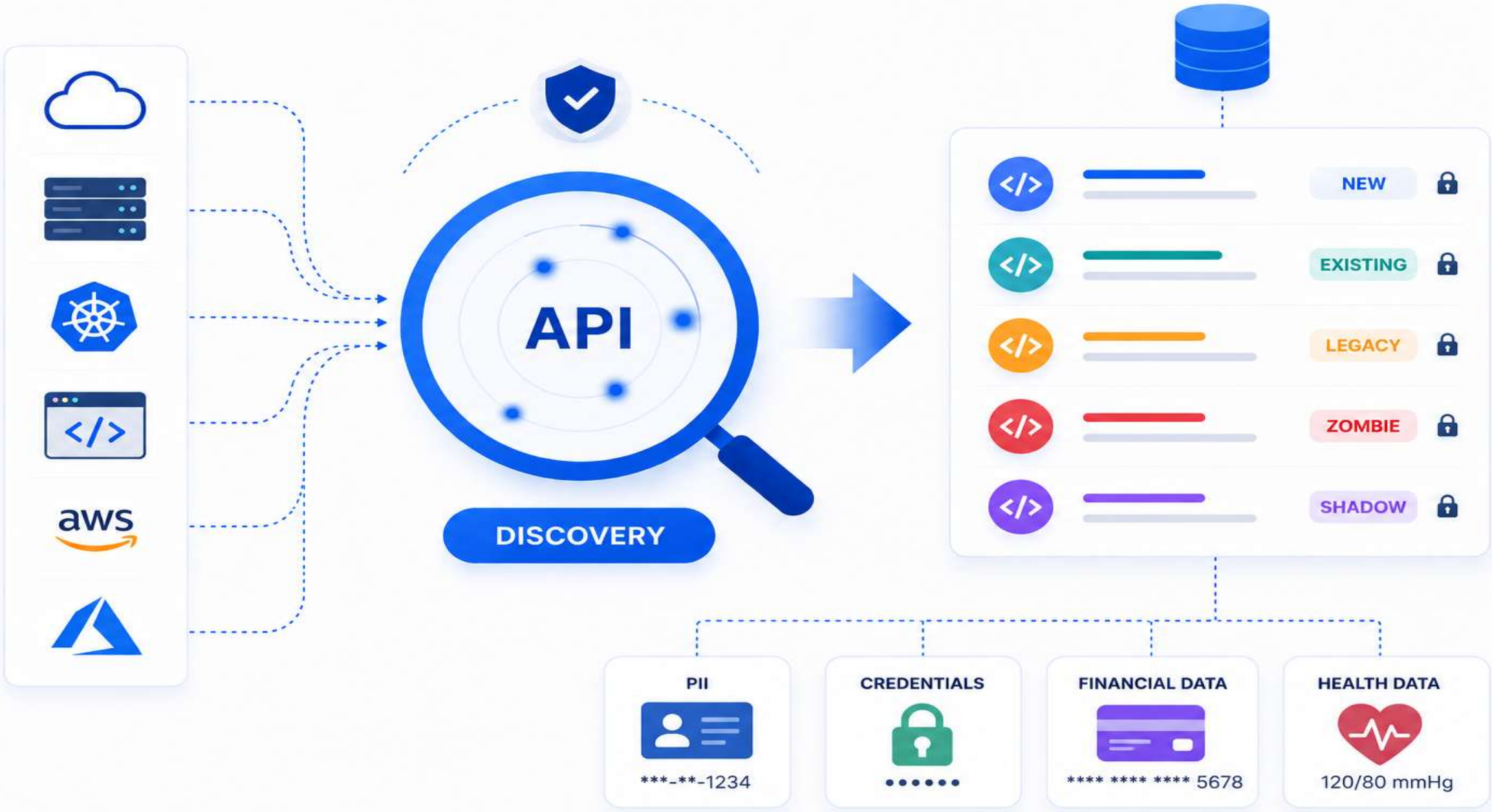
Higher Risk
Unknown APIs become easy attack targets

Data Exposure
Sensitive data may be exposed through APIs

Attack Surface Grows
More APIs = More ways for attackers to get in

Compliance & Audit Risk
Lack of control leads to compliance failures

You Can't Protect What You Can't See | Discover. Inventory. Classify. Protect Every API.


aws
API
DISCOVERY
NEW
EXISTING
LEGACY
ZOMBIE
SHADOW
PII
***-**-1234
CREDENTIALS
FINANCIAL DATA
**** **** **** 5678
HEALTH DATA
120/80 mmHg

API SECURITY ASSESSMENT

ตรวจหาช่องโหว่และความเสี่ยงของ API

DISCOVERED APIs

- GET /users GET
- POST /login POST
- GET /orders GET
- PUT /payments PUT
- GET /admin/report GET
- ...

AUTHENTICATION TESTING

ตรวจสอบการยืนยันตัวตน
และการจัดการโทเค็น

INPUT VALIDATION TESTING

ตรวจสอบการตรวจสอบ
ข้อมูลนำเข้าของ API

BUSINESS LOGIC TESTING

ตรวจสอบตรรกะทางธุรกิจ
และการควบคุมการใช้งาน

AUTHORIZATION TESTING

ตรวจสอบการกำหนดสิทธิ์
และการเข้าถึงข้อมูล

DATA EXPOSURE TESTING

ตรวจสอบการเปิดเผยข้อมูล
ที่อ่อนไหวโดยไม่จำเป็น

CONFIGURATION TESTING

ตรวจสอบการตั้งค่า
และส่วนประกอบที่ไม่ปลอดภัย

RISK & VULNERABILITY FINDINGS

- **Broken Authentication** — CRITICAL
  ไม่พบการยืนยันตัวตน (Authentication)
- **Broken Authorization** — HIGH
  ไม่มีการกำหนดสิทธิ์ (Authorization)
- **Sensitive Data Exposure** — HIGH
  พบการเปิดเผยข้อมูลอ่อนไหว
- **Injection** — MEDIUM
  พบช่องโหว่จากการป้อนข้อมูล
- **Excessive Data Exposure** — MEDIUM
  มีข้อมูลที่ส่งกลับมากเกินความจำเป็น
- **Security Misconfiguration** — LOW
  การตั้งค่าที่ไม่ปลอดภัย

RISK SUMMARY

24 Total Issues

CRITICAL	HIGH	MEDIUM	LOW
3	7	9	5

RECOMMENDED ACTIONS

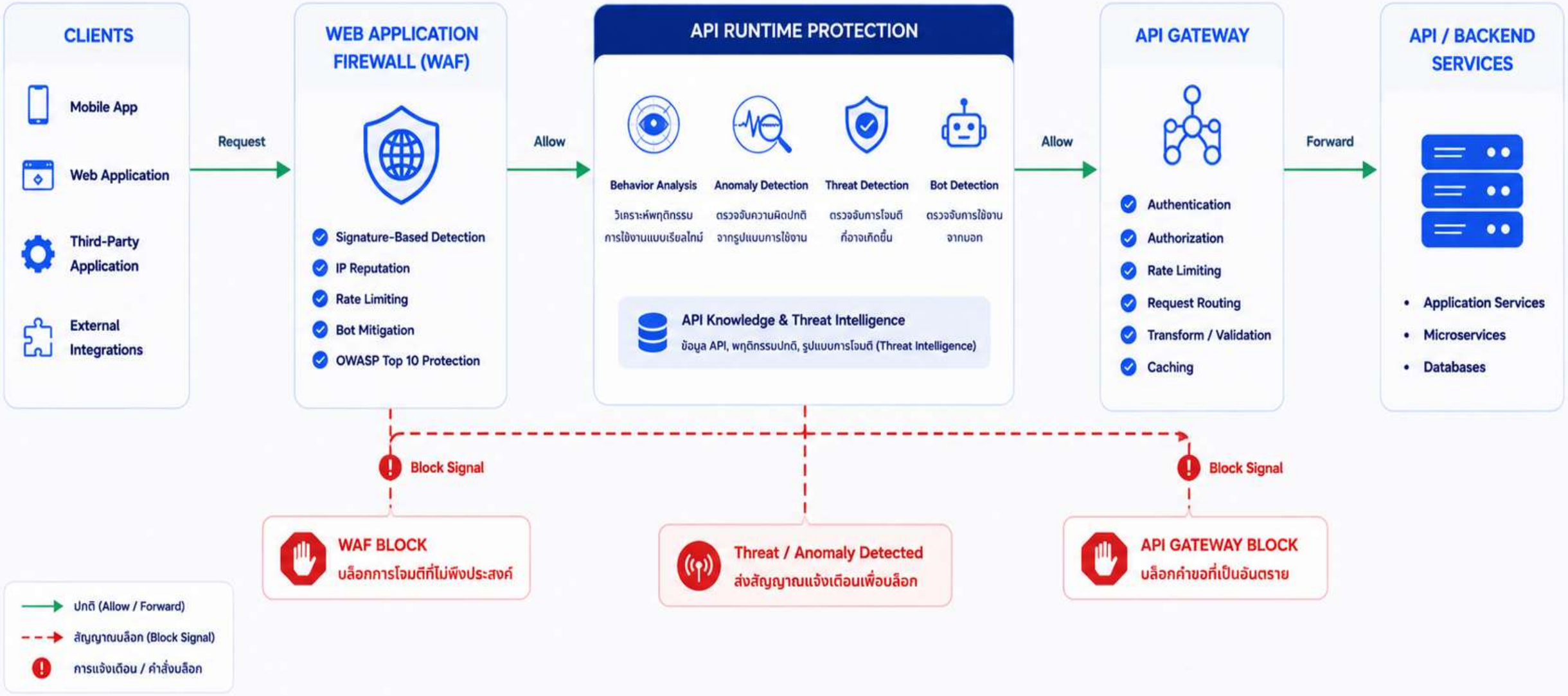
- เพิ่มการยืนยันตัวตน (Authentication) สำหรับทุก API
- กำหนดสิทธิ์การเข้าถึง (Authorization) ตามบทบาท
- จำกัดข้อมูลที่ส่งกลับ และปกปิดข้อมูลอ่อนไหว
- ปรับปรุงการตรวจสอบข้อมูลนำเข้า (Input Validation)

SECURE APIs

จัดการความเสี่ยงและป้องกัน
การถูกโจมตีได้อย่างมีประสิทธิภาพ

API RUNTIME PROTECTION

ตรวจจับและป้องกันการโจมตี หรือการใช้งานที่ผิดปกติแบบเรียลไทม์




PLAN
DESIGN
DEVELOP
TEST
STAGE
PRODUCTION
SHIFT-LEFT SECURITY
ACTIVE TESTING
SECURE APIS
LOWER RISKS & COSTS
FASTER DELIVERY
{ REST }
DEV
STAGING
PROD

Firewall for AI

AI Adoption is Accelerating Faster Than Security

AI is transforming business faster than traditional security can adapt.

AI is a New Attack Surface.

Organizations must secure AI interactions to protect data, ensure compliance, and maintain trust.

Key Risks Organizations Face with AI

AI risk is now a **business risk.**

1 DATA LEAKAGE

Sensitive data may be exposed through AI interactions.

Risk of exposing confidential business data, customer information, and IP.

2 PROMPT INJECTION

Attackers manipulate AI behavior through malicious prompts.

Leads to data disclosure, policy bypass, and unauthorized actions.

3 TOXIC RESPONSES

AI may generate harmful, biased, or inappropriate content.

Harms brand reputation, customer experience, and employee safety.

4 COMPLIANCE RISK

AI usage may violate privacy laws and industry regulations.

Results in legal penalties, regulatory fines, and loss of business licenses.

AI risk is now a **business risk.**

BRAND REPUTATION
Negative incidents can damage public perception and trust.

CUSTOMER TRUST
Customers expect their data to be safe and private.

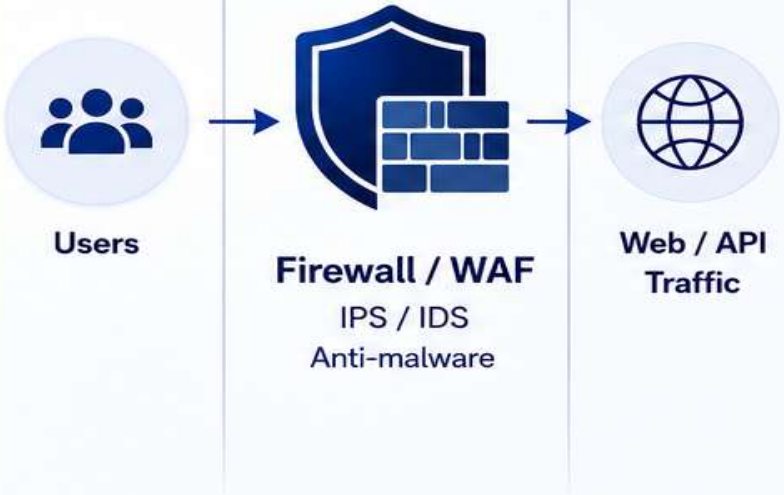
REGULATORY COMPLIANCE
Non-compliance can lead to fines and legal consequences.

INTELLECTUAL PROPERTY
Sensitive IP can be exposed, copied, or misused.

Traditional Security Was Not Designed for AI

AI introduces risks that existing security controls **cannot fully see.**

TRADITIONAL SECURITY
Protects Web & API



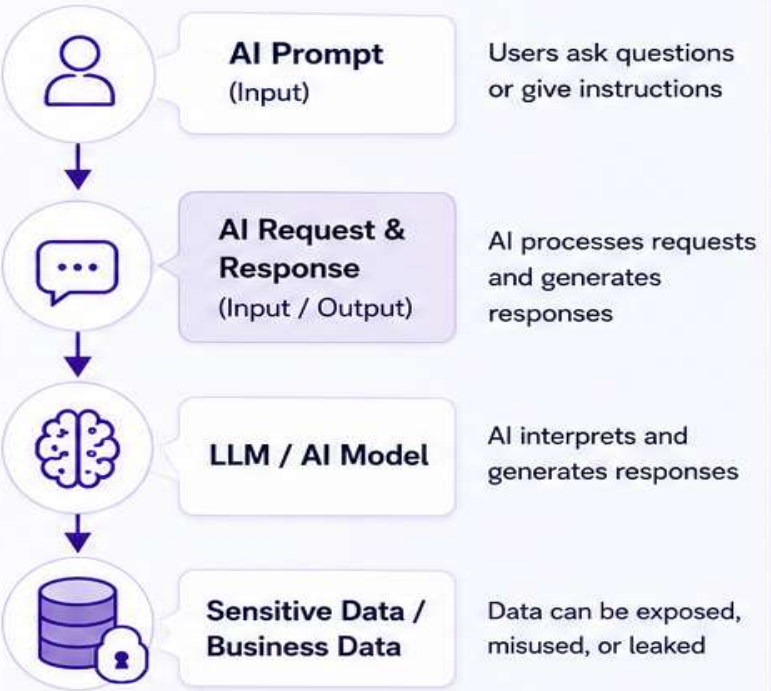
- Sees IP, ports, protocols, and payloads
- Protects infrastructure and applications
- Great for known threats and patterns

UNPROTECTED AI INTERACTIONS

Context, intent, and content are invisible to traditional security controls.

- **Prompt Injection**
- **Sensitive Data Exposure**
- **AI Misuse & Abuse**

AI INTERACTIONS
A New Attack Surface



- Prompts and responses carry intent and context
- Risks are not visible in network traffic alone
- Requires AI-aware security controls

AI requires a new layer of security purpose-built to understand and protect AI interactions.

Firewall for AI

Purpose-built protection for enterprise AI.

Protect every AI interaction. Inbound prompts and outbound responses.

USERS & APPLICATIONS

- Employees
- Customers
- Applications

INPUT

Prompts
Queries

OUTPUT

Responses
Results

LLM / AI MODEL

- Large Language Models (LLMs)
- AI Applications
- AI Services

DEPLOY ANYWHERE

- Cloud AI
- Hybrid AI
- On-prem AI
- Multi-cloud

BUILT-IN PROTECTION AGAINST AI-SPECIFIC RISKS

PROMPT INJECTION
Blocks malicious or manipulative prompts

DATA LEAKAGE
Prevents exposure of sensitive or confidential data

HARMFUL CONTENT
Filters toxic, biased, or inappropriate content

AI ABUSE
Detects and mitigates misuse and adversarial attacks

BUSINESS OUTCOMES

Reduce AI Risk
Protect data, brand, and customers

Ensure Compliance
Meet regulatory and governance requirements

Enable Innovation
Adopt AI with confidence and agility

Maintain Trust
Build customer trust with safe and responsible AI

Enterprise-Ready
Scalable, reliable, and built for any environment

A unified layer of security between your users and AI. Secure AI. Empower Business.

Executive Takeaway

AI is transforming business.
Security and governance determine who wins in the AI era.

AI is a strategic advantage.

Drive innovation, productivity, and growth across the enterprise.

AI security is now essential.

Protect data, prevent misuse, and build resilience against emerging threats.

Governance must evolve with AI.

Establish policies, ensure compliance, and maintain responsible AI use.

Organizations that secure AI early will scale AI faster and safer.

AI as a Core Platform

AI will power core business processes and customer experiences.

Security & Governance Create Advantage

Organizations that act early will lead with trust and responsibility.

Firewall for AI

Purpose-built protection for AI interactions—inputs and outputs.

Enterprise-Ready

Works across cloud, on-prem, hybrid, and multi-cloud environments.

Foundation for Enterprise AI Security

Akamai Firewall for AI helps you innovate with confidence and control.