SKUDONET

Web Application and API Protection (WAAP) Buying Guide

Protecting your web applications and APIs from security threats is crucial in today's digital landscape.

What are a WEB Application and API Protection | WAAP

Web Application and API Protection (WAAP) refers to the **set of security measures** and **technologies** designed to **safeguard web applications** and **application programming interfaces** (APIs) from a wide range of threats and vulnerabilities.

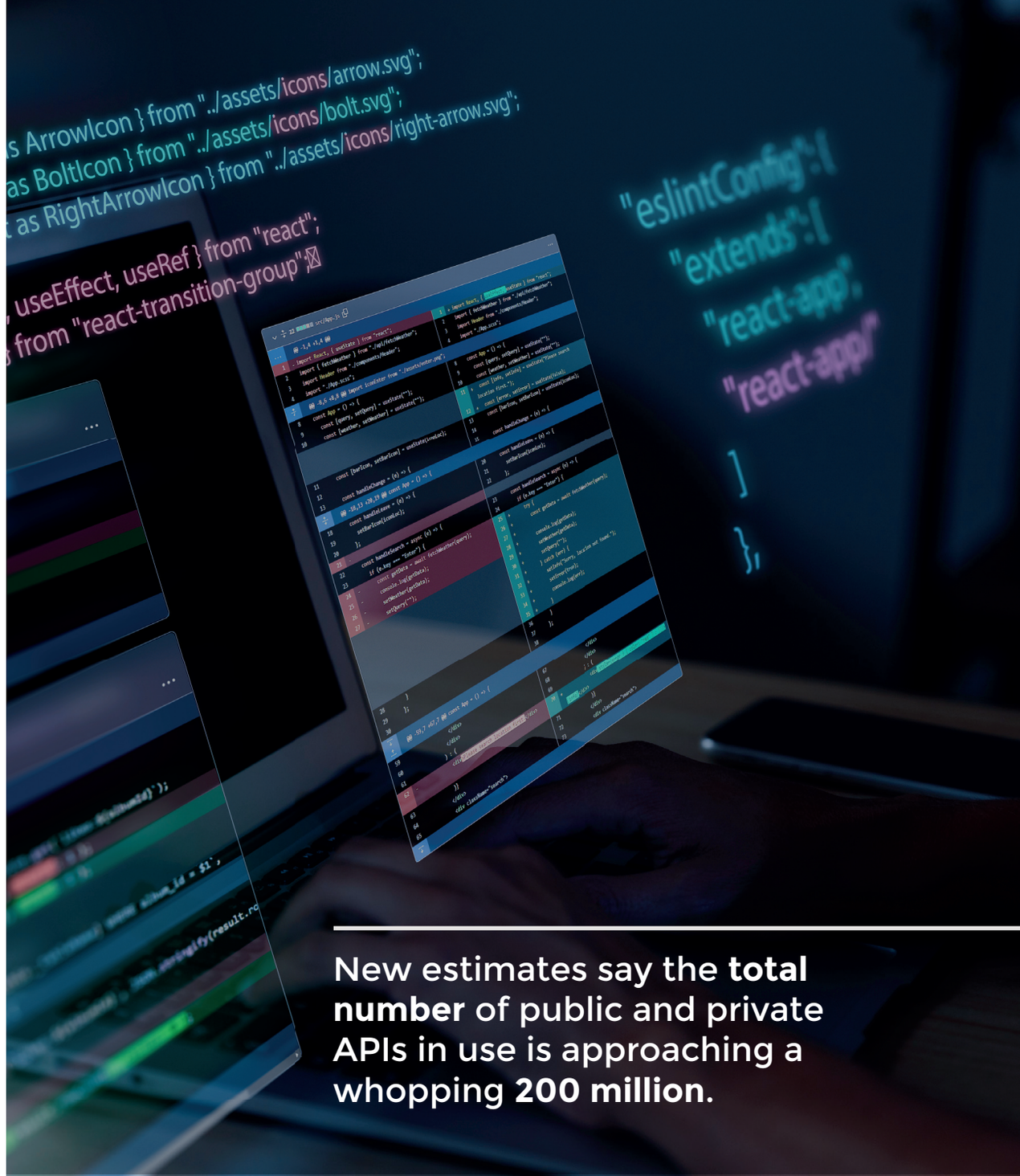
WAAP is a progressive evolution of the **SKUDONET** security product, the Web Application Firewall (WAF). The WAAP offers the same features as a traditional WAF but also protects APIs besides web applications.

With the evolution of cloud services and SaaS (Software as a Service), the need for integrating various environments has advanced the usage of APIs, providing the best solution for orchestrating all those services. This functionality makes the WAAP more advanced than the WAF, as one may deploy A WAAP at the edge of a network containing public services or configure it in the same environment with an ADC.

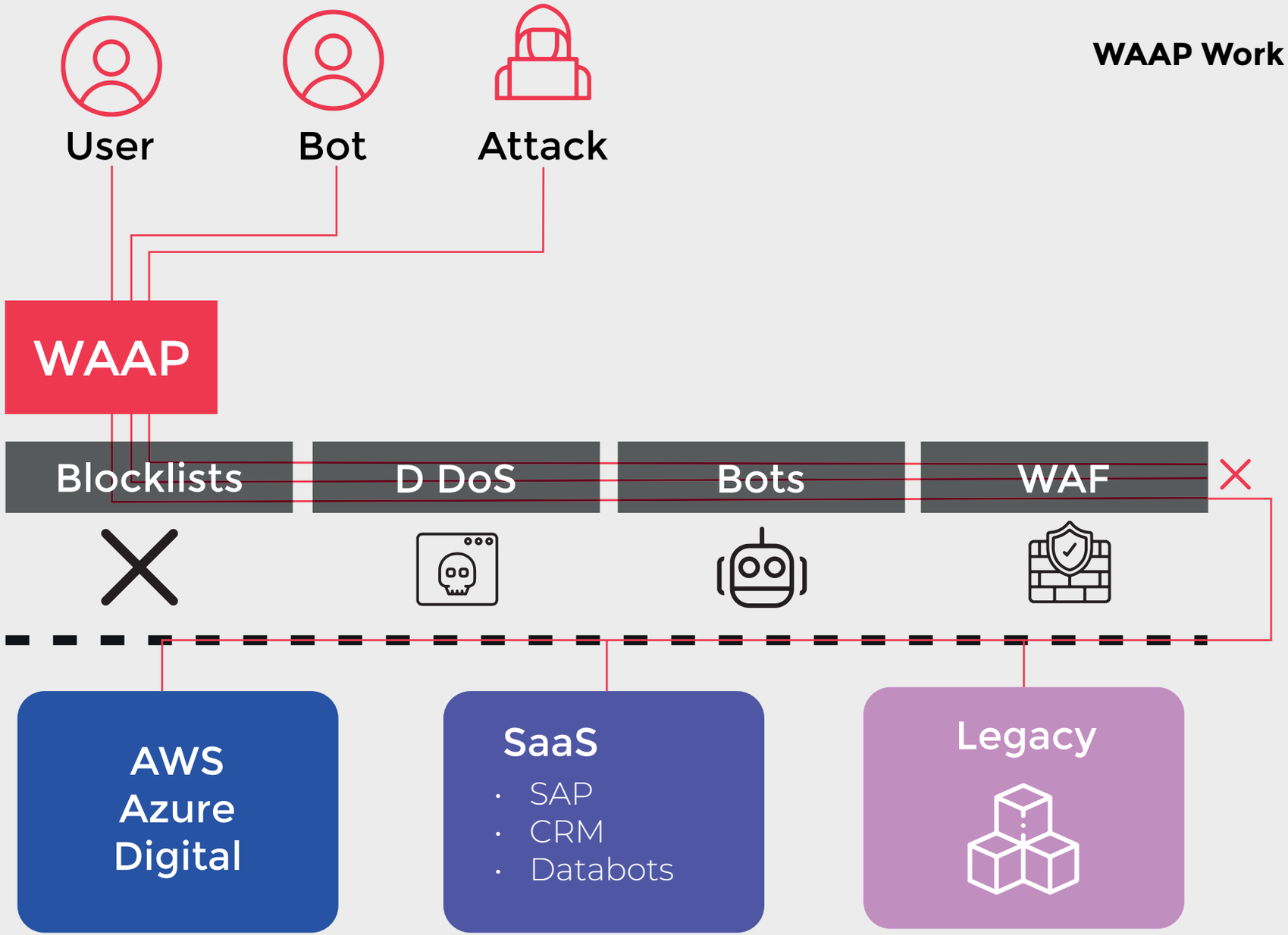
Why A WAAP is required?

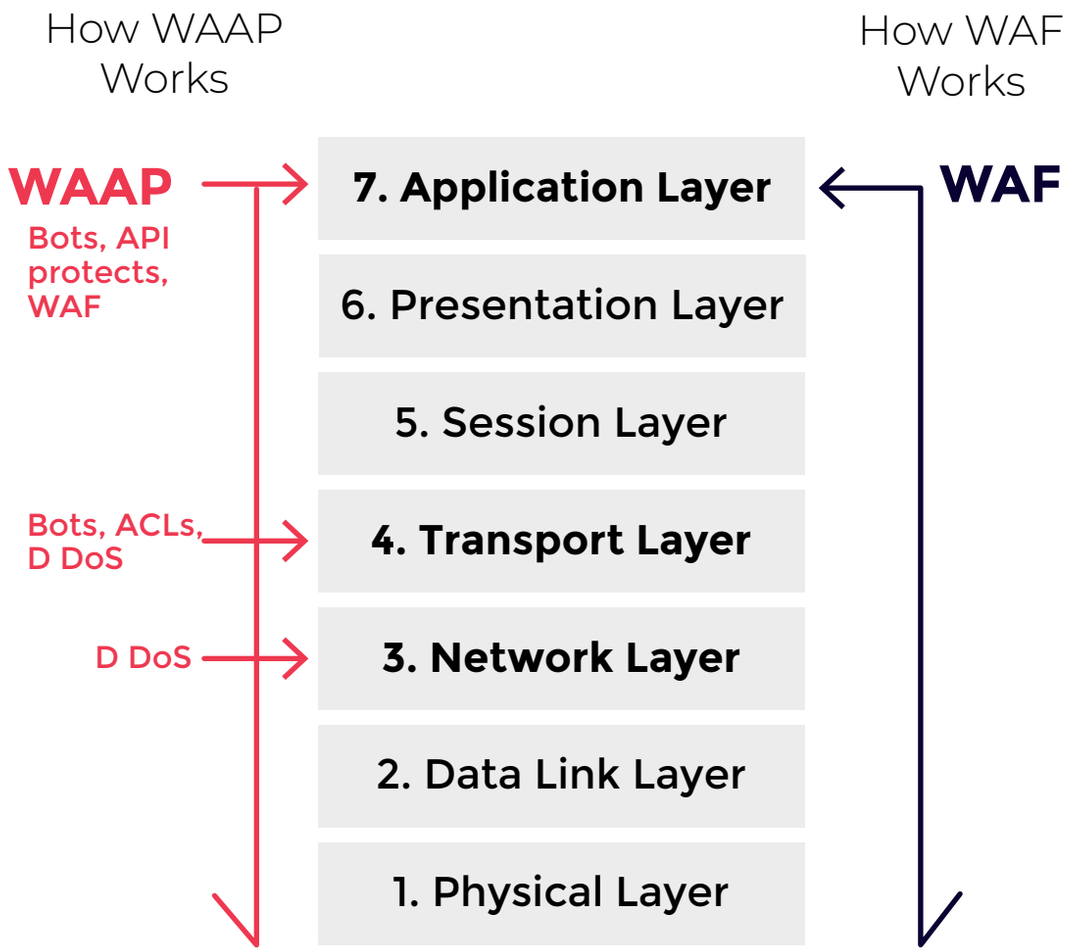
Since one may access APIs and web Applications easily on the internet, **security** is a **big concern** because sensitive data is exposed. An attacker may cause a **security breach** to obtain **private information**. So, a WAAP is necessary since traditional web security won't handle:

- **Signature matching is not enough for application security:** the content of Web applications and APIs are continuously changing. So, the system requires constant learning.
- **Blocking traffic based on source IP or destination Port is not enough:** traditional firewalls block IP and Ports, often facing encrypted data. TLS decryption and analysis enable our WAAP to provide deeper security insights.
- **HTTP(S) traffic is currently the most used and it can offer complexity in the analysis:** Web traffic mainly occurs at OSI Layer 7 with HTTP(S). Modern security must extend beyond traditional IPS/IDS to protect Layer 7 protocols effectively.



WAAP Work Model





Visual difference between WAF (old mechanism) and WAAP (new protection mechanism) based on different levels of security according to the OSI model. WAAP works on layers 3, 4, and 7, while WAF operates only on layer 7.

Which features a WAAP can offer that a traditional WAF can't

Automation and learning

Experienced in Web Application and API Protection (WAAP) integrated within an Application Delivery Controller (ADC). Proficient in real-time threat analysis, utilizing mechanisms like DoS Detection, bot detection, and protocol protection to ensure continuous learning and enhanced security.

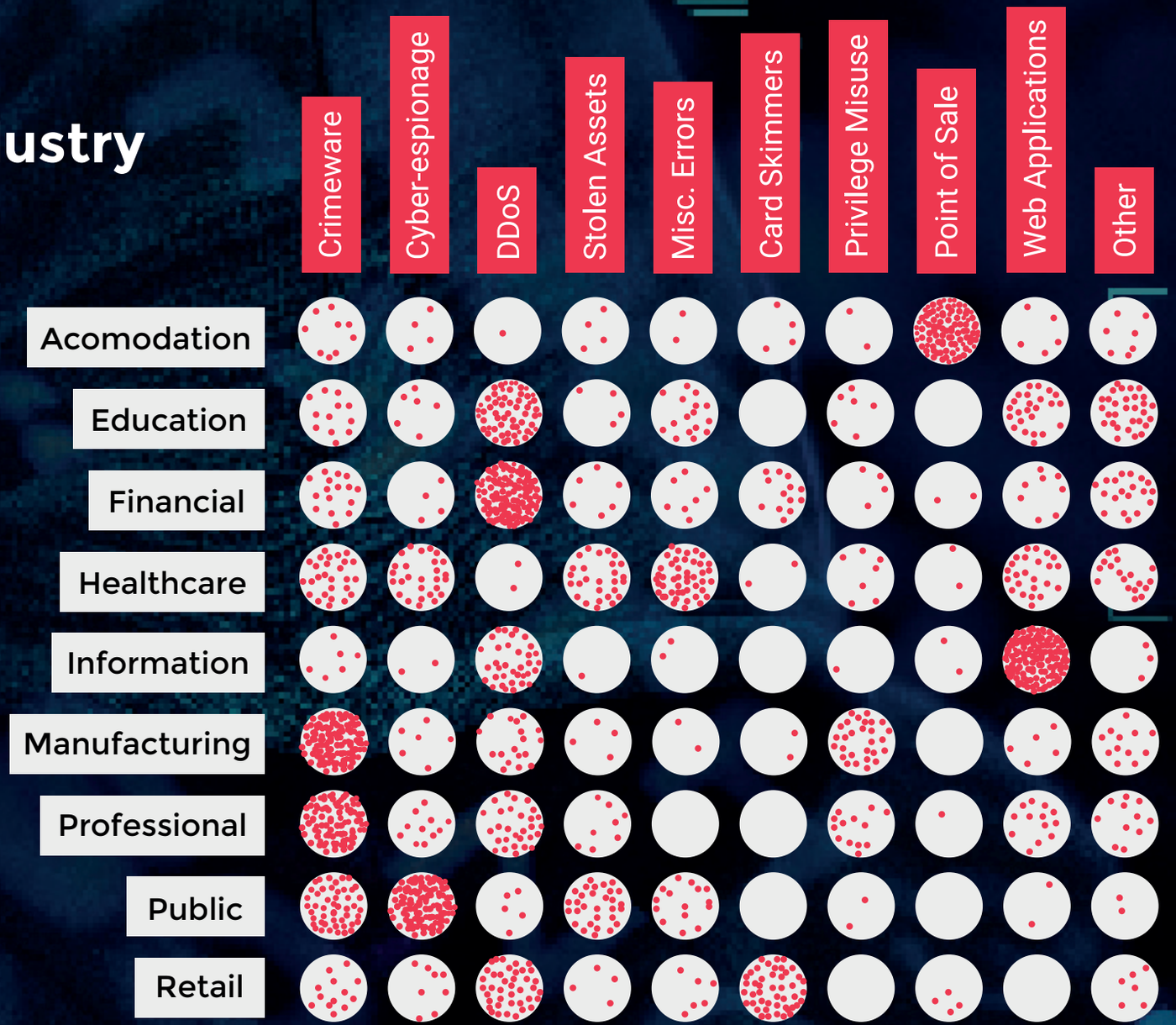
Secure APIs and Microservices

On a daily basis, engineers build APIs and microservices to offer public services. The WAAP must protect these endpoints, taking into consideration the exposed information.

Cyber Incidents By Industry

Some industries are more vulnerable to **cyber attacks** than others, simply due to the nature of their business.

Companies that hold sensitive data or personally identifiable information are common targets for hackers.



Key Points to Consider for Making an Informed Decision For WAAP Solutions:

1 Understand Your Requirements

Before diving into the selection process, **identify your specific security needs**: determine whether you need protection for web applications, APIs, or both. Consider the scalability requirements to accommodate future growth. If you need to comply with specific regulations (e.g., GDPR, HIPAA), ensure the solution aligns with those requirements. Decide between on-premises, cloud-based, or hybrid deployment models.

2 Core Security Features

Evaluate the essential security features offered:

- Look for a Web Application Firewall (WAF) to filter out malicious traffic and protect against OWASP Top Ten threats.
- DDoS Protection, to maintain application availability.
- API Security, check if the solution supports authentication, authorization, and rate limiting to prevent unauthorized access.
- SSL/TLS Encryption.
- Web Application Scanning, to identify and address application weaknesses.

3 Threat Detection and Prevention

The WAAP solution should have robust threat detection and prevention capabilities as:

- Real-Time Monitoring.
- Machine Learning and AI, to detect and respond to evolving threats.
- Behavioral Analysis.

4 Access Control and Authentication

Ensure that the WAAP solution offers robust access control and authentication mechanisms:

- Authentication Methods: Look for support for multi-factor authentication (MFA) and strong password policies.
- Role-Based Access Control (RBAC): If managing multiple users, RBAC can help enforce least privilege access.
- OAuth and JWT Support: For APIs, check for OAuth and JSON Web Token (JWT) support for secure authentication.

5 Reporting and Analytics

Comprehensive reporting and analytics are essential for understanding your security posture:

- Log Analysis: Ensure the solution provides detailed logs for security incidents and user activities.
- Custom Dashboards: Look for customizable dashboards to visualize security data relevant to your organization.
- Compliance Reporting: If needed, check if the solution can generate compliance reports for audits.

6 Integration and Compatibility

Consider how well the WAAP solution integrates with your existing infrastructure:

- API Support: verify compatibility with the APIs you're using (REST, SOAP, GraphQL).
- Integration with SIEM: Ensure the solution can integrate with Security Information and Event Management (SIEM) systems.
- Cloud and Container Compatibility: If you use cloud services or containers, check for compatibility with your cloud provider and container orchestration platform.

7 Ease of Management

Evaluate the ease of management and usability of the WAAP solution:

- User Interface: Ensure the interface is intuitive and user-friendly for your security team.
- Automation: Look for automation features that can streamline security management tasks.
- Updates and Patching: Check how updates and patches are handled to maintain security.

8 Cost and Licensing

Consider the cost factors:

- Total Cost of Ownership (TCO): Evaluate the long-term cost, including licensing, support, and any additional hardware or infrastructure requirements.
- Licensing Model: Understand the pricing model (e.g., per user, per device, or subscription-based).
- Scalability Costs: Determine if costs scale with usage and growth.

9 Support and Maintenance

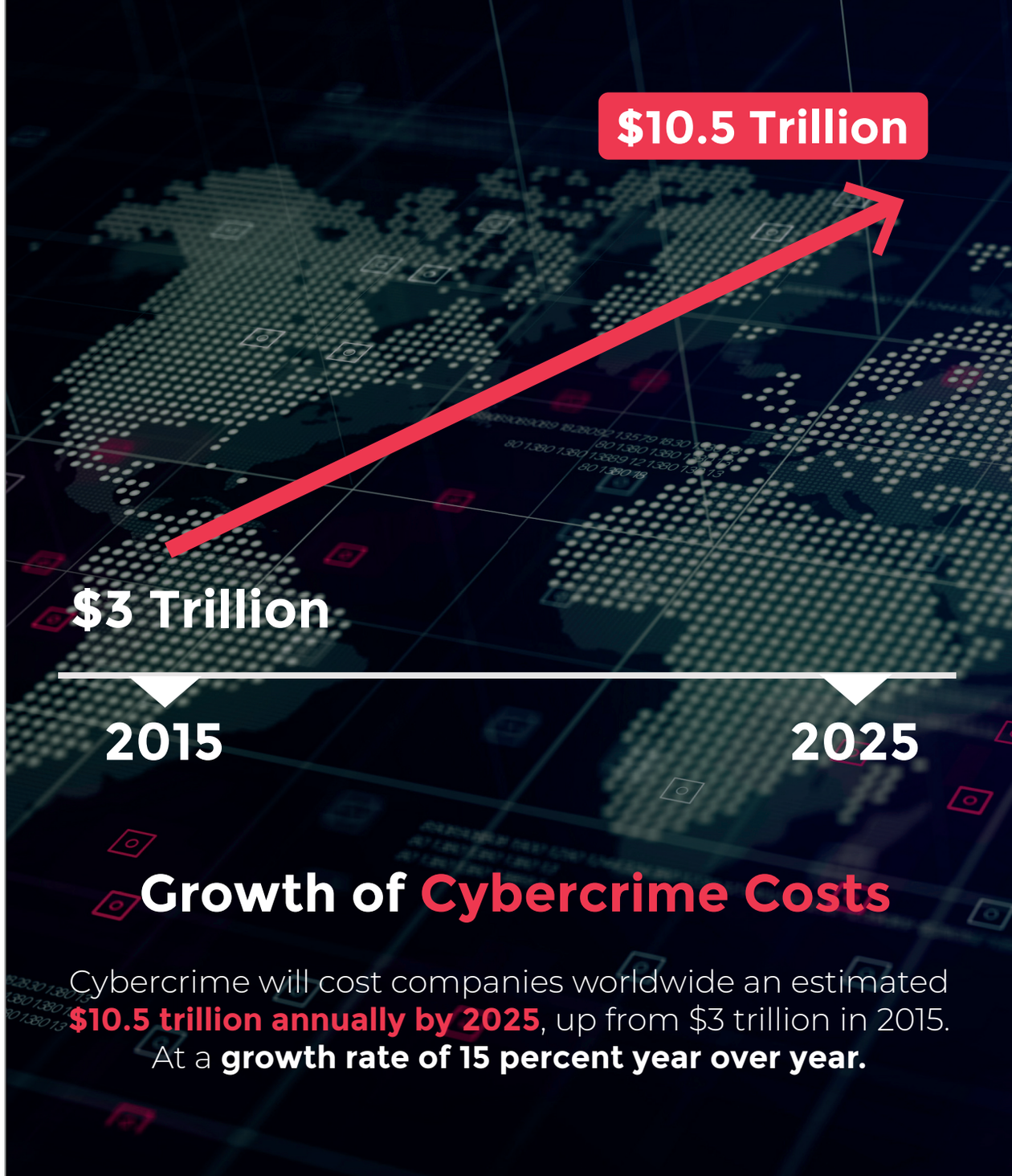
Review the available support options:

- Customer Support: Assess the availability and responsiveness of customer support.
- Documentation: Ensure that comprehensive documentation and training resources are available.
- Maintenance: Check if the solution offers regular updates and patches for security enhancements.

10 Security Community and Reputation

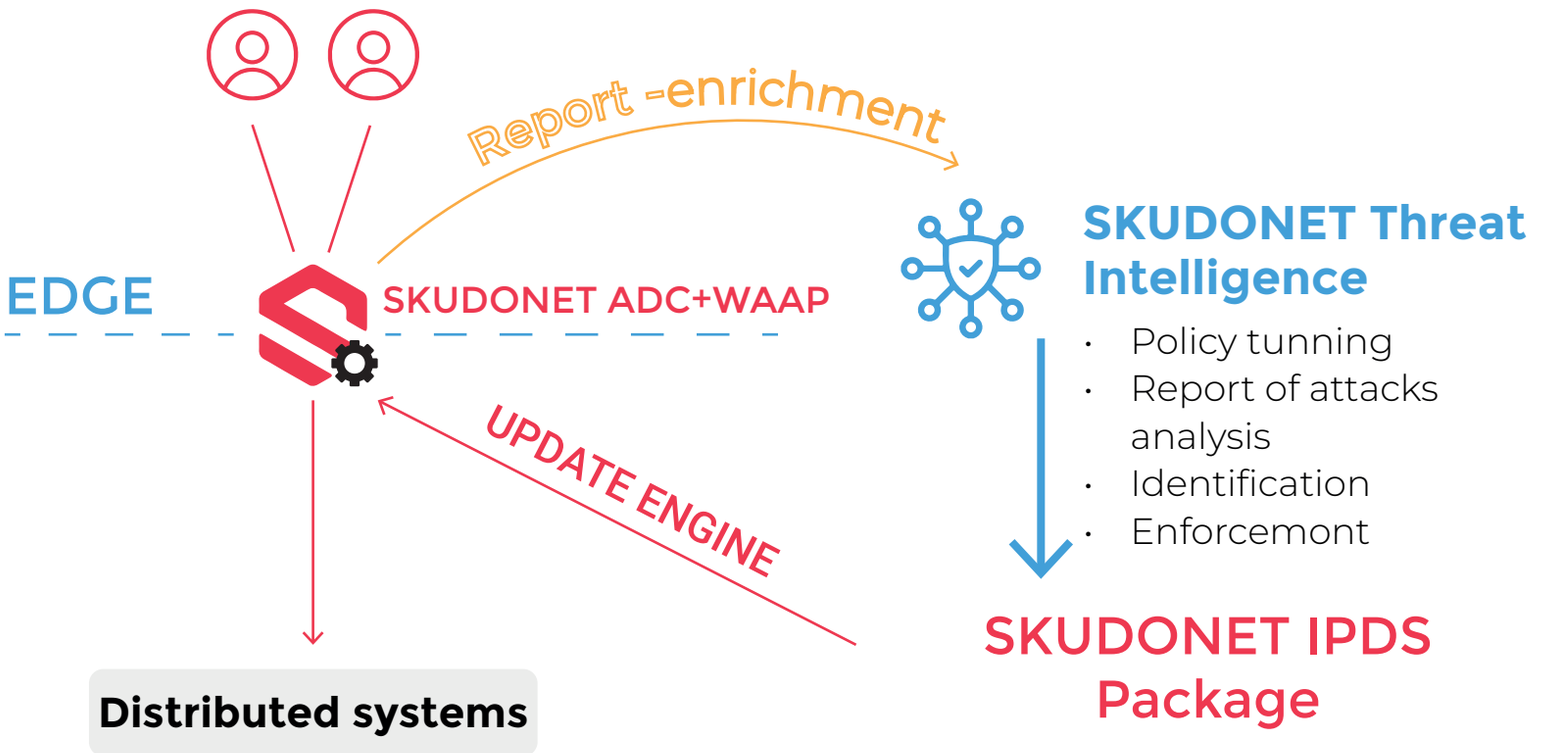
Research the WAAP solution's reputation within the security community:

- User Reviews: Read user reviews and testimonials to gauge customer satisfaction.
- Vendor Reputation: Investigate the vendor's history and reputation in the cybersecurity industry.
- By following this buying guide, you can select a Web Application and API Protection solution that aligns with your organization's security needs and safeguards your web applications and APIs effectively.



How SKUDONET Works as a WAAP?

SKUDONET ADC includes a Cybersecurity module called IPDS (Intrusion prevention and detection system). This module offers WAAP capabilities, automation, and learning for WEBs and APIs. SKUDONET includes a package called skudonet-ipds, and this package is updated daily. This package has more than 4 mechanisms for Web Applications and API protection.



How WAAP Enrichment Works, the Evolution Cycle, and the Lifespan of Attacks and Protection in Our System.

Our threat intelligence captures data, processes, filters, identifies, and compiles it into a final package called 'skudonet-ipds.' This package is sent to our product to update the security engine, allowing WAAP to provide protection. The security engine itself applies the received rules and reports all captured information back to threat intelligence for system nourishment. This process creates a feedback loop for continuous improvement and evolution.

What SKUDONET protects with WAAP?

More than **200 lists** of **IP addresses** and ranges by country.

Lists of attackers sorted by application (email, web, spam...)

Attackers identified as spyware, crawlers, bots, etc.

Protection for APIs through HTTPS protocol identification.

Protection against SELI, XSS, LFI, RCE, RFI.

Protection against PHP, Node.js, Java, and other vulnerabilities.

Protection against DDoS attacks, such as RESET FLOOD and IP ORIGIN.

Daily content updates.

The possibility of seamless integration with third parties.

About SKUDONET

Achieve Perfect Load Balancing With a Flexible Open Source ADC

Effortlesly enhance the **security** and **continuity** of your **applications** with an **open-source ADC** that enables you to **reduce costs** and achieve maximum **flexibility** in you IT infrastructure.

Find out more at **skudonet.com**

SKUDONET