Bayesian Cybersecurity

Traffic-Prism

Adaptive WAF: Session intelligence, DOM based attacks protection

Introduction

About Us:

- Gen AI-powered startup based in Thane, India focused on improving cybersecurity postures of all web-based businesses.
- Works with any WAF to add session level correlations and intelligence features.
- Inbuilt support for ModSecurity, natural upgrade potential for 100,000+ ModSecurity installations.
- First platform offering DOM-based attack detection and Bayesian risk inference for comprehensive web protection.
- Rule-based and Gen AI-based scoring engine with Bayesian Inference option.
- Accepted in Microsoft Founder program.

ISO 27001

What Problems Are We Solving?

Core Capabilities:

- Primary defense against DOM-based XSS, DOM based SQLi, Clickjacking, and similar attacks.
- Complements any WAF in detecting session-level analytics and scoring for attacks that WAFs miss.
- Vulnerability analysis/incident reporting using real-time Power BI reporting.
- Rule based automatic termination of risky sessions is possible.
- Inbuilt support for ModSecurity an opensource WAF and FastNetMon for DDoS detection thus making our stack comprehensive solution that can match or exceed commercial WAFs
- Upgrade for 100,000+ ModSecurity installations to bring them at par with market leading WAFs by providing bot detection, session intelligence and correlation features as well as FastNetMon for DDoS detections.

A. DOM-Based Attack Vectors

- Modern websites are dynamic, enabling innovation but opening doors to **client-side vulnerabilities (DOM XSS, clickjacking, etc.).**
- These vulnerabilities can bypass **traditional defenses like WAFs and cause severe breaches.**
- Platforms like ours **monitor malicious DOM manipulations in real-time** to stop threats before escalation.
- Once the session is deemed risky then based on score, rule can be set to automatically terminate such sessions reducing the possible impact.

B. Complement WAF: Bridging WAF Security Gaps

Advanced Threats Bypass Traditional WAF Controls:

- Bots mimic human behavior.
- Complex attacks span multiple sessions.
- Sophisticated threats adapt to binary rules.
- Automated browser attacks via Playwright-Selenium.
- Risk score based rule to automate session termination.

WAF Limitations:

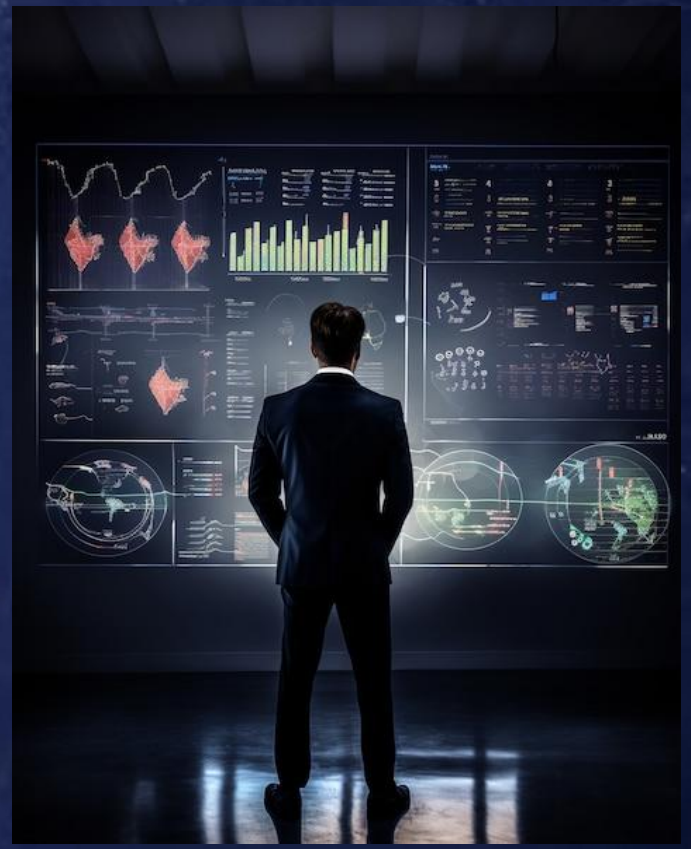
- Binary allow/block decisions.
- No session-level intelligence.
- Misses behavioral attack patterns.

ModSecurity and FastNetMon:

- Support all commercial WAFs
- Inbuilt support for opensource WAF ModSecurity.
- Automated update of static rules.
- PowerBI analytics for ModSecurity.

How Do We Complement WAF

- **OLAP-based sub-second historical pattern analysis:** Even for terabytes of data, calculates the first risk score.
- **Gen AI:** Takes the next step to check for zero-day attacks and calculates the second risk score.
- **Bayesian model:** Used to calculate the final risk score from these two, considering client-specific nuances.
- **Known historical pattern detection:** 800+ patterns, 170+ for web.
- **Detection of different types of bots:** Includes bots such as Huawei Petalbot.
- **Geography, time, and device-based OLAP triggers.**



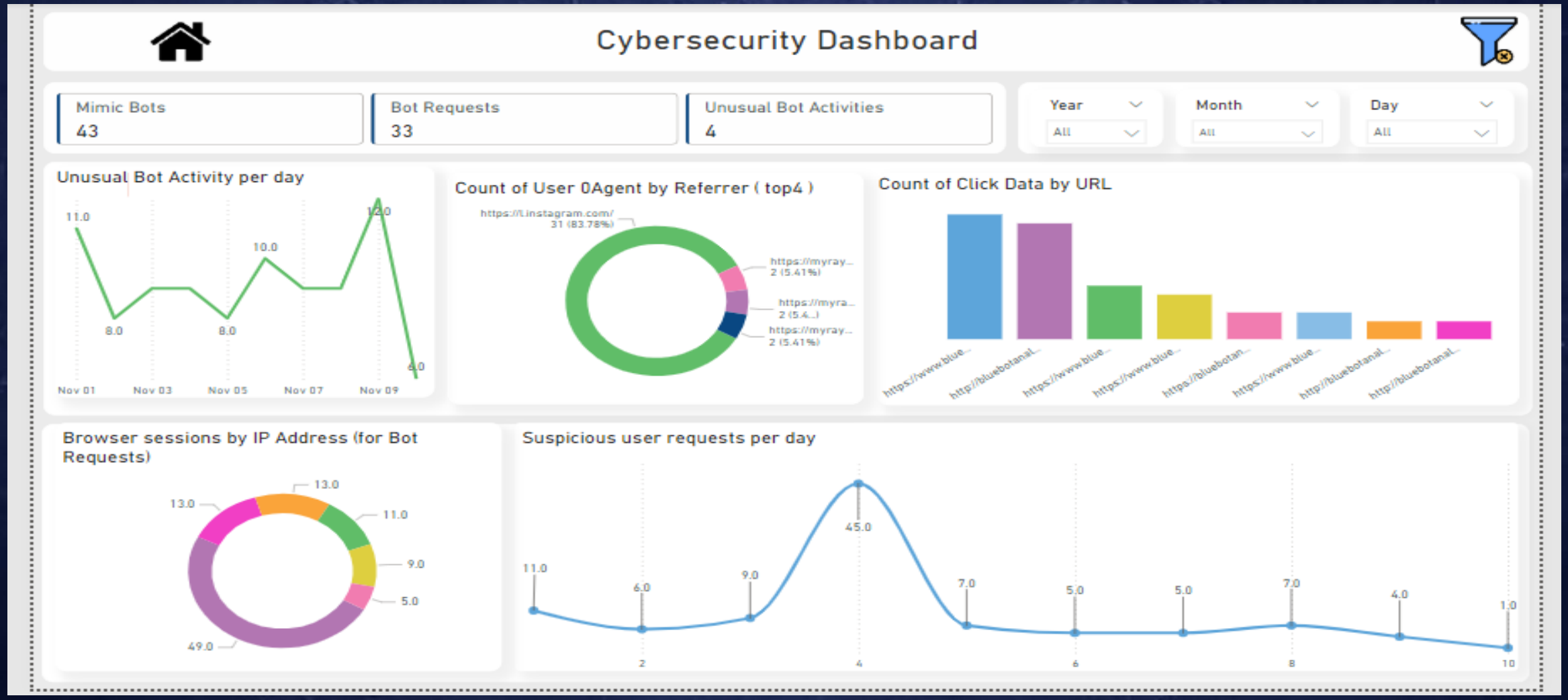
WAF Comparison

Product	Session-Level Security	Bot Detection	Dynamic Risk-Based Controls	Generative AI Integration	Deployment Complexity
Bayesian - Traffic Prism	ONLY product with real time session-layer controls with OLAP and Generative AI integration	Mimic bot behavior distinction with multi-dimensional analysis	Real-time session scoring with adaptive responses	Utilizes Generative AI for zero-day threat detection and real-time insights	5-minute deployment with a single pixel; no infrastructure changes required
Akamai Kona Site Defender	Primarily focuses on network and application layer security	Offers bot management as an add-on feature	Customizable security rules with manual adjustments	Employs advanced data analysis techniques	Requires integration with existing infrastructure; moderate complexity
Imperva WAF	Offers application-layer security with some session awareness	Advanced bot protection capabilities	Automated policy formulation with rapid rule propagation	Uses machine learning for threat detection	Deployment varies; cloud-based options are simpler
Cloudflare WAF	Focuses on network and application layer security	Provides bot mitigation features	Managed rules with limited customization	Implements machine learning for threat detection	Easy to deploy and manage through a user-friendly interface
AWS WAF	Provides basic rule-based protections	Includes bot control features	Customizable web security rules	Focuses on rule-based threat mitigation	Integrated with AWS services; setup complexity varies
F5 Advanced WAF	Includes behavioral analysis for application security	Integrated bot protection services	Behavioral analysis for threat detection	Leverages machine learning for advanced threat detection	Deployment flexibility for virtualized and private clouds; may require specialized knowledge

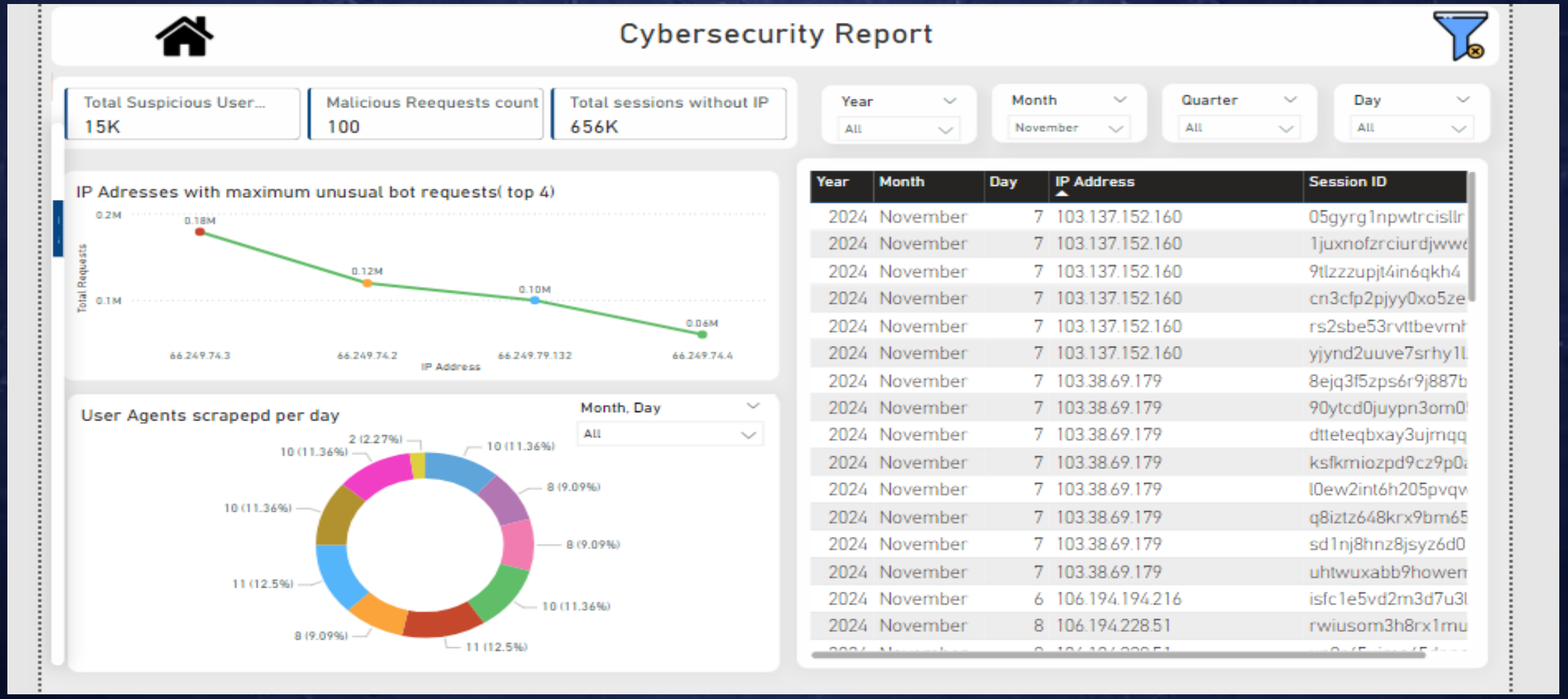
C. Power BI-Based Vulnerability Analysis

- We provide detailed **session logs and forensic data**, helping security teams understand and respond to incidents effectively. This data is invaluable for **root cause analysis** and improving overall defenses.
- We also have real time POWER BI report layer integration that has canned reports as well as customized reports feature
- Integrated PowerBI reports for ModSecurity WAF, pipeline for other WAFs
- Can support terabytes of data analytics with PowerBI

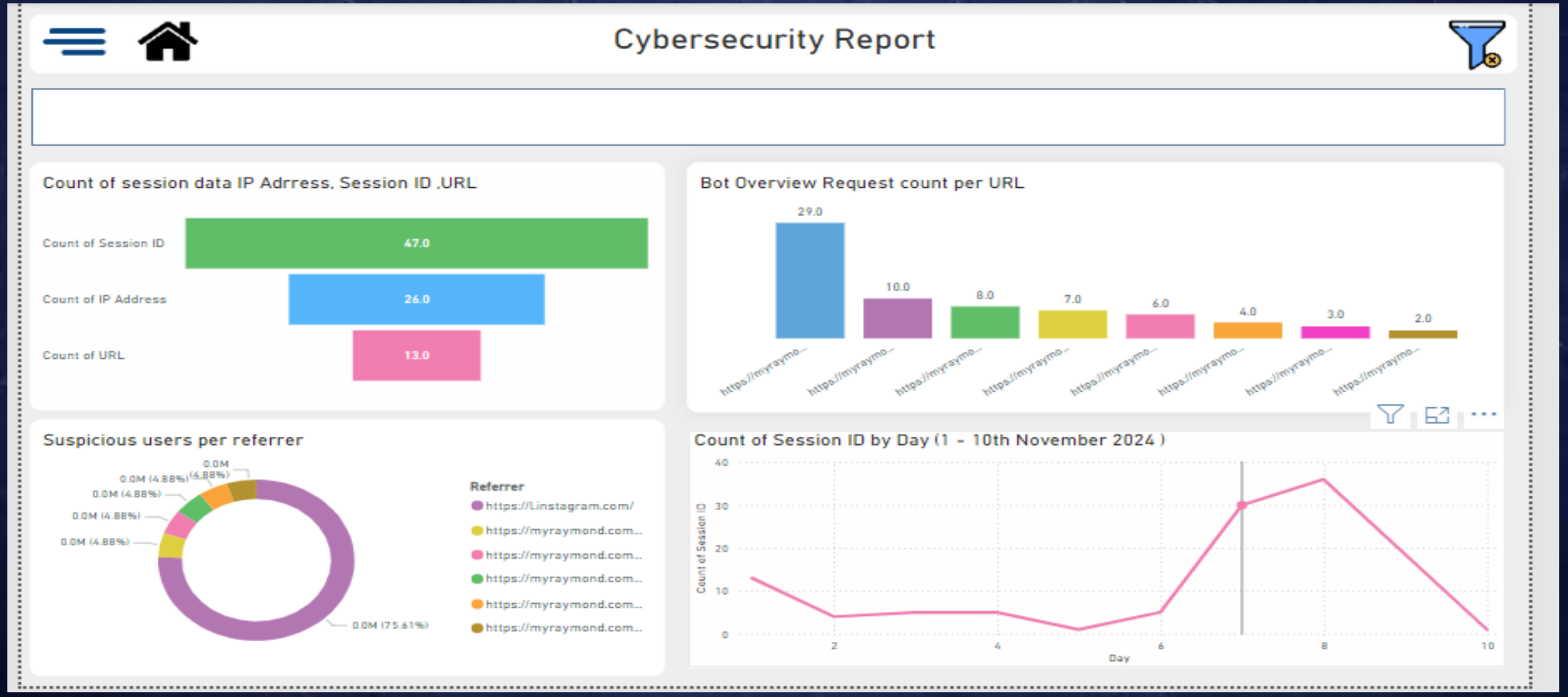
Sample Dashboards



Sample Dashboards



Sample Dashboards



Future Roadmap

The Traffic-Prism platform identifies itself as an OLAP-powered, distributed cybersecurity platform with immense potential.

- We are working on integrating IoT application cybersecurity (such as smart meters).
- With proven expertise in handling millions of real-time sessions, IoT devices can also be treated as persistent sessions with different protocols (like Zigbee) and device types.
- The backend infrastructure for real-time, two-way communication has been battle-tested.

Context: Web Page Performance Beginnings

- **Our Dynamic Session Control** technology, powered by Generative AI and OLAP multidimensional analysis, has been widely used by us for a variety of clients to enhance web performance optimization during high-demand campaigns. This powerful solution enables selective prioritization of high-quality traffic, ensuring optimal load times of under 5 seconds, even under heavy visitor loads.
- By dynamically managing session engagement and filtering for the most valuable user sessions, **Dynamic Session Control** has allowed clients to achieve a seamless user experience and maximize their campaign effectiveness. While primarily utilized for performance optimization, this technology is also grounded in robust rule-based session management capabilities, adaptable to both performance and security applications.
- Below, you'll find a selection of companies that have successfully utilized our **Dynamic Session Control** to improve web performance and deliver a high-quality user experience.

Our Clients

hindware

VECTOR CONSULTING GROUP

0101 Data based conversion specialist

Raymond

incor BUILDING LIFEMARKS™

IESA India Energy Storage Alliance

Mercedes-Benz

Carestream

circular angle aim higher

BRASS TACKS

CellBeans

Godrej SECURITY SOLUTIONS

BAYLEAF

ashdeen

LAKSHMI

Recycle rewards Think Waste, Think Rewards

EXIMIOUS

KHS improving lives

STEFANO RICCI

Share India You generate, we multiply

adventure

APPENDIX A: DOM-Based Attack Vectors

DOM-Based Attack	Description	Platform Protection
DOM-Based Cross-Site Scripting (XSS)	Malicious scripts executed due to insecure DOM manipulations.	Monitor and flag updates to innerHTML, eval, or document.location.
Clickjacking	Visual manipulation of DOM to trick users into interacting with hidden elements.	Detect iframe injections, overlays, or visual anomalies.
Content Spoofing	Manipulates DOM to display misleading or malicious content.	Identify unauthorized content updates in the DOM.
Keystroke Logging via DOM Manipulation	Injects scripts to monitor and capture user keystrokes.	Monitor event listener injections and unusual keypress activities.
Credential Harvesting with Modified Forms	Modifies legitimate forms to redirect sensitive information.	Validate and track changes to form actions and critical DOM elements.

APPENDIX B: Where Do We Complement WAF

ATTACK THROUGH BROWSER?			
Attack Type	Browser Sessions (%)	Burp Suite / cURL (	Reasoning
Cross-Site Request Forgery (CSRF)	90	10	CSRF relies on browser behavior (e.g., automatic cookies) and user interaction. Burp/cURL lacks the browser environment needed to perform CSRF effectively.
Session Hijacking	40	60	Hijacking via the browser happens through social engineering (e.g., phishing) or stealing cookies via XSS. Tools are used for advanced session token abuse.
Open Redirects	20	80	Typically exploited via URLs in browser sessions, but tools like Burp can test redirect functionality and chain it with other attacks like phishing.
Clickjacking	90	10	Requires user interaction via browsers (e.g., clicking on hidden iframes). Tools like Burp/cURL are ineffective for executing such attacks.
Credential Stuffing	20	80	Tools like Burp Suite are ideal for automating bulk login attempts. Browser-based attacks require manual efforts, making them less effective for this attack.
Phishing	95	5	Almost entirely browser-based, as phishing relies on tricking users via fake websites or emails. Tools are irrelevant for direct phishing execution.
CORS Misconfiguration	20	80	Exploiting CORS often involves testing API endpoints, which is easier and faster with tools like Burp or cURL. Browser sessions can still reveal misconfigurations.
File Upload Vulnerabilities	30	70	Both browsers and tools can exploit file upload vulnerabilities. Tools like Burp allow easier testing of file validation mechanisms.
XSS (Cross-Site Scripting)	40	60	XSS primarily targets browser behavior and user interaction. Tools are more useful for testing payloads but not the actual execution in users' browsers.
SQL Injection (SQLi)	10	90	Tools are more likely to exploit SQLi due to their flexibility in bypassing client-side validation and automating payload testing.

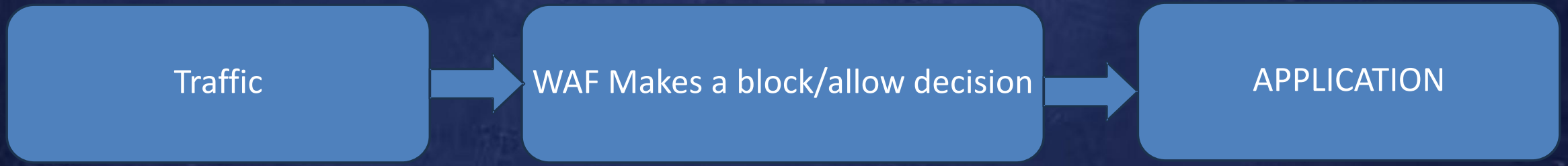
How Likely WAF Will Catch It

Attack Type	WAF Prevention (%)	Session-Level Reliance (%)	Why Session Termination is Needed
CSRF	80	20	Detect anomalies in user actions after the attack succeeds.
Session Hijacking	40	60	Detect and stop abuse of stolen session tokens.
Open Redirects	70	30	Stop malicious redirects once detected in session behavior.
Clickjacking	20	80	Identify suspicious clicks and terminate sessions to prevent further harm.
Credential Stuffir	60	20	Block further abuse after detecting compromised credentials.
Phishing	50	50	Detect suspicious actions following credential compromise.
CORS Misconfigu	70	30	Detect abuse of APIs due to misconfigured policies.
File Upload Vulne	70	30	Stop malicious file use by detecting abnormal upload behavior.
XSS	80	20	Prevent stolen session cookie abuse or malicious actions post-injection.
SQLi	80	20	Stop abnormal session activity post-SQLi exploitation.

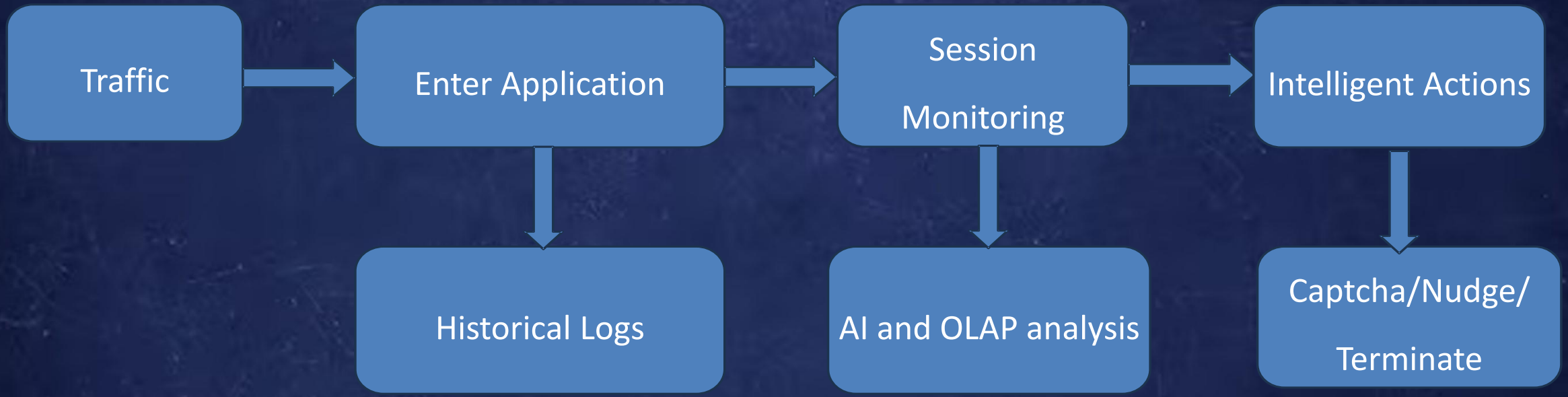
Relevance of Session Platform

Attack Type	ATT&CK	Platform Share (%)	Daily Attacks (Global)
CSRF	T1110.004	18	10000000
Session Hijacking	T1539	24	500000
Open Redirects	T1608.001	6	1000000
Clickjacking	T1185	72	50000
Credential Stuffing	T1110.001	16	530000000
Phishing	T1566	45	15000000
CORS Misconfiguration	T1090.003	24	100000
File Upload Vulnerabilities	T1203	21	25000
XSS	T1509.007	12	1400000
SQLi	T1190	2	1000000
RED	Critical		
Orange	Severe		
Blue	Limited Impact		

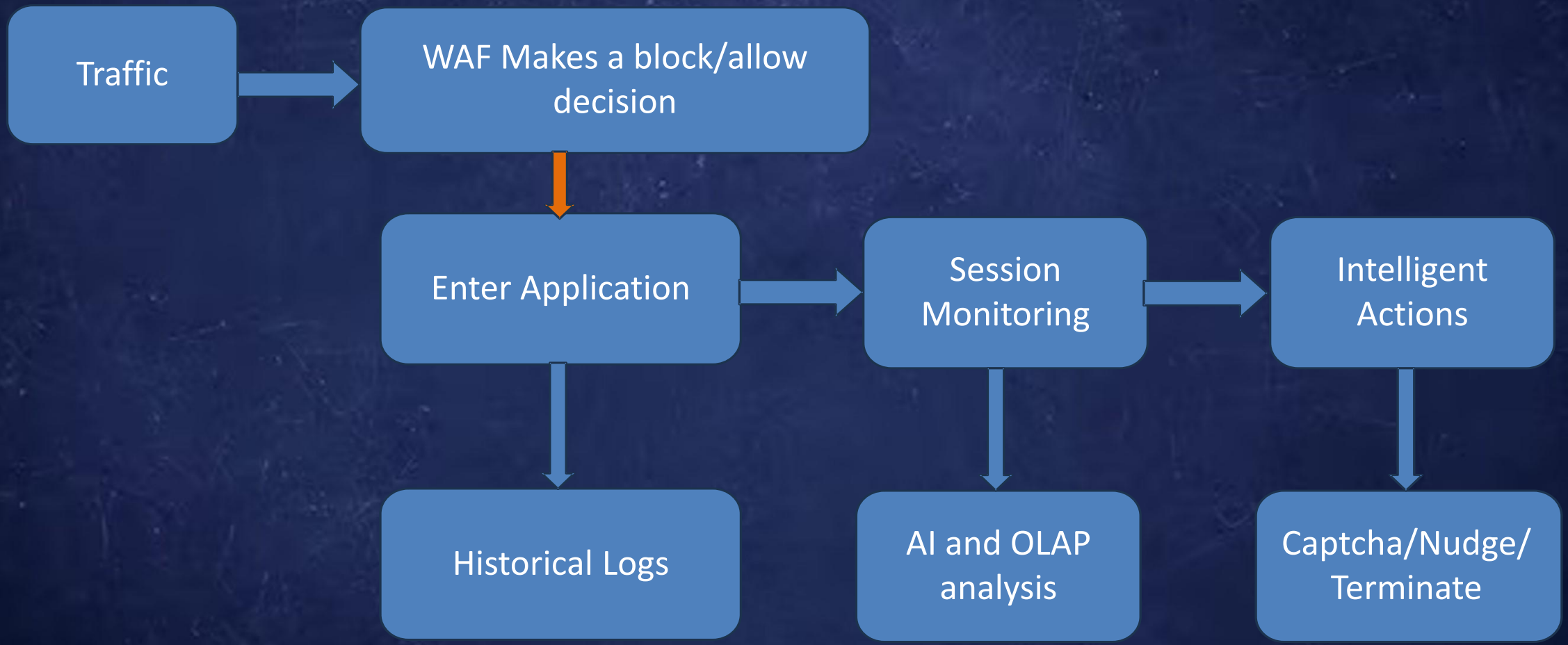
WAF ONLY ARCHITECTURE



TRAFFIC-PRISM ONLY (HOSTED WEBSITES)



WAF + TRAFFIC-PRISM ARCHITECTURE



APPENDIX C: Changes in CORS Headers

APPENDIX C: HEADER CHANGES		
Scenario	**Why WAF May Miss It**	**Why Bayesian Pl Platform Catches It**
User-Agent Changes Mid-Session	WAFs don't correlate changes across requests unless explicitly configured.	Tracks the session context and flags inconsistencies in User-Agent.
IP Address Changes Mid-Session	WAFs inspect individual requests, so IP changes within the same session are ignored.	Monitors session continuity and flags unusual IP transitions.
Anomalous Referer Header	WAF might miss subtle anomalies in legitimate-looking headers.	Correlates referer anomalies with navigation patterns and geographic inconsistencies.
Header Spoofing (e.g., X-Forwarded-For)	WAFs might allow spoofed headers if they look legitimate.	Detects inconsistencies between X-Forwarded-For and other session attributes.
Dynamic Header Updates by Bots	Bots mimic legitimate headers to bypass static WAF rules.	Identifies bots through timing anomalies and header inconsistencies over the session.

Case Study - Fashion Brand IP Protection

Challenge:

- Bot scraping attacks
- Targeted design theft
- Region-specific threats

Implementation:

- Session-layer controls
- Bot detection rules
- Geographic filtering

Results:

- Blocked malicious bots
- Protected designs
- Preserved IP assets

Case Study - Fintech Platform Security

Challenge:

- Suspicious regional access
- Reconnaissance attempts
- High-risk sessions

Solution:

- Session scoring
- Rule-based termination
- Geographic controls

Impact:

- Blocked high-risk sessions
- Reduced attack surface
- Enhanced security posture

XSS,CSRF, Clickjacking→Ransomware, RAT , APTs

Initial Access

- Use CSRF, open redirects, or clickjacking to direct users to malicious phishing or extension-installation pages.

Persistent Hook

- Once the browser extension is installed, it gains access to session data, DOM elements, and browsing activity.

Targeted Phishing

- The extension injects malicious URLs into the user's browser or hijacks search results for targeted phishing campaigns.

Reverse Browser Shell

- Malicious URLs can immediately establish a reverse session within the browser, capturing keystrokes and various browser-level data without the user being aware.
- This can exfiltrate Office 365 documents, ERP system access, credit card details, passwords, and much more.

System Reverse Shell

- This requires users to download attachments, such as a file disguised as .cert but actually being .exe, to establish a reverse system shell.

Case Study: APT41 and Similar Actors

Advanced Persistent Threat Tactics

- Documented use of browser automation tools

Target Critical Workflows:

- Application submission systems
- Document processing portals
- Financial transaction interfaces
- Administrative consoles

Why Traditional Security Fails

WAF Limitations:

- Cannot detect legitimate browser execution
- Misses session-level patterns
- Blind to user behavior context

Standard Security Gaps:

- No visibility into browser actions
- Cannot differentiate between automated and human interactions
- Missing cross-session correlation

WebSocket based Browser Reverse Shell- Capture Keystrokes

Initial Attack Vector

XSS Vulnerability Discovery:

- Leveraging tools like Nikto for automated XSS scanning.

Session Exploitation:

- Using Playwright/Selenium to automate browser mechanics and manipulate session behaviors.

Browser Hook Establishment:

- Employing browser extension frameworks to gain an initial foothold within the user's browser.

Escalation Path

Malicious Payload Delivery:

- Activated through browser hooks for precise targeting.

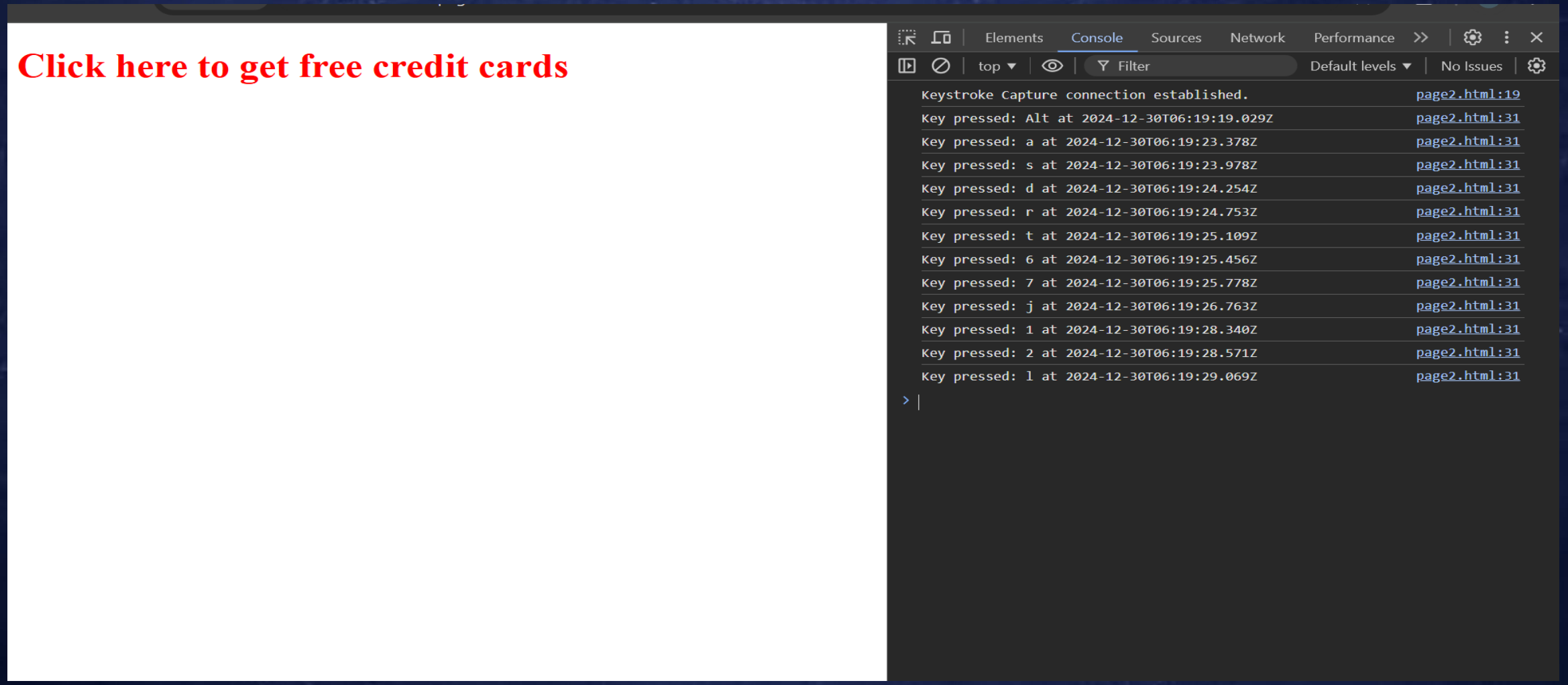
Reverse Session Establishment:

- Achieving WebSocket-based reverse sessions for real-time interaction, allowing immediate keystroke capture.

Lateral Movement Capability:

- Leveraging Command and Control (C2) infrastructure for pivoting deeper into the network.

WAF Can’t Detect Keystroke Capture with a Phishing Link



Keystroke Capture: Backend Capture

```
12|keystro | Received: {"key":"a","code":"KeyA","timestamp":"2024-12-30T06:14:37.329Z"}
12|keystro | Received: {"key":"s","code":"KeyS","timestamp":"2024-12-30T06:14:37.339Z"}
12|keystro | Received: {"key":"v","code":"KeyV","timestamp":"2024-12-30T06:14:37.711Z"}
12|keystro | Received: {"key":"Alt","code":"AltLeft","timestamp":"2024-12-30T06:14:38.513Z"}
12|keystro | Connection from ('103.177.175.203', 11519)
12|keystro | Received: Connected to reverse shell
12|keystro | Received: {"key":"Alt","code":"AltLeft","timestamp":"2024-12-30T06:16:53.141Z"}
12|keystro | Received: {"key":"a","code":"KeyA","timestamp":"2024-12-30T06:16:58.143Z"}
12|keystro | Received: {"key":"s","code":"KeyS","timestamp":"2024-12-30T06:16:58.258Z"}
12|keystro | Received: {"key":"d","code":"KeyD","timestamp":"2024-12-30T06:16:58.505Z"}
12|keystro | Received: {"key":"f","code":"KeyF","timestamp":"2024-12-30T06:16:58.729Z"}
12|keystro | Received: {"key":"Alt","code":"AltLeft","timestamp":"2024-12-30T06:16:59.177Z"}
12|keystro | WebSocket server running on ws://0.0.0.0:4444

12|keystroke_server  | Connection from ('103.177.175.203', 11591)
12|keystroke_server  | Received: Connected to reverse shell
12|keystroke_server  | Received: {"key":"Alt","code":"AltLeft","timestamp":"2024-12-30T06:19:19.029Z"}
12|keystroke_server  | Received: {"key":"a","code":"KeyA","timestamp":"2024-12-30T06:19:23.378Z"}
12|keystroke_server  | Received: {"key":"s","code":"KeyS","timestamp":"2024-12-30T06:19:23.978Z"}
12|keystroke_server  | Received: {"key":"d","code":"KeyD","timestamp":"2024-12-30T06:19:24.254Z"}
12|keystroke_server  | Received: {"key":"r","code":"KeyR","timestamp":"2024-12-30T06:19:24.753Z"}
12|keystroke_server  | Received: {"key":"t","code":"KeyT","timestamp":"2024-12-30T06:19:25.109Z"}
12|keystroke_server  | Received: {"key":"6","code":"Digit6","timestamp":"2024-12-30T06:19:25.456Z"}
12|keystroke_server  | Received: {"key":"7","code":"Digit7","timestamp":"2024-12-30T06:19:25.778Z"}
12|keystroke_server  | Received: {"key":"j","code":"KeyJ","timestamp":"2024-12-30T06:19:26.763Z"}
12|keystroke_server  | Received: {"key":"1","code":"Digit1","timestamp":"2024-12-30T06:19:28.340Z"}
12|keystroke_server  | Received: {"key":"2","code":"Digit2","timestamp":"2024-12-30T06:19:28.571Z"}
12|keystroke_server  | Received: {"key":"l","code":"KeyL","timestamp":"2024-12-30T06:19:29.069Z"}
```

How Do We Use Generative AI

- **Gen AI plays** crucial role in our platform mainly to calculate real time risk across sessions
- While OLAP rule-based system can score faster for historical patterns, it struggles for zero day or novel attacks. So, we use combination of Gen AI and OLAP for best of both worlds.
- Our AI models analyze session behavior patterns to predict potential threats with combined accuracy above 90%.
- Deployment on edge devices can be done using our specialized C++ interface, or a Python-based endpoint is also available.

AI Transparency

Proven Results

- Delivers actionable insights, protecting your business from sophisticated attacks.
- Decision engine powered by continuously updated threat intelligence and historical attack patterns.
- Augmented by OLAP.
- Enhanced detection rates for complex, multi-layered threats.

Seamless Integration

- Deploys effortlessly into your existing infrastructure with lightweight, scalable solutions.
- Fully compliant with GDPR, SOC 2 Type 2, and ISO 27001 standards.

Built for Business

- Transparency and accuracy drive better decision-making.
- No unnecessary tech jargon—just security that works for you.

Certificate of Registration

This is to certify that

BAYESIAN RESEARCH PRIVATE LIMITED

2nd, 22, 44-A, VRINDAVAN COMPLEX, MAJWADE, THANE - 400601,
MAHARASHTRA, INDIA

has been independently assessed by IAB accreditation and is compliance with the requirement of the standard

ISO/IEC 27001:2022

Information Security Management System

For the following scope of activities

SaaS Based Cyber Security Platform Mainly Focusing on Session Level Security using OLAP and Generative AI.

Certificate Number: IN19543

To verify this certificate please visit at www.uscertifications.uk

Date of Certification	19TH NOVEMBER 2024
Issuance Date	19TH NOVEMBER 2024
1st Surveillance Due	19TH NOVEMBER 2025
2nd Surveillance Due	19TH NOVEMBER 2026
Re-Certificate Due	19TH NOVEMBER 2027

Registered

ISO 27001

Authorized Signatory

CAB Address : Merry Terrace Woking, London FU21 3EH UK Validity of this certificate is subject to annualsurveillance audits to be done successfully This certificate is the property of U.S. Certification and shall be returned immediately on request U.S. Certification is an independent Systems Products and Personal assessment Body, U.S. Certification is a accredited by IABCERT.NU

MQA Certification

Certificate of Compliance

This is to certify that

BAYESIAN RESEARCH PRIVATE LIMITED

2ND, 22, 44-A, VRINDAVAN COMPLEX, MAJWADE,
THANE - 400601, MAHARASHTRA, INDIA

Has been assessed and certified by MQA Certification Services
As meeting the requirements of:

GDPR

(General Data Protection Regulation)

For the Following Scope of Activities:

SAAS BASED CYBERSECURITY PLATFORM MAINLY FOCUSING ON SESSION LEVEL SECURITY USING OLAP AND GENERATIVE AI

:: Certificate No. :: UG/24M05983

Date of initial registration:	**27 November 2024**
First Surv. Audit on or before:	**26 November 2025**
Second Surv. Audit on or before:	**26 November 2026**
Re-certification Due:	**26 November 2027**

This Certificate is property of MQA and remains valid
Subject to satisfactory surveillance audits.

Authorized Signatory
MQA CERTIFICATION SERVICES
130 Thessaly Rd, Nine Elms, London
SW8 5EJ, United Kingdom

UKAF-CB-011

To check validity of the certificate please visit at www.mqacertification.com

This certification of registration is issued by MQA Certification Services accredited with UKAF CERT LIMITED Accreditation Board for Certification Bodies (www.ukafcert.org.uk).This certificate remains the property of MQA Certification Services having and must be returned upon request.

MQA Certification

Certificate of Compliance

This is to certify that

BAYESIAN RESEARCH PRIVATE LIMITED

2ND, 22, 44 A, VRINDAVAN COMPLEX, MAJWADE,
THANE - 400601, MAHARASHTRA, INDIA

Has been assessed and certified by MQA Certification Services

As meeting the requirements of:

SOC 2 TYPE 2

For the Following Scope of Activities:

SAAS BASED CYBERSECURITY PLATFORM MAINLY FOCUSING ON SESSION LEVEL SECURITY USING OLAP AND GENERATIVE AI

:: Certificate No. :: UG/24M05892

Date of initial registration:	22 November 2024
First Surv. Audit on or before:	21 November 2025
Second Surv. Audit on or before:	21 November 2026
Re-certification Due:	21 November 2027

This Certificate is property of MQA and remains valid
Subject to satisfactory surveillance audits.

Authorized Signatory

Thank You