**Contextuele AI biedt preventieve bescherming van webapplicaties en API's tegen zero-day-bedreigingen**

Nu organisaties steeds afhankelijker worden van cloudtechnologieën, is de beveiliging van cloudplatformen een belangrijk punt van zorg geworden dat zowel hun potentieel als kwetsbaarheid benadrukt. Traditionele beveiligingsmaatregelen schieten vaak tekort in het aanpakken van de dynamische en geavanceerde aard van bedreigingen waarmee organisaties in cloudomgevingen worden geconfronteerd. Dit maakt het absoluut noodzakelijk om over te schakelen van een reactieve naar een preventieve houding in cloudbeveiligingsstrategieën. CloudGuard WAF (Web Application Firewall) gebruikt contextuele AI om webapplicaties en API's op een preventieve manier te beschermen tegen zero-day-bedreigingen.

**Meer grip op cloud security**
Indien er software in de cloudomgeving draait die kwetsbaar is door een erkende (zero day) kwetsbaarheid, zou dit de hoogste prioriteit en criticaliteitsstatus krijgen. Doordat de WAF-oplossing functioneert als de zogenoemde 'voordeur' van de cloudomgeving, zorgt deze ervoor dat er bescherming is tegen zero-day aanvallen, waaronder de betreffende kwetsbaarheid, zonder dat er gewacht hoeft te worden op een signature. Dit stelt organisaties in staat om de prioriteit en criticaliteit van incidenten met betrekking tot deze kwetsbaarheid te verlagen, waardoor er meer tijd en aandacht beschikbaar is voor overige, meer kritieke incidenten. Voor organisaties met een complex cloudlandschap, waar het aantal incidenten aanzienlijk kan oplopen, is dit van onschatbare waarde. Maar ook voor kleinere organisaties en organisaties zonder toegewijde cloud security-teams biedt deze aanpak grote voordelen.

**Cloud security innovatie**
CloudGuard WAF van Check Point is een krachtige, innovatieve, unieke en veelzijdige oplossing voor webapplicatie- en API-beveiliging. Naast de overal deploybare agent versie biedt Check Point de WAF-oplossing sinds april van 2024 ook in SaaS-vorm aan. De oplossing onderscheidt zich door:

1. **Machine learning**: Het maakt gebruik van een gepatenteerde machine learning-engine die continu HTTP/S-verzoeken analyseert om patronen te identificeren en automatisch kwaadaardige verzoeken te blokkeren.
2. **Bescherming tegen Zero-Day aanvallen**: CloudGuard WAF biedt pre-emptieve bescherming tegen zero-day aanvallen zoals Log4Shell en Spring4Shell, zonder dat software-updates nodig zijn.
3. **API-beveiliging**: Het detecteert automatisch API-gebruik en gevoelige inhoud, en biedt beveiliging door zichtbaarheid en handhaving van API-schema’s.
4. **Bot preventie**: Het identificeert en stopt geautomatiseerde aanvallen voordat ze een negatieve impact hebben op de bedrijfsvoering of klantervaring.
5. **Integratie**: CloudGuard WAF kan naadloos worden geïntegreerd met verschillende cloudplatforms en derde-partij applicaties, wat het geschikt maakt voor multi-cloud omgevingen zoals AWS, Azure en Google Cloud Platform.
6. **Gebruiksvriendelijke beheerconsole**: Een gecentraliseerde console vereenvoudigt het beheer en verbetert de zichtbaarheid door de controle van dreigingsbescherming en zelfinspectie over applicaties te stroomlijnen.

**WAF Comparison Project**
Een open-source versie is voor iedereen beschikbaar om te gebruiken, verkennen en testen. Meer informatie (incl. een 2 min. instructievideo): [open-appsec | Automatic Open Source WAF & API Security (openappsec.io).](https://www.openappsec.io/) Hier kan tevens kennis gemaakt worden met het **Check Point WAF Comparison Project.** Dit is een initiatief, inclusief een praktisch framework, voor het testen en vergelijken van de effectiviteit van verschillende Web Application Firewalls (WAF’s). Dit comparison project maakt gebruik van datasets en tools om de prestaties van WAF’s te evalueren op twee belangrijke gebieden:

* **Security Coverage (True Positive Rate)**: Dit meet de capaciteit van een WAF om kwaadaardige verzoeken correct te identificeren en te blokkeren. Dit is cruciaal in het huidige dreigingslandschap, omdat het zowel zero-day aanvallen als bekende aanvalstechnieken moet kunnen afweren.
* **Precision (False Positive Rate)**: Dit meet de capaciteit van een WAF om legitieme verzoeken correct toe te staan. Onterechte blokkeringen van legitieme verzoeken kunnen leiden tot bedrijfsverstoringen en een verhoogde werklast voor beheerders.

Dit WAF comparison project biedt een gedetailleerde methodologie en tools om deze tests uit te voeren, inclusief datasets van zowel legitieme als kwaadaardige HTTP-verzoeken, afkomstig uit real-world scenario’s.

**Praktijkverhaal: Digitale activa van financiele dienstverlener beschermt tegen zero-day**
BBVA, een grote Spaanse multinationale financiële dienstverlener, heeft zijn web- en API-beveiliging versterkt door gebruik te maken van Check Point’s CloudGuard Web Application Firewall (WAF). Het bedrijf stond voor verschillende uitdagingen: de noodzaak om een uitgebreid netwerk van diensten, applicaties en API’s te beschermen, een behoefte aan betere zichtbaarheid en eenvoudiger beheer ter ondersteuning van hun ontwikkelings- en CI/CD-automatisering, en de vereiste om zich te verdedigen tegen zero-day bedreigingen en de OWASP (Open Worldwide Application Security Project) top 10 kritieke kwetsbaarheden.

Om deze uitdagingen aan te pakken, besloot BBVA Check Point’s CloudGuard WAF te implementeren. Deze oplossing bood preventieve bescherming door middel van machine learning-gebaseerde beveiliging die niet afhankelijk is van signatures, wat essentieel was voor het verdedigen tegen zero-day aanvallen. Daarnaast zorgde de WAF voor verbeterde zichtbaarheid en eenvoudiger beheer via een enkel dashboard, wat gedetailleerd inzicht gaf in de workloads en API’s. Ook bood het naadloze integratie met cloudserviceproviders zoals Azure, AWS, GCP en Oracle OCI, evenals met CI/CD-processen.

De implementatie leverde verschillende positieve resultaten op. BBVA’s diensten en applicaties zijn effectief beschermd tegen zero-day aanvallen, waaronder de beruchte Log4J-kwetsbaarheid. De operationele efficiëntie is aanzienlijk verbeterd door eenvoudiger beheer en bredere zichtbaarheid, waardoor de behoefte aan constante afstemming en updates afnam. Bovendien kon BBVA zijn diensten en applicaties wereldwijd veilig uitbreiden zonder zich zorgen te maken over beveiligingsinbreuken en zero-day exploits.

Deze case study illustreert hoe BBVA geavanceerde beveiligingsoplossingen heeft ingezet om zijn digitale activa te beschermen en zijn operationele processen te optimaliseren