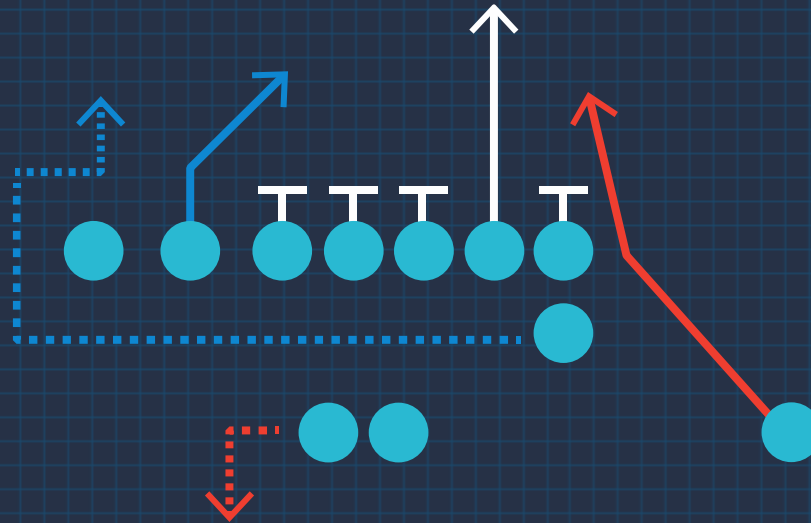


APPLICATION + CLOUD SECURITY

SALES PLAYBOOK



Secure Your Application and Cloud Journey

Contents

- ★ Market Overview
- ★ Customer Context
- ★ Solution Overview
- ★ Competitive Scouting Report
- ★ Top Plays and Landing Zones
- ★ Resource Index



Market Overview

AppSec Market

(Source: Gartner, G00385344)

\$3.4B

Market in 2019

\$12.1B

Projected market in 2025

Breaches Worldwide

(Source: Verizon DBIR 2021)

95%

Web Apps as hacking vector in breaches

Merging Categories

WAF + DDoS + Bot + API =

WAAP

(Web App & API Protection)

WAAP Protected

(Source: Gartner, G00382805)

10%

of apps
in 2019

30%

of apps
in 2023

Global IT Leaders

(Source: Barracuda*)

72%

admit that their web apps were hacked
at least once in the last 12 months

Top AppSec Challenges

(Source: Barracuda*)

43%

Bot Attacks

39%

Supply Chain Attacks

37%

API Attacks

* The state of Application Security in 2021, May 2021

Evolving Threat Environment

Digital Transformation and Agile

- Digital transformation accelerated by COVID-19 pandemic
- Agile, DevOps/SecOps, CI/CD
- Security is “shifting left”, now part of the development cycle
- AppSec is critical but can be seen as a speed bump in fast release cycles

Web App and API Vulnerabilities

- Application vulnerabilities are different from network vulnerabilities – NG firewalls don't protect
- App vulnerabilities are a function of the way apps are built and patched
- Attacks can be manual or automated
- New attack vectors and vulnerabilities pop up every day

Threats from Automated Attacks (Bots)

- Automated attacks by bots are growing at an increasingly rapid pace
- Bots are used to perform mass attacks against tens of thousands of sites at one go
- Bots are increasingly more intelligent and bypass standard defenses like reCAPTCHA

Web Application and API Protection (WAAP)

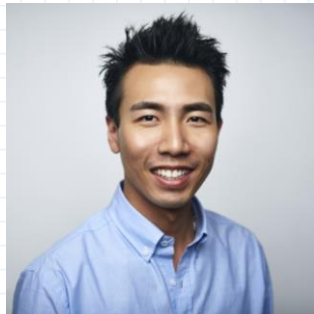
- Expansion and consolidation - Bot Protection, DDoS Protection, API Security, Fraud Prevention
- Customer preferences shifting to SaaS offerings - SaaS is seen as solving the problems of speed and ease-of-use

Target Personas



Application Security Manager / Director

- Typically present in larger organizations
- May be part of a larger (network) security team, application team or DevOps/SecOps team
- Willing to learn and use a WAF
- May have religion due to previous experience (Imperva, Fortinet, F5, etc - expect questions about how we compare)



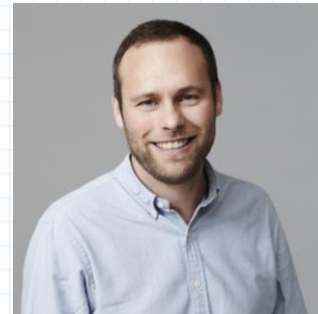
Developer/ Dev Manager / Dev(Sec)Ops

- Believe that security processes slow them down, WAF's will break their applications
- Automation of deployment, usage of scanners for virtual patching, feedback loops are important
- Dev(Sec)Ops: Speed of deployment and configuration are among the most important considerations for these teams



Security Manager / Director

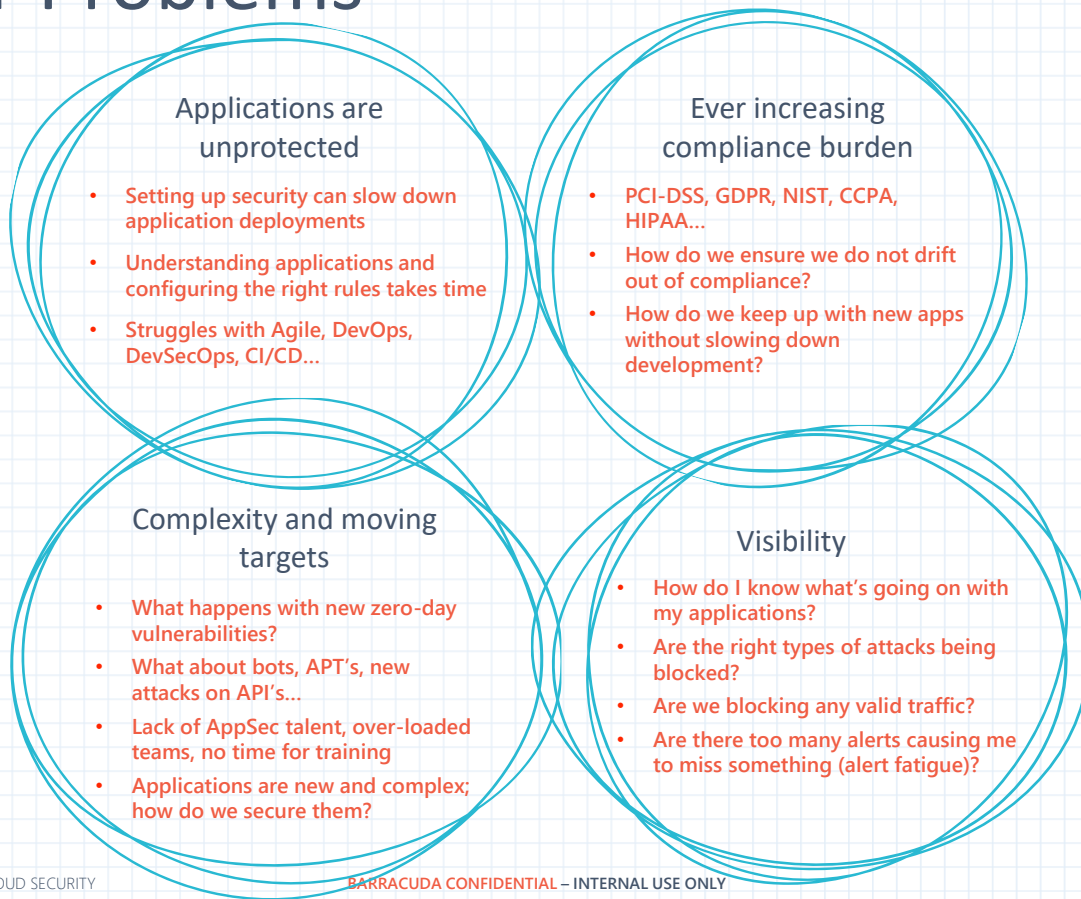
- Need to see proof that their firewall cannot stop the attacks
- Tend to have religion (Fortinet, Cisco etc..)
- See WAF as a burden
- How do we integrate it in our security stack? It is too complex, we don't have sufficient knowledge



CIO / CTO / CISO / IT Director

- Can be a champion and actual decision maker
- Tend to have religion (F5, Akamai, Fortinet), based on previous experiences
- RFP driven in larger organizations

Customer Problems



Solution Requirements



Reduce complexity

- Deployment complexity
- Management complexity



Provide more than a WAF

- Scanning & remediation
- DDoS, bot, API protection



Use platform approach

- Integrate all components
- Provide as simple solution

Cloud Application Protection (CAP) 2.0

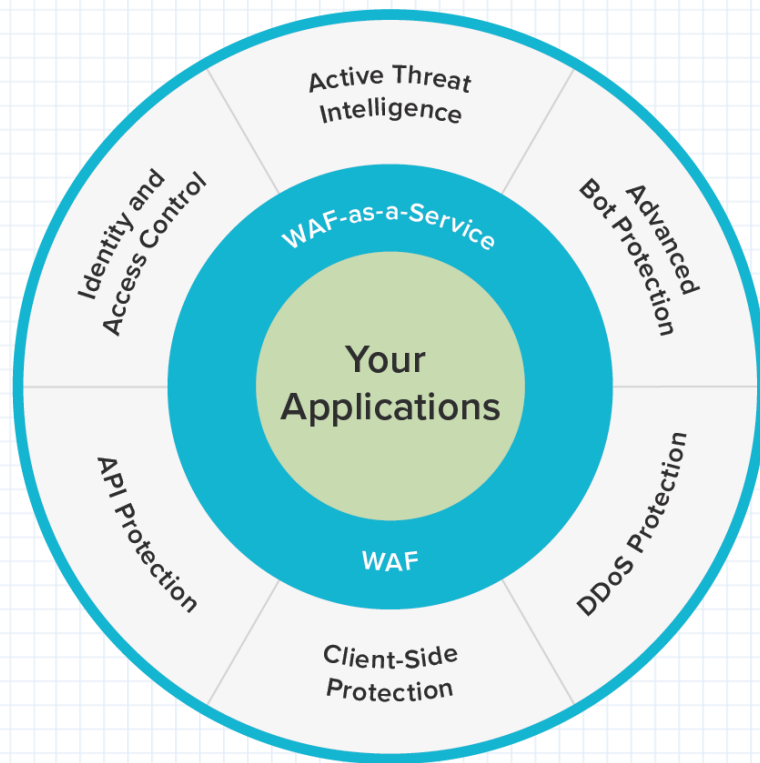
Comprehensive application security platform

Protection wherever you are in your journey

- Single hosted website to hundreds (sometimes thousands) of apps
- Data center or hybrid
- Public cloud, microservices, serverless

Easy to use and deploy

- From SMBs to Fortune 100 enterprises
- Auto-Configuration Engine to automatically fine-tune your configuration
- Flexible deployment options



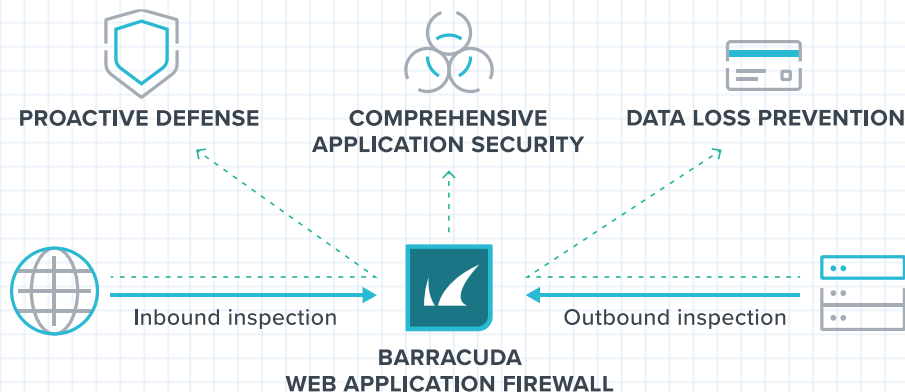
CAP Components

Barracuda Web Application Firewall

- Comprehensive Application Security: OWASP Top-10 attacks and more, XML and JSON protection; application DDoS protection, bot protection
- Proactive Defense: Geo IP control, reputation lists
- Data Loss Prevention: credit card numbers; social security numbers; custom policies

Barracuda WAF-as-a-Service

- Built on the same proven technology
- 5-step setup wizard adds protection in minutes
- Intuitive structure for fine-tuning policies
- Fully featured REST API
- Unmetered DDoS protection included
- Automated vulnerability identification/ remediation
- Deploy as-a-Service or as containers within your environment



CAP Components (continued)

Active Threat Intelligence

Cloud-based Machine Learning enabled Threat Intelligence to identify and block emerging threats in near-real time

- Encompasses
 - Barracuda Vulnerability Manager and Remediation Service,
 - Barracuda Advanced Threat Protection
 - Barracuda Advanced Bot Protection's Cloud ML Layer
 - Auto-Configuration Engine

Client-Side Protection

Stops browser-side attacks and website supply chain attacks that other WAFs cannot

- Auto-configuration of CSP and SRI settings for ease of use
- Cloud Dashboard to provide deep visibility into the status of third party scripts and their usage/changes

Advanced Bot Protection

- Protection from OWASP automated threats
- Defense against advanced bots
- Multi-layer approach for advanced protection

API Protection

Supported API types

- XML Web Services
- JSON APIs
- RESTful Web Services
- OpenAPI Support

API Discovery for ease of use and configuration

DDoS Protection

- Always-on DDoS prevention solution
- Prevents volumetric DDoS attacks from reaching your applications
- Included with WAF-as-a-Service/available with WAF

Identity and Access Control

Supported identity services

- LDAP
- RADIUS
- Kerberos
- MFA
- SAML & Oauth/JWT

Delivering Value with Barracuda CAP

Powerful protection

- Comprehensive, multi-layered application protection
- Compliance enabler
- Deep visibility

Easy to use

- Built-in ease-of-use functionality
- Virtual patching and feedback loops
- 3rd party integrations for SIEM, scanners and authentication mechanisms

Protect any app env

- Fully automated deployment
- Protect applications anywhere they are deployed
- Secure application delivery
- Cloud native platform

Customer Benefits

✓ Comprehensive Security

- Cover every type of application – web, mobile, API
- Secure against all advanced application threats and unknown zero-day vulnerabilities
- Full spectrum DDoS prevention and file upload security in a single solution

✓ Ease of Use and Flexibility

- Set it and forget it or go deep into the configuration
- Ease of use features built with admin in mind (fix config from logs, exception profiling, etc.)
- Configure on one platform, move to any other (WAF to CGWAF to WaaS)
- Near native integration with AWS, Azure and GCP

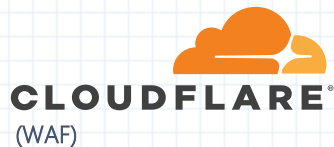
✓ Move Fast, Securely

- Fully automatable with REST API
- Get up and running in a matter of minutes
- Virtual patching and automated configuration for DevOps/SecOps and agile deployments
- Content routing enables deployment methods like A/B testing, Canary/Blue Green rollouts etc.

✓ Well-integrated with allied solutions

- SIEM integrations for visibility (Splunk, Azure Log Analytics, Sumologic & more)
- Authentication integrations for AAA offload (LDAP, SAML, RADIUS, OpenID Connect; 2FA and SSO integrations)
- Scanner integrations for virtual patching (25+)
- Automation tools integrations (Puppet, Terraform, CloudFormation & more)

Competitive Scouting Report



Product Focus

- Started as a CDN & DDoS protection
- Positioning as WAF & bot protection

Competitive Positioning

- Limited WAF, not fully customizable
- Missing many features compared to our WAF: not easy to tune, no file upload security, limited rules based on subscription
- Gets expensive very fast, e.g. DDoS protection is expensive
- Frequently see vulnerabilities published for the WAF rules



Product Focus

- Formerly known as Incapsula
- Originally a CloudFlare competitor with a \$25 plan - now an enterprise-targeted solution

Competitive Positioning

- Limited WAF, not fully customizable
- We beat them in multiple cases as they charge extra for many features
- Missing many features compared to our WAF: not easy to tune, no file upload security, limited number of rules based on subscription



Product Focus

- Hosted on AWS
- Their version of the Barracuda WAF-as-a-Service; uses Fortiweb on the backend

Competitive Positioning

- No Advanced Bot Protection equivalent
- A number of features and the UI are inspired by Barracuda WAF-as-a-Service
- No ease-of-use features for configuration tuning
- No file upload security

Competitive Scouting Report (continued)



(SecureSphere)

Product Focus

- Original product from Imperva
- In heavy use by large enterprises

Competitive Positioning

- Expensive and complex to setup
- Limited API protection
- No file upload protection
- Needs expensive license for bot protection
- Needs a lot of work to get it working in the public cloud
- Missing many features that we have



(Advanced WAF & ASM)

Product Focus

- Pivot from the ADC world
- Focus on bot protection and mobile

Competitive Positioning

- Expensive
- Complex to set up and manage
- Often requires admin to be a programmer
- No Machine Learning for bot protection
- No built-in file upload protection



(FortiWeb)

Product Focus

- Their WAF for Fortinet customers
- Not a focus product, used competitively with large discounts

Competitive Positioning

- Incomplete product
- Missing API protection
- File upload security requires FortiSandbox
- Built-in Machine Learning functionality is limited
- Look out for deep discounting

Landing Zones

Web Application Security (Basic)	Web Application Security (Public Cloud)	DDoS Protection
Advanced Bot Protection	API Security	Regulatory Compliance



Landing Zone: Web Application Security (Basic)



Web Application Security (Basic)



Use Case

- Every website needs to be secure
- OWASP Top 10 threats (SQL Injection, XSS, etc.)
- As sites are updated, newer vulnerabilities emerge (zero-day threats, etc.)
- HTTPS is essential, but can be painful to implement



Pain Points

- Breaches (fines, reputation damage, loss of jobs)
- DDoS can bring down the business
- Common website framework vulnerabilities (WordPress, Drupal)
- Websites can be hacked and then used to attack others; site may be marked as unsafe on browsers



Discovery Questions

- How do you secure your site? When was it last updated?
- Do you have forms on your site? How do you protect form fills?
- Want to run a free scan to see how secure your website is?
- Accept file uploads on your website? How do you secure against malware?
- I see your website uses HTTP – interested in converting it to secure HTTPS with a free cert?
- Have you recently put internal apps on the Internet or on VPN due to Covid? How do you secure them?

Web Application Security (Basic)



Solution Pitch

- Easy to deploy and manage
- Solve complex problems in minutes (especially WAF-as-a-Service)
- Convert aging websites into secure solutions without a massive overhaul
- Unlimited DDoS Protection with WAF-as-a-Service
- BVRS to continually scan and remediate without much effort
- Award winning support



Competitive Positioning

- Use BVM/BVRS to your advantage in the sales cycle (similar to ETS)
- Full AppSec platform, not just a WAF
- Especially in SMB and local government, emphasize our award-winning support



Objection Handling

- **"We don't see a need to secure our website."**
Offer a free BVM scan to see how secure the website really is
- **"We have an NG/UTM."**
These don't protect against application attacks. Offer a BVM scan for this.
- **"We don't have the people to do this."**
WAF-as-a-Service can be setup in minutes and doesn't require in-depth knowledge.

Win Analysis

Pain Points

- Public facing web applications needed security
- Existing vendor (Imperva Cloud WAF) was not blocking all attacks
- Need ease of use, without compromising security

Solution

Barracuda WAF-as-a-Service

- Quick 5 step deployment
- Complete control for fine tuning security

Results

- Solution set up & running in 10 min.
- All applications secured without any compromises
- Ease of use and full control makes admin happy



Provides construction and facility maintenance solutions

Landing Zone: Web Application Security (Public Cloud)



Web Application Security (Public Cloud)



Use Case

- Protect web applications on Azure, AWS and GCP
- Automatic scaling to handle load as traffic increases
- Ensure application performance and security in the public cloud



Pain Points

- Shared responsibility model* for cloud security is misunderstood, leading to lack of security
- App vulnerabilities follow apps to the cloud
- Compromised apps can be used to go deeper into cloud deployment – lateral movement
- Security can hamper deployments
- On-premises security usually doesn't work in the cloud



Discovery Questions

- What workloads are you running in the public cloud today?
- Are you planning to lift-and-shift apps to the public cloud? How will you secure them?
- Do you have concerns about the performance and availability for apps running in the cloud?
- How well do you understand the shared responsibility model?
- Have you had issues securing apps in the public cloud before?

* Shared responsibility model for cloud security:

Cloud provider responsible for "security of the cloud"; customer responsible for "security in the cloud"

Web Application Security (Public Cloud)



Solution Pitch

- Easy to deploy and manage
- Cloud Native feature set, complete automation
- Single architecture secures many apps – set it and forget it
- AWS Security Competency certified
- First security solution on Azure
- BVRS to continually scan and remediate without much effort
- Award winning support
- Flexible subscription models



Competitive Positioning

- Barracuda customer running over 4,000 WAF's on AWS (Fortune 100 financial services company)
- Imperva is difficult to deploy and tries to replicate on-prem model to cloud
- F5 is big, complex and difficult to operationalize
- Azure WAF is limited and does not provide full WAF security
- AWS WAF is complicated and requires a lot of work to operationalize



Objection Handling

- **"Cloud is secure by default."**
This is not what the shared responsibility model* means
- **"We use the Azure WAF/AWS WAF."**
Neither are full fledged solutions that provide actual app security to your apps
- **"I'm using the same solution as on-premises."**
These typically don't work in the cloud, and there are new types of vulnerabilities

* Shared responsibility model for cloud security:

Cloud provider responsible for "security of the cloud"; customer responsible for "security in the cloud"

Win Analysis

Pain Points

- Need to protect public cloud hosted applications (Azure)
- Uneven levels of demand throughout the year
- Highly sensitive data

Solution

Barracuda CloudGen WAF for Azure

- On-demand scalability
- Maximized uptime
- Security and compliance

Results

- All applications secured without any compromises
- Handled by their existing security team



Provides benchmarking and diagnostic assessments to UK schools



“With Barracuda, we are able to extend our business on a global scale without employing a team of thousands of IT employees. Barracuda allows us to manage our infrastructure much more easily and enables us to punch above our weight.”

– D. Glover, Digital Director

Landing Zone: DDoS Protection



DDoS Protection



Use Case

- Protection against DDoS attacks that can bring the application down
- These attacks sometimes come with a ransom
- Need to protect against DDoS and application attacks



Pain Points

- DDoS attacks are increasing at a rapid rate*
- Attacks are being used to extort ransom
- Popular DDoS mitigation platforms do not have proper WAF's
- DDoS protection gets expensive fast based on usage



Discovery Questions

- Are you worried about DDoS attacks?
- Are you aware that people are getting ransom notes from DDoS attackers?
- Do you know about application DDoS attacks, and the difference from network DDoS attacks?
- Did you know that DDoS attacks are used as a cover for other hacks?

* DDoS Attacks Skyrocket as Pandemic Bites:
<https://threatpost.com/ddos-attacks-skyrocket-pandemic/159301/>

DDoS Protection



Solution Pitch

- Simple, easy to use and deploy
- Blocks all types of DDoS – not only volumetric
- Unlimited DDoS protection
- Azure native DDoS protection for WAF-as-a-Service
- Easy to use solution for both web attacks and DDoS
- Can configure WAF-as-a-Service in monitor-only mode and simply block DDoS attacks



Competitive Positioning

- Most WAF vendors do not offer an unlimited/reasonably priced DDoS protection service
- Vendors like CloudFlare charge based on DDoS throughput
- Look for smaller organizations with this positioning



Objection Handling

- **"We don't need a WAF, only a DDoS solution."**
Basic WAF-as-a-Service plan has unlimited DDoS protection
- **"It will be difficult to set up and manage."**
WAF-as-a-Service can be set up in minutes and doesn't require constant maintenance
- **"We already have the basic CloudFlare plan."**
Walk away, we can't beat this price

Win Analysis

Pain Points

- Massive DDOS attacks followed by ransom
- Critical public-facing services were taken down
- Attackers kept coming back at unpredictable times – sometimes after weeks of no attacks

Solution

Barracuda WAF-as-a-Service

- Full Spectrum DDoS Protection
- Unlimited DDoS Protection
- Quick and easy to deploy
- WAAP features helped detect and block application attacks

Results

- Application uptime and availability was increased
- Multiple Vol. DDoS attacks were mitigated successfully
- Other, previously unknown attacks were seen, and quickly blocked

Anonymous Public Library

Current Barracuda Customer
Multi-branch library system in the USA

Landing Zone: Advanced Bot Protection



Advanced Bot Protection



Use Case

- Protect against bots that attack all types of web sites
- All verticals: web scraping, denial of service, account takeover, credit card fraud
- Retail vertical: price scraping, listing scraping, scalping, inventory hoarding, denial of service, account takeover, credit card and related fraud



Pain Points

- Account Takeover attacks, stealing accounts of paying customers
- Sudden increase in payment failures
- Competitors suspiciously able to undercut pricing on website
- Marketing-led complaints about the website (e.g. website is slow, lots of form spam on registrations)



Discovery Questions

- How do you protect your e-commerce storefront from fraud?
- Your site has a login for suppliers/customers/partners. How is it protected from account takeover attacks?
- You collect payments on your site – have you run into problems with carding or other fraud?
- Do you get a lot of spam on your contact forms?

Advanced Bot Protection



Solution Pitch

- Single solution for AppSec and Advanced Bot Protection
- Cloud based machine learning layer that crowd sources bot intelligence to block almost-human bots
- Easy to set up and operationalize
- Award winning support



Competitive Positioning

- Imperva is expensive and complex/difficult to operationalize (we have replaced them in some accounts due to this)
- F5 has limited capabilities – its protection is all on-box, no cloud based machine learning
- PerimeterX is a bot mitigation company trying to be a WAF



Objection Handling

- **“We make our users change passwords frequently, not worried about account takeover.”**
This does not stop password re-use, and these could be previously compromised
- **“We use reCAPTCHA.”**
reCAPTCHA is easily bypassed using commercial and free tools

Win Analysis

Pain Points

- Large amount of automated traffic that caused website slowdowns
- Bots scraping online stores for inventory lists and prices (fake items sold elsewhere at lower prices)
- reCAPTCHA was unable to block these bots (creating pain for actual human customers)
- Existing solution was expensive and complex to use

Solution

Barracuda CloudGen WAF for Azure

- Identified the actual bots hiding in their traffic
- Helped them set up and monitor Advanced Bot Protection trial on the CGWAF
- Proved that we could catch bots better than reCAPTCHA

Results

- Many hidden valid bots are blocked with ease
- Customers are happy due to reduced reCAPTCHA
- Admin burden reduced drastically

Anonymous Online Retail

Current Barracuda Customer

Provides e-commerce platform for over 400 educational institutions

Landing Zone: API Security



API Security



Use Case

- APIs are becoming a massive attack vector and need to be secured
- Apps are increasingly using APIs to provide features at a faster pace – and these need to be secured



Pain Points

- Understanding API security – it is still early days
- Implementing API security – many competing solutions, adding to admin burden
- API security attacks can expose app and data directly and result in breaches causing significant damage
- Easier for bots to attack and wreak havoc



Discovery Questions

- How do you secure your APIs?
- Do you have a mobile application?
How do you secure its API?
- Do you deploy any Single Page Apps*?
How do you secure them?

*** Single Page Application:**

A Single Page Application is an app that works inside the browser and does not require page reloading during use.
Eg: Gmail, Google Maps, Facebook

API Security



Solution Pitch

- Easy to set up and operationalize API security
- Complete protection for JSON and XML APIs
- API discovery for ease of configuration
- Content routing for easy API delivery
- Caching and compression for faster API delivery
- Detailed logging and reporting for audit



Competitive Positioning

- Ease of use and operationalization
- Award winning support
- Improved visibility into configuration and traffic
- Advanced Bot Protection to protect against any bot attack
- Imperva – does not have a full API security solution
- F5 – complex, painful to operationalize
- Fortinet – limited feature set, especially with bot protection



Objection Handling

- **“We already use an API Gateway”**
API Gateways are more for API delivery, not security
- **“It is too complex for my IT person.”**
API discovery provides you with easy to use configuration wizards to set up API security

Win Analysis

Pain Points

- Large API-based systems that need protection
- Attacks included bots that were scraping this information for profit
- Denial of Service attacks that reduced accessibility of data
- Application slowdowns due to the above
- Attacks against the API itself, to exfiltrate large amounts of data

Solution

Barracuda WAF Vx

- Quickly imported the API definition files and configured the API firewalls
- Detected and blocked bots attacking the system
- Tar pitted abusive clients, reducing denial of service attacks
- Improved application SLA's with traffic management features

Results

- Easy configuration and management of API security with definition file import
- Application performance increased significantly
- Hidden attacks were detected and blocked, leading to a safer experience
- Tarpitting feature helped manage abusive clients
- Content Routing features enabled faster deployment of new API versions

European Govt. Agency

Provides public GIS data via API's

Landing Zone: Regulatory Compliance



Regulatory Compliance



Use Case

- Every organization needs to comply with some regulations (see upcoming table slide)
- Non-compliance can lead to massive fines
- Internal compliance requirements can be more stringent than external ones



Pain Points

- Staying in compliance – how do we stay in compliance, once the solution is set up?
- Breaches result in large fines and job and reputation loss
- Internal compliance needs can be higher than those from regulation



Discovery Questions

- Do you collect any personally identifiable information (PII)? Are you worried about breaches and fines?
- I see that you are in <industry>. How are you complying with <list of regulations>?
- Do you have internal compliance needs for your applications?

Regulatory Compliance



Solution Pitch

- Easy to set up and operationalize security
- Built-in reporting for PCI-DSS compliance
- Detailed logging and reporting for audit
- Virtual patching for automated compliance
- Data Leak Prevention (DLP) and file upload security to protect against PII leakage and complex malware (e.g. APTs) in file uploads



Competitive Positioning




- Ease of use and operationalization
- Award winning support
- Improved visibility into configuration and traffic
- ATP for file upload protection
- Advanced Bot Protection to prevent account takeover attacks – stop data breaches
- Free BVRs for virtual patching and integrations with over 20 external scanners



Objection Handling

- **“We already have an NG Firewall.”**
These cannot protect you from application attacks and may not qualify for compliance
- **“We have a UTM.”**
UTMs are not built to protect against web attacks, and turning on the WAF module will reduce performance
- **“It is too complex for my IT person.”**
WAF-as-a-Service can be set up in minutes, and our award-winning support has your back

Compliance Regulations and Verticals

REGULATION	VERTICAL	WHERE WE HELP
PCI-DSS	Any website that collects payments, but primarily online Retail/ e-commerce	Compliance with Section 6.6, where WAF is specifically mentioned; Compliance reports for ease of use 
HIPAA	Healthcare, primarily in the US	HIPAA requires compliance with NIST 800-52 standards – we can help with this 
NIST	Primarily US Federal, State and Local Government Standards are used as a base by many industries.	We can help enforce application protection and encryption standards defined by NIST
GDPR, CCPA, PDPA etc	Personal data protection and privacy regulations that apply across industries	Block attacks that can result in loss of PII, and help with compliance
FISMA	Primarily US Federal, State and Local Gov. and related entities	NIST 800-53 standards are developed based on this act 
SANS 20 Critical Security Controls (20CSC)	Primarily US Federal, State and Local Government and related entities	Baseline of 20 controls that help with FISMA compliance
Banking Regulations	Financial industries in various countries have their own regulations	Help comply with application security parts of these regulations

Win Analysis

Pain Points

- Secure patient data for regulatory compliance purposes HIPAA
- Provide protection for new patient web applications
- Looking for a solution aligned with Microsoft Azure
- Ease of deployment and ongoing use

Solution

Barracuda CloudGen WAF for Azure

- On-demand scalability
- Security
- Compliance

Results

- Added a layer of protection on top of Barracuda CGF on Azure
- Protection for sensitive web and mobile apps
- Deep visibility into application traffic
- Protection without any adverse effects on performance



Large private healthcare system based in the US



“We wanted to have the highest level of security and privacy for our patients. That led us to see how we could complement what Azure offers with additional security through Barracuda CloudGen WAF.”

– Dr. Ashish Atreja, Chief Technology, Innovation and Engagement Officer

Resource Index



Analyst Feedback

Gartner WAF Magic Quadrant 2021

- Part of the **Challenger Quadrant**
- "Barracuda WAAP management portal offers easy and modular administration capabilities with multiple built-in features, hidden until used. Features such as validating false positive alerts from the logging interface make fine tuning easier. It also comes with a mature risk scoring feature offering the option to customize risk levels and threshold values."
- "Customers often score the vendor high for its easy onboarding process. They have also rated the ability to create custom roles as easy to select and configure."

Forrester Wave 2019

- Part of the **Strong Performer Wave**
- "Barracuda's reference customers praised the WAF as offering good value for the price, appreciated the ease of use, and noted recent improvements in logging"
- "Given the company's focus on the CloudGen and SaaS WAF products, customers looking for a public cloud deployment option should consider Barracuda."

Cloud Application Protection (CAP)



Overview Video

A short video overview of Barracuda Cloud Application Protection

CloudGen WAF



Datasheet (AWS)

Datasheet for CloudGen WAF on AWS



Datasheet (Azure)

Datasheet for CloudGen WAF on Azure



Datasheet (GCP)

Datasheet for CloudGen WAF on Google Cloud Platform

WAF-as-a-Service

Quick Demo (right)

A short demo video that demonstrates the easy setup of WAF-as-a-Service



Overview Video

Video introduction to the Barracuda WAF-as-a-Service



Datasheet

Datasheet for Barracuda WAF-as-a-Service

The screenshot displays the Barracuda WAF-as-a-Service dashboard. The top navigation bar includes the WAF logo, account name 'Barracuda WAF-as-a-Service', and user information 'Account: Barracuda (default account)' and 'trichabadaa@barracuda.com'. The main navigation menu has tabs for APPLICATIONS, REPORTS, RESOURCES, and AUDIT LOGS. The APPLICATIONS tab is active, showing a search bar and an 'ADD APPLICATION' button. Below is a table with the following columns: NAME, DNS CONFIGURATION, SERVER STATUS, BLOCK ATTACKS, and ACTIONS. The table contains one entry for 'DVWA' with the following details: DNS CONFIGURATION is 'Update Pending', SERVER STATUS is 'Checks Off', and BLOCK ATTACKS is a toggle switch set to 'YES'. The footer of the dashboard includes the serial number 'Serial Number: BAR-WF-DEV', version 'Version: WAFaaS 2020.8', a link to the 'Privacy Policy', and copyright information '© 2020 Barracuda Networks, Inc. All rights reserved.' The Barracuda logo is in the bottom right corner.

NAME	DNS CONFIGURATION	SERVER STATUS	BLOCK ATTACKS	ACTIONS
DVWA	Update Pending	Checks Off	YES	

Web Application Firewall



Overview Video

Quick introduction video the Barracuda Web Application Firewall



WAF and CGF

How the Barracuda WAF and CGF complement each other



Datasheet (Hardware)

Datasheet for the Barracuda WAF Hardware



Datasheet (Virtual)

Datasheet for the Barracuda WAF Vx



Datasheet (WAF Control Center)

Datasheet for the Barracuda WAF Control Center

Customer Success

Azure

Agrifirm

Dutch Agricultural Cooperative



Blinkbox

Video Streaming Service



Energisme

IoT Platform



GL Education

Benchmarking assessments to UK schools



Mt. Sinai Healthcare System

Large healthcare system in the US



Azure (Regulatory Compliance)

Unicre

Payment solutions and credit card management system provider



Azure (GDPR Compliance)

Unit4

ERP Solution Provider



Customer Success

AWS

NoMoreRansom.org

Initiative to help victims of ransomware



Smithfield

Global Food Company



WAF-as-a-Service

L&Q

Large housing association in the UK



WAF Hardware

Sogegross Group

Dutch Agricultural Cooperative

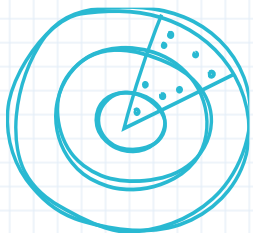


University of Malaysia, Perlis

Malaysian University



Customer Assist Plays



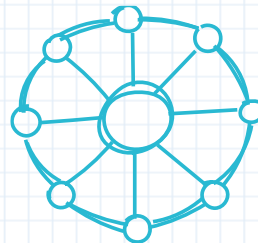
Run a free scan
of their application.

READY! SET! HIKE! 



Sign up for a free trial
of WAF-as-a-Service.

READY! SET! HIKE! 



Contact us for architecture
advice and help.

READY! SET! HIKE! 