



# How to improve your security posture with a web application firewall (WAF)

Serge Borso

Certified SANS Instructor  
SANS Institute

Geoff Sweet

Security Solutions Architect  
AWS

# How to Improve your Security Posture with a Web Application Firewall (WAF)

# Today's Speakers

- Serge Borso, Certified SANS Instructor
- Geoff Sweet, Security Solutions Architect, AWS

# Today's Agenda

- Premise
- OWASP
- WAFs for Security
- Implementation
- Challenges with WAFs

# What is a WAF?

- We have “workloads”: Web applications and APIs
- Lots of attack traffic coming from the internet
- A WAF is a tool to detect and prevent attacks
- The WAF *ideally* blocks web-based attack traffic
- Specifically designed to defend our workloads
- Relevant and useful due to the complexities of modern web applications
- Physical, virtual, cloud-based

# Premise Explained

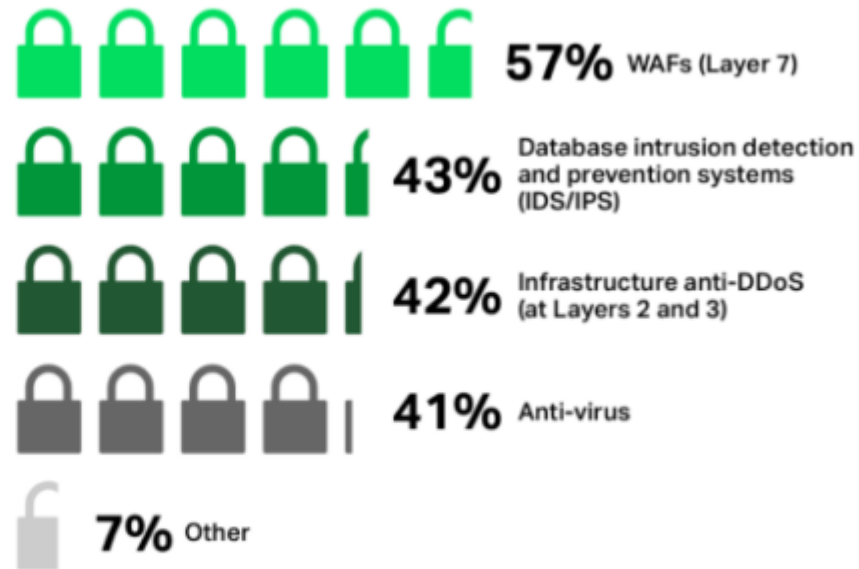
- Since a website is accessible to anyone in the world, it's constantly under attack
- Without a WAF, our environment is at a higher risk
- *Ideally* application codebase would be updated to reduce risk – but this isn't always feasible
- Multiple attack vectors equate to multiple teams
  - Developers
  - Infrastructure/engineering
  - Cloud Security

# Popularity and Relevancy

## Most popular security techniques

57% of organizations use WAFs

**SURVEY QUESTION** Which techniques are your organization using to improve security (choose all that apply)?



# What are we Defending Against?

## OWASP (Open Web Application Security Project)

### The 2021 OWASP Top 10 list

#### **A01:2021**

Broken  
Access Control

#### **A02:2021**

Cryptographic  
Failures

#### **A03:2021**

Injection

#### **A04:2021**

Insecure Design

#### **A05:2021**

Security  
Misconfiguration

#### **A06:2021**

Vulnerable  
and Outdated  
Components

#### **A07:2021**

Identification  
and Authentication  
Failures

#### **A08:2021**

Software and  
Data Integrity  
Failures

#### **A09:2021**

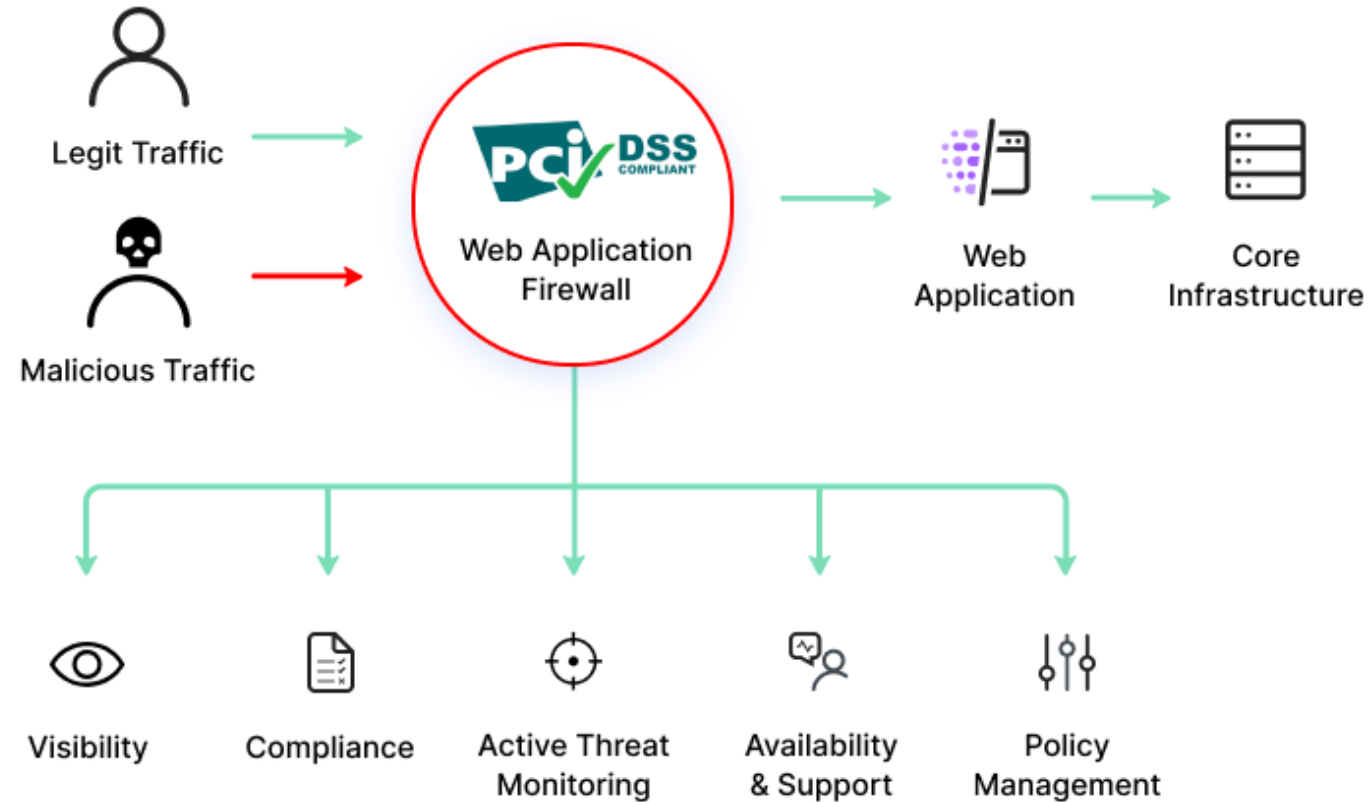
Security Logging  
and Monitoring  
Failures

#### **A10:2021**

Server-Side  
Request Forgery

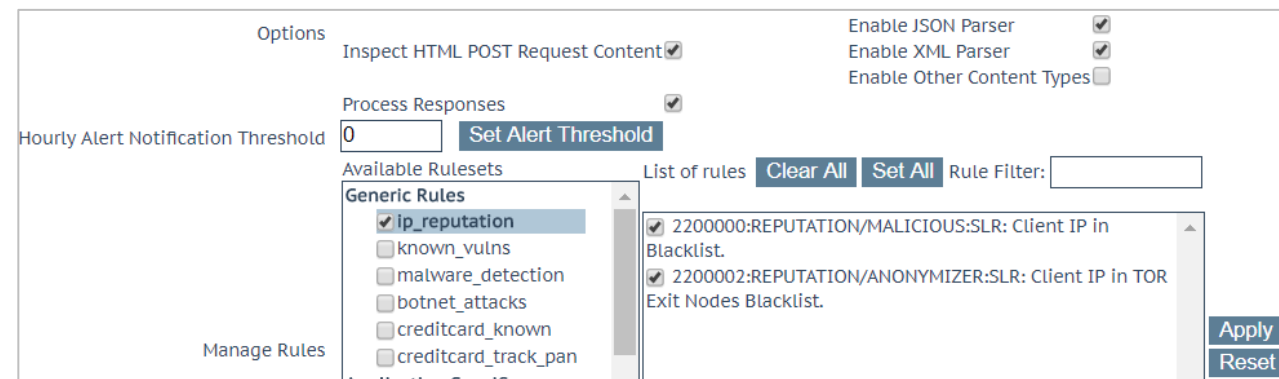


# Role of WAF in Action



# Configuration & Tuning

- Blocking vs Learning (prevent vs detect)
  - Extremely important difference between the two
- Think back to #9 on the OWASP list
  - Security Logging and Monitoring Failures
- Custom rules
- Per app/api settings
- Payload inspection
- AV, Bot Protection, CAPTCHA, Geolocation Blocking



# WAF Challenges

- Real-world issues (as real as it gets!)
  - Trust
  - Confidence
  - Expertise
  - Workload protections
  - False positives and false negatives
  - Adoption
  - Ownership and implementation
  - False sense of security
  - Global coverage

# WAF Takeaways

- Block traffic or don't waste everyone's time
  - Maybe not a popular opinion, and certainly not set in stone
- Not a panacea
  - Fix the APPLICATION! That's where the problem is
- Much easier to deploy and use today
- Tight integration with cloud providers
  - And relatively cost effective
- When tuned properly, a WAF can be formidable
- If you're not using one – look into it; it's worth it



# How to improve your security posture with a web application firewall (WAF)

Geoff Sweet

Security Solutions Architect  
AWS

# AWS WAF

## AWS-native Web Application Firewall



**AWS WAF**

- Protect web applications or APIs against common web exploits and bots.
- Get started quickly using Managed.
  - Pre-configured set of rules managed by AWS or AWS Marketplace Sellers
  - OWASP Top 10 security risks and automated bots



**AWS Shield  
Advanced**

- Deploy AWS WAF on Amazon CloudFront, Application Load Balancer, Amazon API Gateway, or AWS AppSync.
- Integrated with AWS Shield Advanced to provide layer-7 DDoS protection for your applications.

# Customer success stories

**FORTINET**®



# Deploying web application & API security

Get the security expertise you need to protect applications in the cloud.

Enable robust security controls for AWS WAF with Fortinet OWASP Top 10 Managed Rules.

 **Fortinet Managed Rules**  
for AWS WAF

 **AWS WAF**

Unlock additional security controls for web apps and APIs leveraging ML.

 **FortiWeb Cloud**  
WAF-as-a-Service

- AI-based Threat Protection
- Simplified Deployment and Management
- Advanced Visual Analytics

Requiring no hardware or software, **FortiWeb Cloud WAF** gateways run in most AWS regions.

Free trial available on AWS Marketplace

# Case study: BK Bank

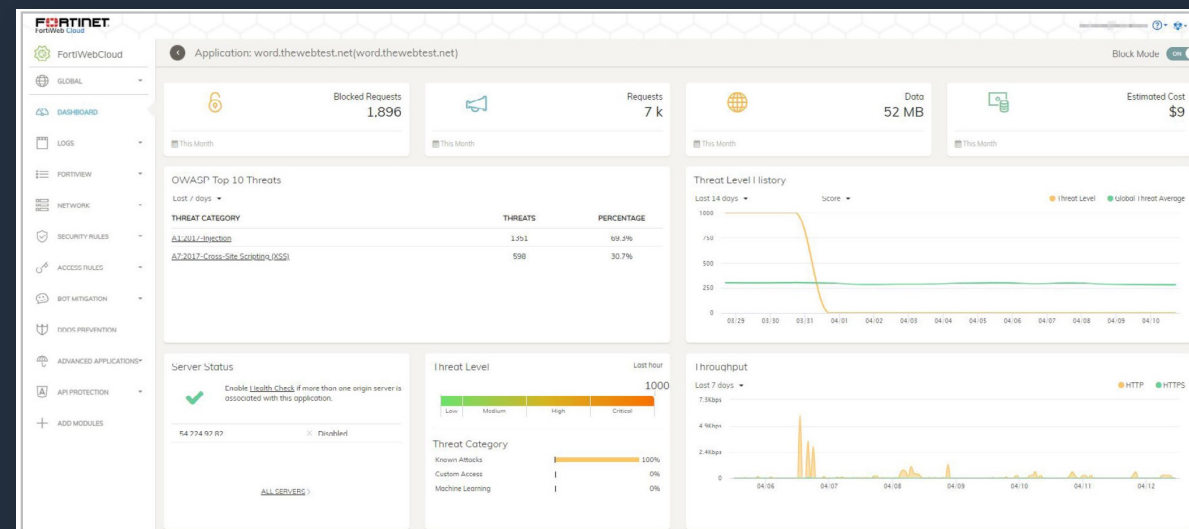
## Challenge

As a financial services provider, information security has always been a top priority for BK Bank. The bank was looking for a state-of-the-art solution that would minimize or eliminate 80,000 fraudulent intrusion attempts every day.

## Solution




The company deployed the Fortinet FortiWeb web application firewall (WAF) on AWS to protect its critical web applications from attacks. They also deployed FortiGate next-generation firewalls and FortiCNP on AWS for cloud-native protection. These integrated solutions provide BK Bank with comprehensive security, all managed from a single pane of glass.

FortiWeb Dashboard



# Case study: BK Bank

## Business Impact

-  Reduced PCI DSS compliance time
-  Improved protection of customers' financial data
-  Gained greater visibility into virtual banking environment on AWS

**“Integrated Fortinet solutions give us broad visibility, which provides for far easier and more proactive network management. This helps us improve all business processes.”**

**Caio Hyppolito**  
CTO, BK Bank



# Case study: Barracuda

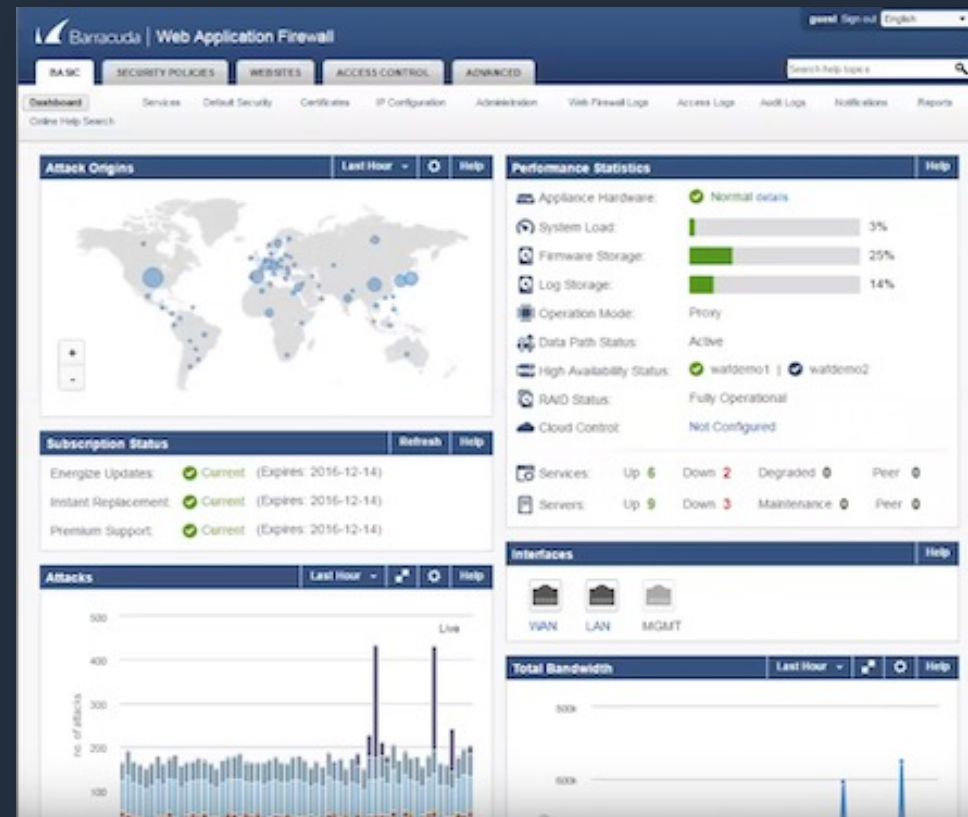
## Challenge

Smithfield Foods wanted to migrate all external-facing websites and applications to AWS while ensuring security against cyber threats. Previously, it had relied upon outsourcing companies to host and manage its datacenter operations. But as its needs evolved, it needed less costly solutions, more agile, and more ownership of its IT infrastructure and data.

## Solution

Smithfield chose Barracuda Web Application Firewall to provide the needed controls, but also a very easy user interface, even for people without a strong technical background. For Smithfield, being able to configure and provision directly through the AWS Marketplace made it very convenient.

Barracuda Dashboard



## Case study: Barracuda

### Business Impact



Cloud migration project proceeded smoothly



Deployment and configuration completed in one day



Barracuda Web Application Firewall provides security across all internet- and public-facing applications

**“The Barracuda Web Application Firewall provides the controls we need, but also has a very easy user interface, even for people without a strong technical background.”**

**Jeff Thomas**

Chief Technology Officer, Smithfield Foods



# Preventing account takeovers and romance fraud at Zoosk

Advanced protection for sophisticated attackers targeting APIs for abuse


## Challenge

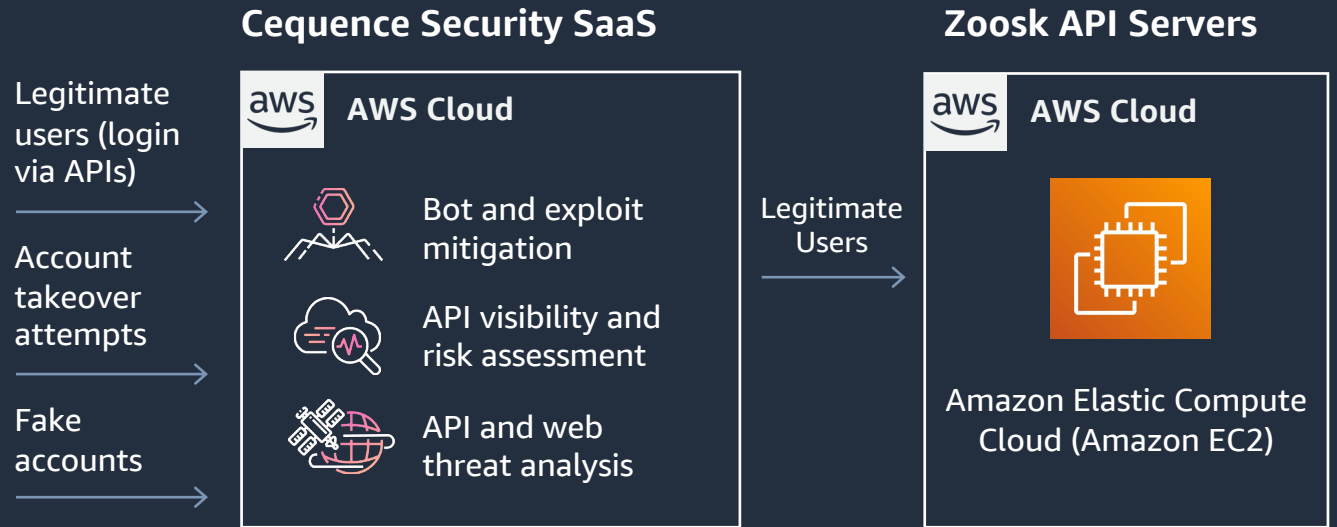
Legitimate users were targeting for fraud, losing on average \$12K per successful attempt

## Solution

Prevented account takeovers and fake account creation using AI and ML to identify malicious users

## Business Impact

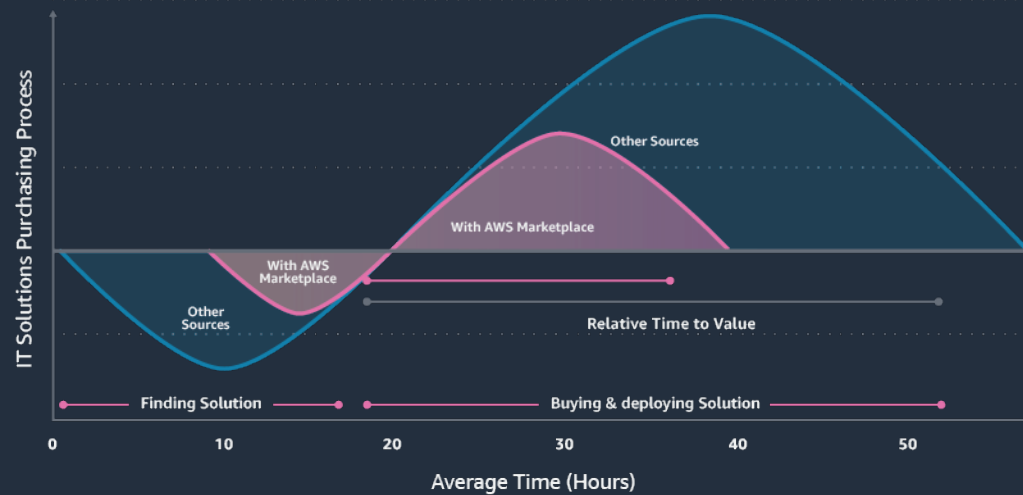
 Improved CSAT and user trust by reducing fraud across multiple dating applications





# Why AWS Marketplace?

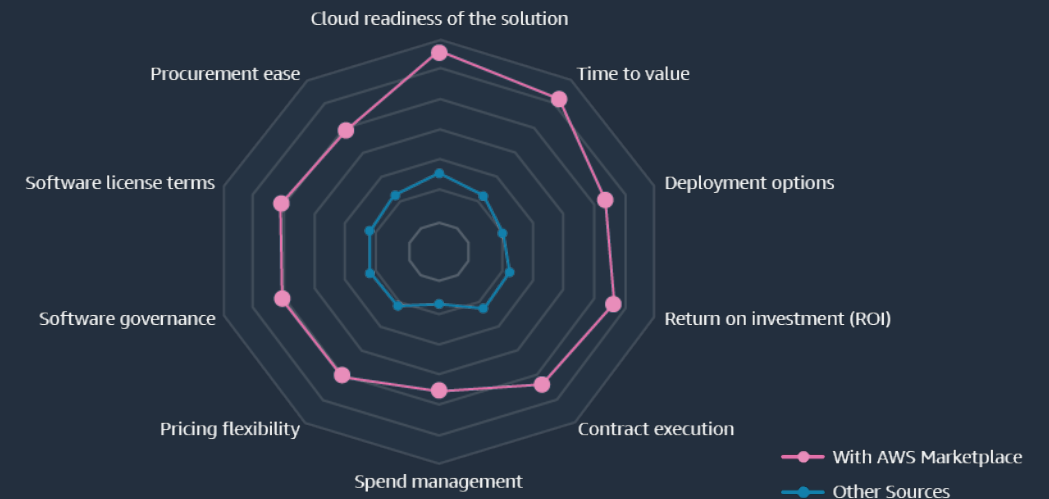
## Find, buy, and deploy solutions quicker



IT decision-makers (ITDMs) cut their time in half using AWS Marketplace compared to other sources.

Amazon Web Services (AWS) Marketplace surveyed 500 IT decision-makers (ITDMs) and influencers across the U.S. to understand software usage, purchasing, consumption models, and compared savings.

## Make more satisfying purchases



ITDMs feel 2.4 times better about purchasing using AWS Marketplace compared to other sources.

# How can you get started?

Find



A breadth of security solutions including:

**FORTINET**®

 **Barracuda**®

 **CEQUENCE**®  
SECURITY

**And more:**

<https://aws.amazon.com/marketplace/solutions/security/>

Buy



Through flexible purchasing options:

- Free trial
- Pay-as-you-go
- Budget alignment
- Bring Your Own License (BYOL)
- Private Offers
- Billing consolidation
- Enterprise Discount Program
- Private Marketplace

Deploy



With multiple deployment options:

- SaaS
- Amazon Machine Image (AMI)
- CloudFormation Template
- Containers
- Amazon EKS/Amazon ECS
- AI/ML models
- AWS Data Exchange

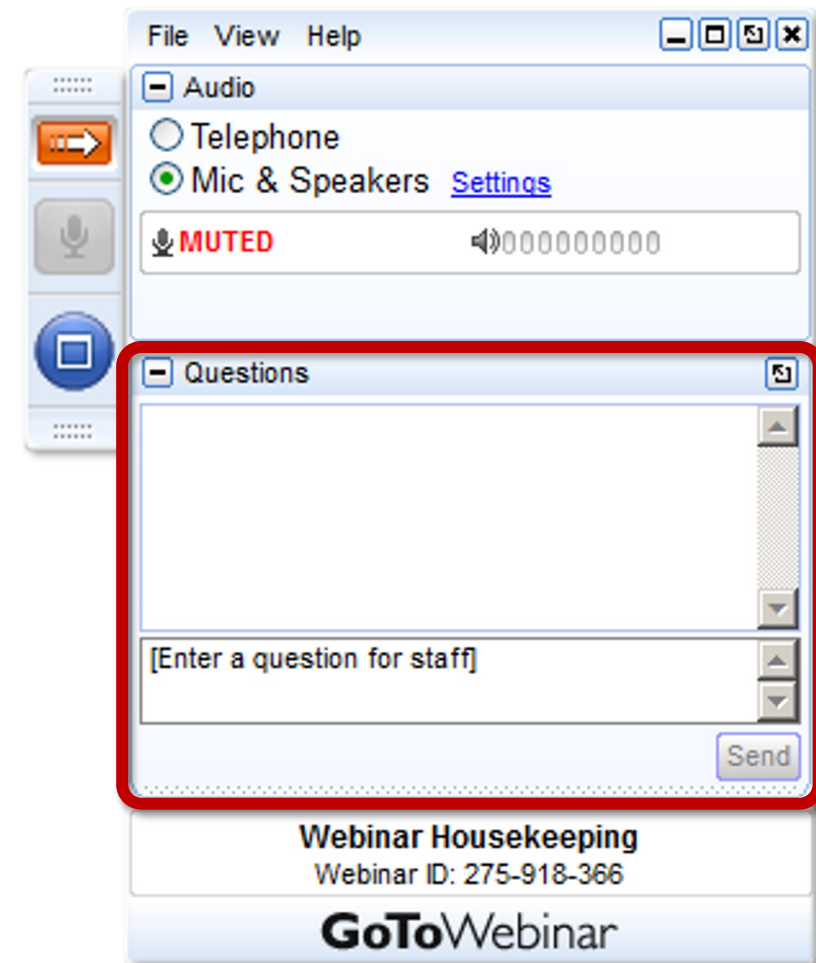
# Webinar summary

- Premise
- OWASP
- WAFs for security
- Implementation
- Challenges with WAFs
- Customer success stories
- Solutions in AWS Marketplace

# Q&A

Please use **GoToWebinar's** Questions tool to submit questions to our panel.

Send to “Organizers” and tell us if it’s for a specific panelist.



# Acknowledgments

Thanks to our sponsor:



To our  
special guest: **Geoff Sweet**

And to our attendees, thank you for joining us today!

aws marketplace

**Thank you!**