# Application Security for Businesses

Presented by Venkatesh Sundar, CMO, Indusface

# The Importance of Information Security

**10**

recent start-up Hacking incidences in ecommerce, online song portals, taxi-for-hire services and other sectors.

**Loss of customer database, credit card details, financial disruption** and **defacement** are only few of the disasters that **application layer hacking** brings.

**75%**

of these security breaches happen at the **application layer**:

*Gartner*

Little or no application security assistance for start-ups in India



INDUSFACE™

# Total Application Security Concept

# Detect

# Detection Challenges

1

Web applications are critical to online business processes.

2

Web applications have become increasingly **complex, having tremendous amounts of sensitive data** which can be used in unexpected ways, abused, stolen, and attacked.

3

Increasing **threats, regulations, and the changing IT landscape** has made dynamic software security testing important.

4

**Vulnerabilities in applications lead to security breaches**, which are a threat to brand reputation.

5

There are complex **business logic flaws** that are specific to application process and cannot be detected automatically.



INDUSFACE™

# Comprehensive Application Testing

1

Combining automated and human intelligence to **test web applications during and after development.**

2

Automated **detection and reporting of underlying weaknesses** as listed by the Open Web Application Security Project.

3

Manual penetration testing of web application by experts to find **flaws specific to business logics.**

4

Continuous **scanning for malware and other bugs.**

5

Inspection of spammy changes on the website that could lead to **blacklisting and defacement.**

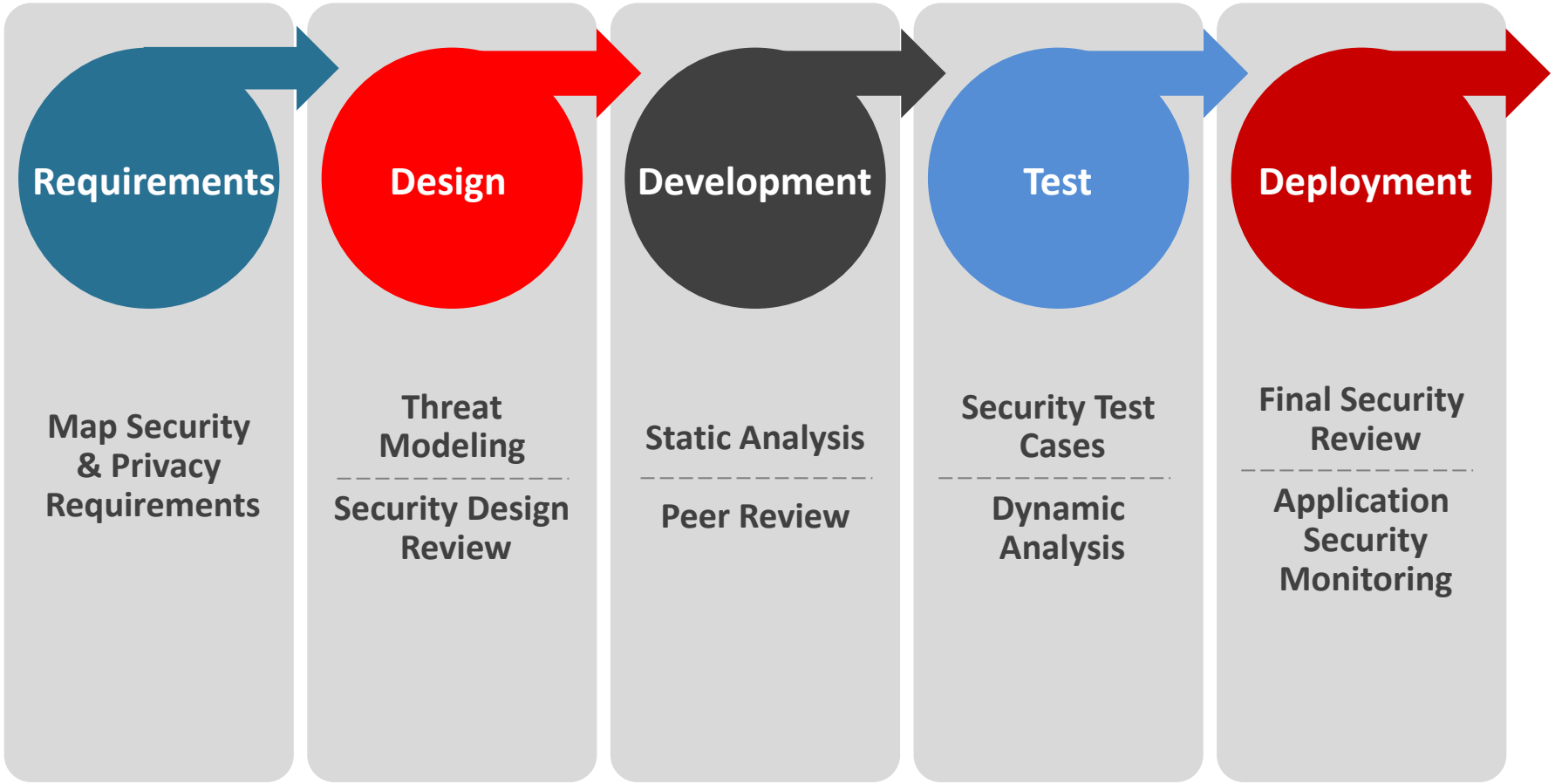
# Security in Software
# Development Processes

Implementation of a Secure Development Life Cycle (SDLC) program ensures that security is inherent  in good enterprise software design and development, not an afterthought later in production.

## An effective Secure Development Life Cycle program:

- Designs security imperatives from the beginning of development process.
- Releases nothing to production until security standards are met, as a matter of policy.
- Sets up checkpoints, during the build and test process.

# SDLC Process Flow



# Protect

# Why Protect?

## Detection alone does not prevent attacks.

- 8 in 10 ‘Critical’ level vulnerabilities remained unpatched for almost 175 days after detection
- 9 in 10 ‘High’ level vulnerabilities remained unpatched for 115 days after detection
- Patching web applications is a costly and time-consuming process.

# Detection Isn't Enough

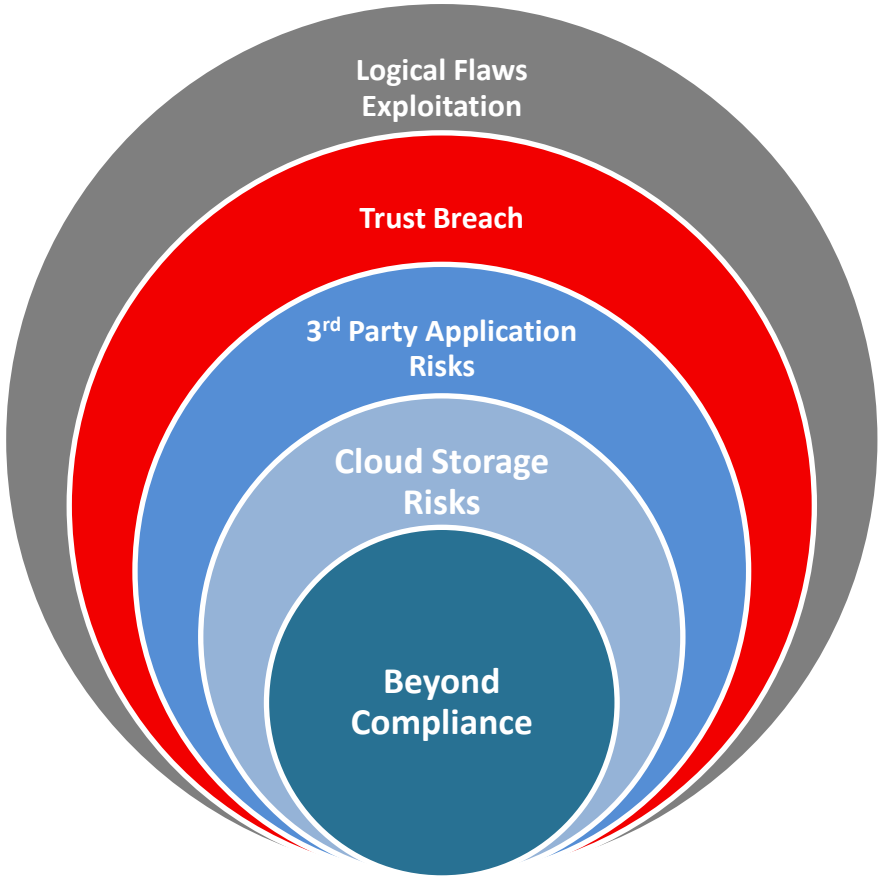
**Logical Flaws Exploitation :** Even average developers are getting aware of CSRF , XSS. Attackers are always looking into newer exploitation methods.

**Trust Breach :** Shellshock and Heartbleed showed, how exploiting vulnerabilities in UNIX Bash Shell and OpenSSL cryptographic library can help breach into secure systems.

**Third-Party Application Risks:** Complexities with web application security getting fierce.

**Cloud Storage Risks :** More individuals and organizations will be shifting towards cloud computing, which also involves cloud-based web applications and their penetration risks.

**Beyond Compliance :** Compliance should be a start point. It's just a baseline security posture and organizations will need to look beyond that and develop a security trend on their own.




Enterprises need to adopt more holistic, integrated security solutions that can continuously monitor and defend against emerging attacks

Total Application Security (TAS), an integrated solution which can Detect, Protect and Monitor systems on a continuous basis 24X7.



INDUSFACE™

# Existing Security Infrastructure Not Enough !

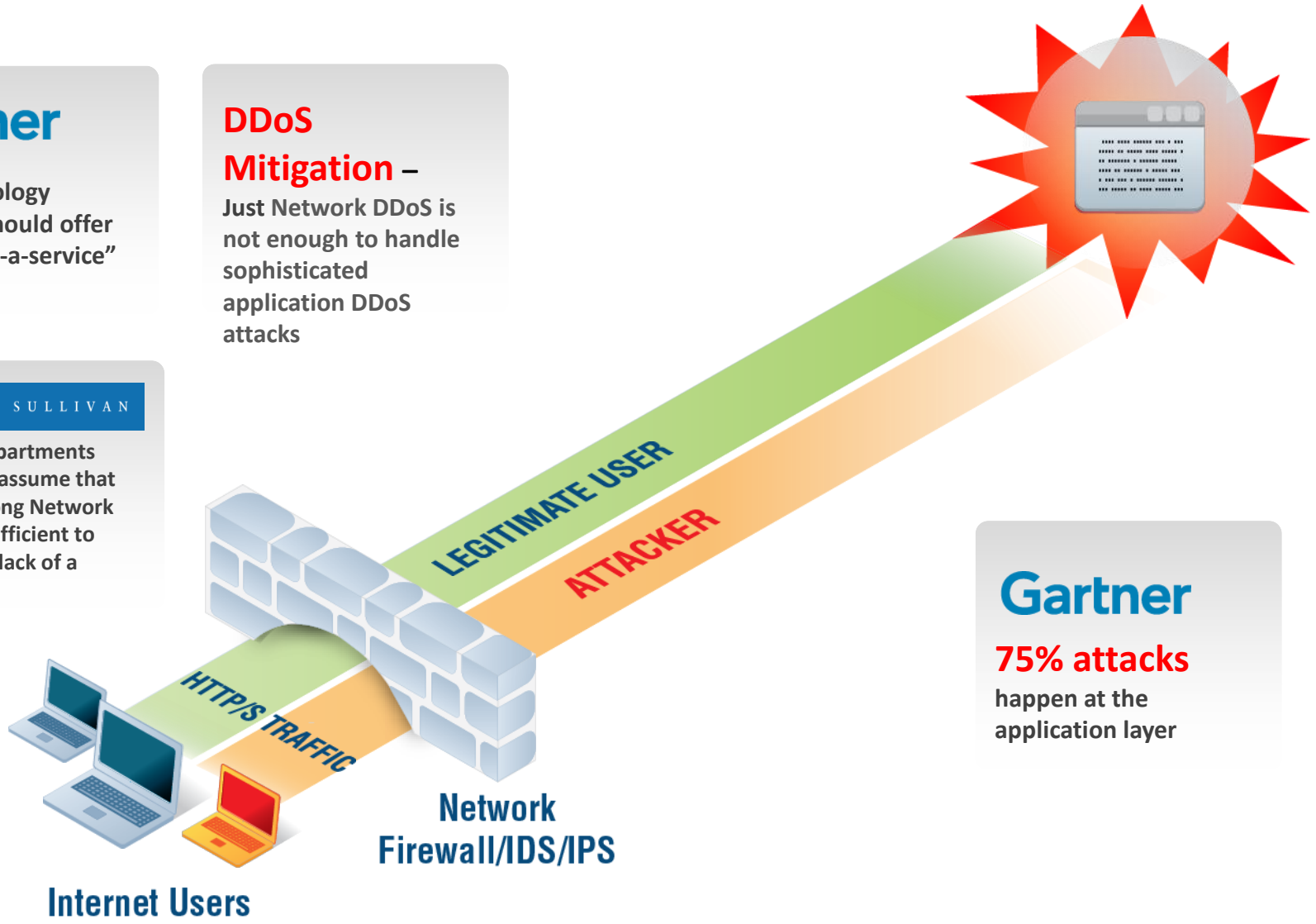
Gartner

WAF Technology providers should offer "security-as-a-service"

**DDoS Mitigation –** Just Network DDoS is not enough to handle sophisticated application DDoS attacks

FROST & SULLIVAN

55% of IT departments erroneously assume that having a strong Network Firewall is sufficient to make up for lack of a WAF




451

"Expert tuning can mean the difference between a working defense layer and a technology that is just gathering dust and using up budget." Wendy Nather, Feb. 2012

Gartner

**75% attacks** happen at the application layer

INDUSFACE™

**100 days** required on average to fix a serious vulnerability



INDUSFACE™

# Web Application Firewall

1

Proactive web application **protection** through **virtual patching without code change**

2

Automated protection from exploitation of **OWASP Top 10 vulnerabilities**

3

**Custom rules for business logic flaws** by security experts

4

Zero False Positives to ensure **genuine traffic remains unaffected**

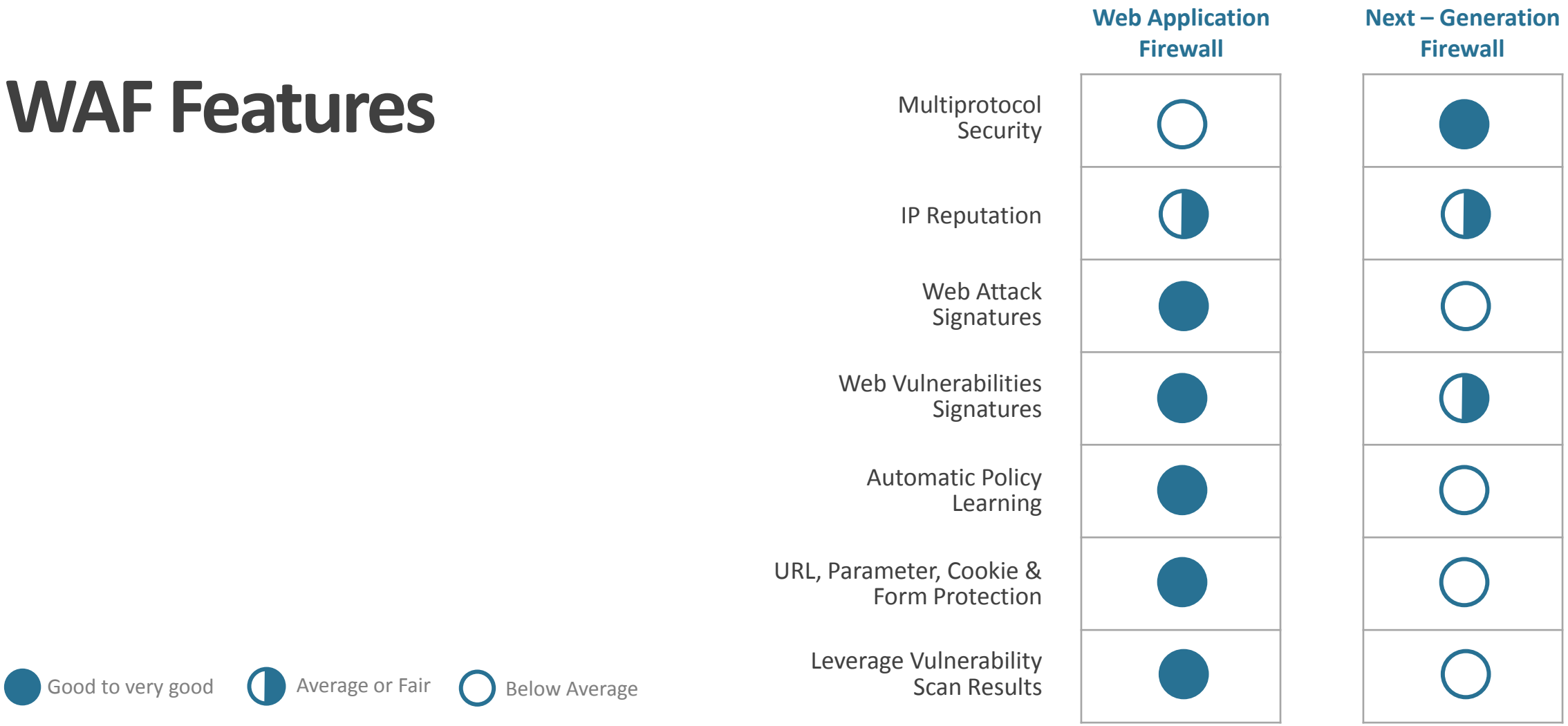
5

Compliance to Payment Card Industry's **(PCI)** Requirement 6.6



INDUSFACE™

# WAF Features

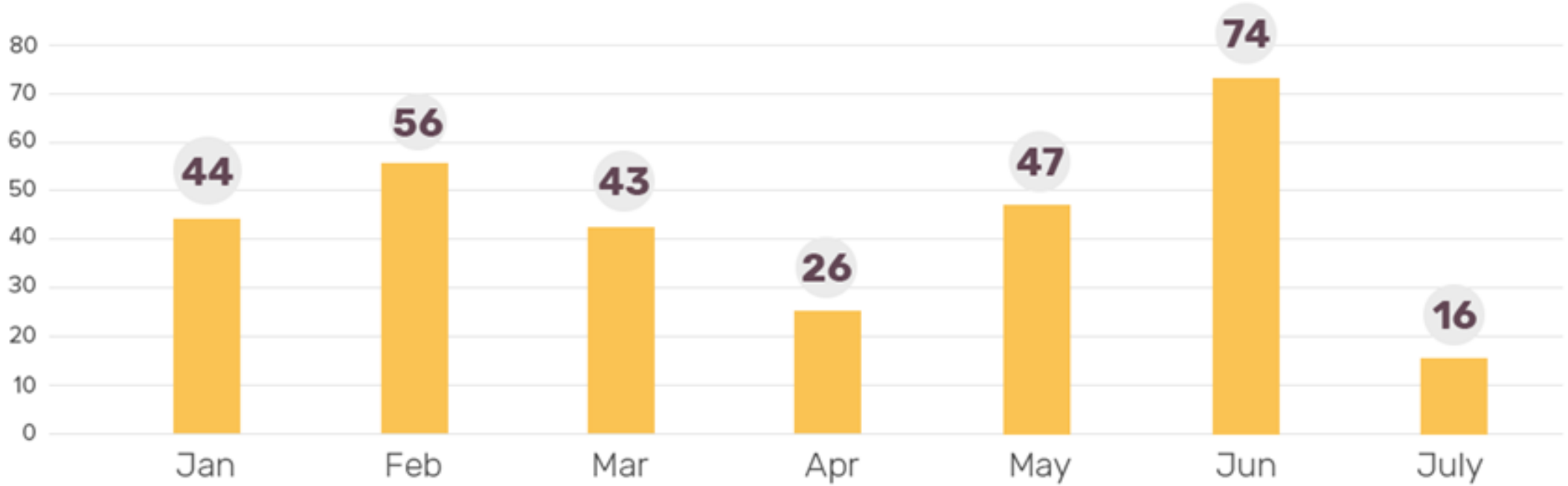


# Zero Day Vulnerability Report Data

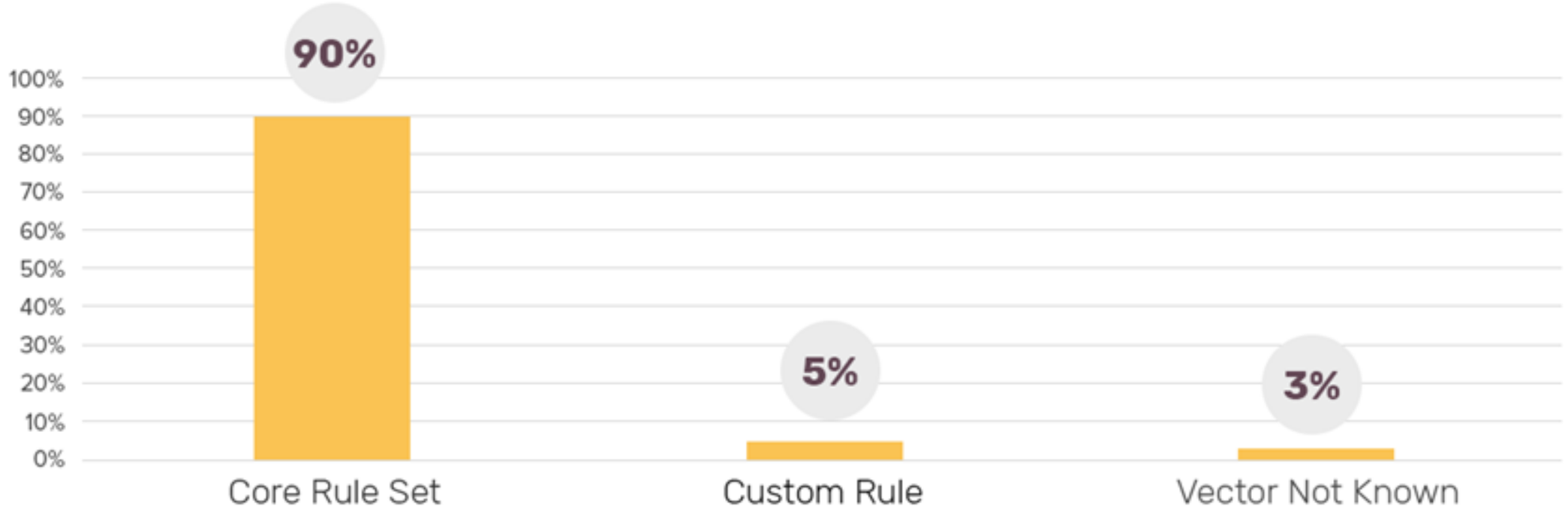
by Indusface

# Application Zero-Day Vulnerability

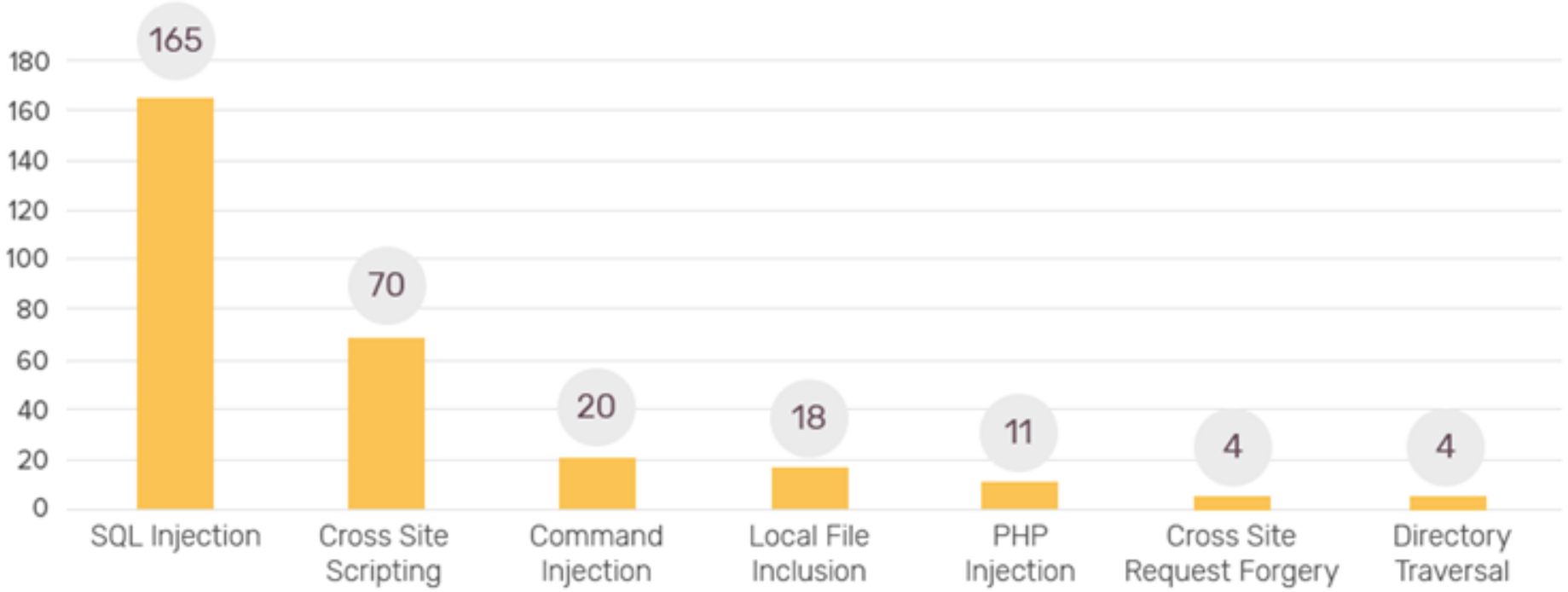
## Month on Month Count



# % of App Zero Day Vul blocked via CRS, Custom rules & Vector not known



# Application Zero-Day Vulnerability
# Categories & Count



# Top Vulnerability in the last 6 months

Apache struts command injection protected via core rules.

SQL injection vulnerbibility in Wordpress plugin for messages via core rules

CSRF in a popular helpdesk system vis custom rules.

# Monitor

# Continuous Inspection for

1

Monitoring provides in-depth data to identify and **mitigate Distributed-Denial-of-Services attacks.**

2

It helps **improving detection and protection policies.**

3

Real-time **incidence monitoring, response and reporting** ensures application security day in and day out.

4

Startups can take **informed security decisions** with actionable insights and not just random data feeds.

5

**Proof-of-Exploitation** demonstrating how hackers use vulnerabilities to attack.

# Proactive Learning with Analytics

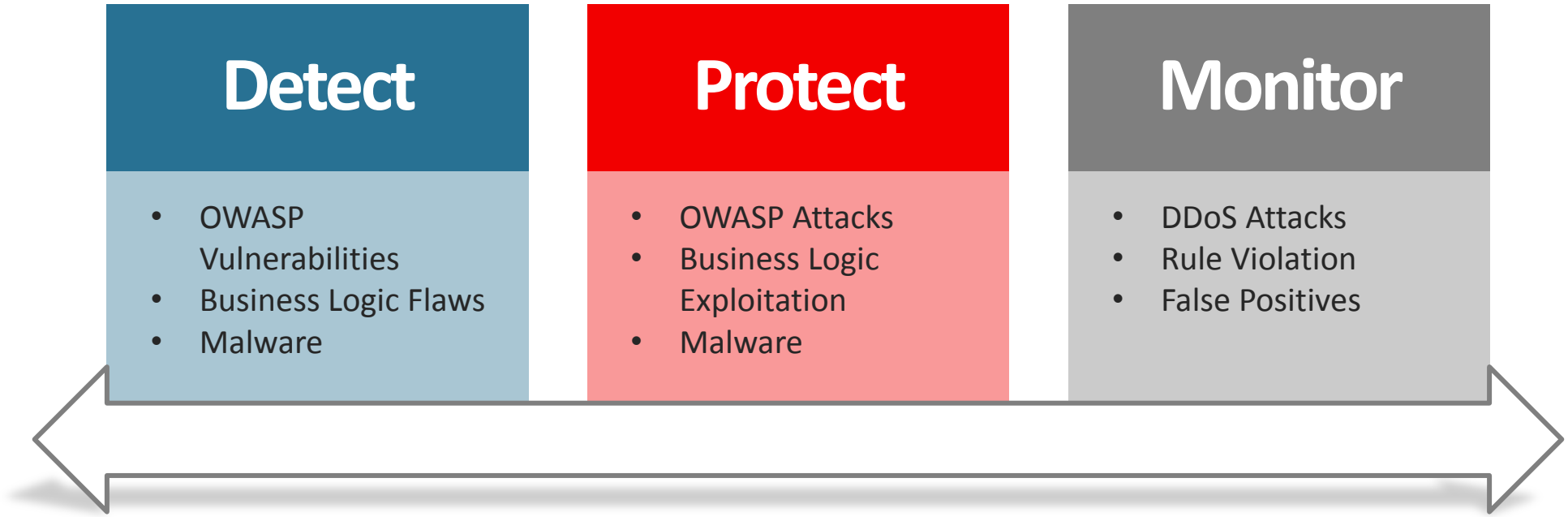
Studying WAF traffic data to identify attack attempts

Analyzing and understanding patterns through machine fingerprints, IPs, payload and bot signatures

Integrating acquired knowledge to develop smarter detection and protection policies

Refining the process to strengthen overall security posture

# Web Application Security Process for Startups:



# Free WebSite Scan OFFER

to

**Send email with Email Title COIMBTORE2017**

**to Fayaz.dhandargi@indusface.com**

**Venkatesh.sundar@indusface.com**