APPTRANA

WHITEPAPER

SECaaS (Security as a Service)

With growing adoption of Infrastructure as a Service (IaaS), businesses are moving towards the web (cloud) and it has become necessity for businesses across all verticals including health, retail and manufacturing to have a web presence if they want to scale. In-fact, new-age companies solely rely on digital business for growth doing all their business online

No matter what business strategy is, successful digital presence is a must and there are key factors that determine success. They are:

Availability

Gen Y are an impatient lot, as they become the primary consumers, it is paramount that they have a seamless digital experience no matter where and how they are accessing the content. These buyers are born into the world of mobiles, iPad, spoiled with multiple options. For these buyers, any downtime is not acceptable and they will move to competitors.

Performance

Online content is becoming richer day- by-day. How fast and seamlessly one can serve their customers with data rich, high graphic content is as important as availability.

Brand Reliability

With the fast-moving world, customers do not have too much time to investigate and their buying pattern depends on what they hear. Trust becomes a key factor for success. With the advent of social media, many people depend on crowd-sourced review to make their decisions. In such an environment, any breach of trust will become disastrous for the business and reliability is very important to achieve all this, any digital strategy should be built on top of strong, secure foundation. Web applications are diverse, built on rapidly changing technology and their security is complex.

Hackers are working 24/7 to exploit the vulnerabilities available in the application layer. If they succeed, depending on kind of breach, it could lead to loss of availability, compromise of personal information or loss of trust creating an existential crisis to business.

Organizations are under intense pressure to deliver web apps and web services to meet the demands of modern digital customers. However, app security is not keeping pace with the development cycle, which broadens a brand's threat surface.

Current State

As of March 2016, Google reports that over 50 million website users have been greeted with some form of warning that websites visited were trying to either steal information or install malicious software. In March 2015, that number was 17 mil- lion. Per Cenzic's research, 96% of appli- cations have an average of 14 vulnerabil- ities. Gartner says 70% of website attack is targeting application layer.

Though companies continue to invest on security, hacks continue to grow. Major reason for this is the short coming of existing cloud solutions. They provide standard out of the box rules without understanding specific application needs. This is akin to shooting darts in the dark and has very little chance of success. Perils of such approach are:

- There is very little understanding of the application needs, vulnerabilities specific to the application that hackers can exploit are left unprotected. As the saying goes, security is as good as the weakest link
- Standard rules are good in ideal scenario. But as in life, applications in real world are far from ideal, leading to lot of false positives & false negatives, making the solution ineffective
- Proper implementation of WAF requires tuning of standard rules to meet application specific needs but unfortunately this needs lot of expertise and time, which are not easy to find.

All this leads to inadequate web security which is bound to be breached by motivated hackers through targeted attacks.

For any business, hackers playing havoc exploiting application security is a clear and present danger, which is evolving every day. Your application security is as strong as the weakest link. One vulnerability, which hackers can exploit, is all that is required to bring down your site with that your business.

Security threat to the application layer is constantly evolving and hackers are working 24/7 updating themselves and constantly trying new ways to exploit. To be ahead of the curve, every application needs a way to understand the risk posture of the appli- cation upfront and tune the site defenses based on the risk identified constantly. This requires lot of time and expertise which business. However, the problem is that not everyone is an expert. It takes years of experience to understand how hackers think and build defense around it. Web application security is a continuous process not a one-time scan done every quarter or year.

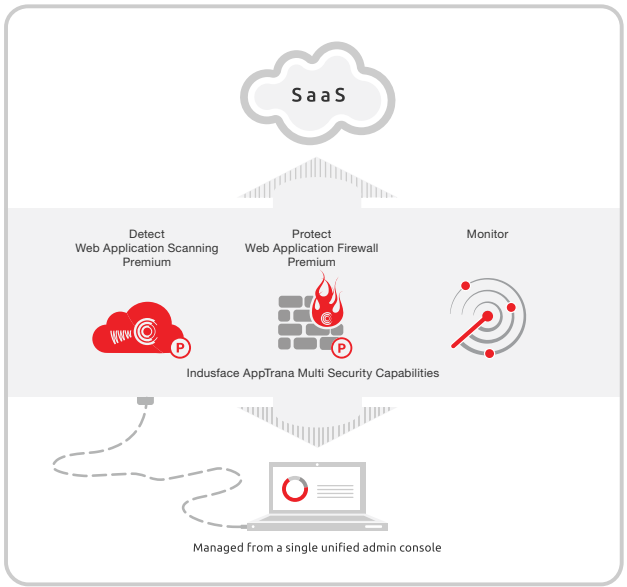
AppTrana

Through AppTrana, industries first fully managed security as a service solution. With AppTrana, organizations can identify the vulnerabilities in the application through its automated and premium (manual penetration testing done by experts) scans. This guarantees that organization understand the risk posture of their application upfront. AppTrana through fully managed detection module ensures that vulnerabilities reported have zero false positive.

With AppTrana

- Customer will be quickly get AppTrana protection within minutes with zero downtime during the entire transition.
- Customers get access to highly scalable PCI complaint, infrastructure for their web application security that is scalable to Terabytes of data seamlessly with no configuration required from customer side
- Provide ability to detect vulnerabilities, protect them instantly through virtual patches and get round the clock visibility to risk posture through integrated AppTrana portal
- Get round the clock, experts monitored protection for the site against complex DDOS attacks

Now, customers can concentrate on business without worrying about security and availability of their site



Indusface is an example of an Indian WAF vendor that provides the SaaS-based managed Web Application Firewall. This type of solution is a good alternative for enterprises that do not want to procure new hardware and hire or train staff to manage it

Gartner Report

Gartner

Let's see how AppTrana can be used as part of building cyber security strategy for the company.The first step of any cybersecurity strategy is to identify the current security posture and weakness.

Detect:

AppTrana Web Application Scanning helps you do just that. AppTrana's automated Web Application Scanner detects OWSAP Top 10 and WASC 25 vulnerabilities. This combined with manual penetration testing by AppTrana's security experts also identifies complex business logic flaws, which can seriously compromise security if unattended. AppTrana WAS through its managed solution, ensures that the vulnerability reported has zero false positive and helps organizations concenterate on vulnerabilities that require immediate attention.

Protect:

Once risk posture is identified, AppTrana enables organizations to virtually patch vulnerabilities through its WAF module. For this, AppTrana provides

Advance Rules – Rules which are written by security experts and that comes with zero false positive guarantee

Premium Rules – Rules which are experiential in nature which is monitored by security experts and fine-tuned to meet application need before they are put in block mode. No action is required from customer

Custom Rules- Application specific rules written by security experts with zero false positive guarantee based on customer request.

With this 3-prong approach, AppTrana ensures that security is tuned to meet specific application need guarantying zero false positive.

While it's true that the ideal place to fix a vulnerability is in the application, the aver- age time to fix critical vulnerabilities is 100 days due to debugging, development, im- pact analysis, QA i.e. normal release cycle timelines. AppTrana provides day zero protection against these vulnerabilities, keeping the application secure until the vulnerability is fixed in the application.

Monitor:

AppTrana Monitor module with perfect amalgamation of machine learning and human intelligence provides the best defence against ever-growing security threats to your application. AppTrana constantly monitors the landscape for evolving threats, DDOS and other attack patterns. The analytics help our experts in updating core rule sets and custom rules reinforcing security on customers' applications.

Application DDOS

Application DDOS has become ever more prevalent and DDOS mitigation is core to any application security strategy. One of the key aspects of the monitor module is to build a strong defense across DDOS. It is almost impossible to build out of the box DDOS protection without affecting legitimate users, hence Indusface AppTrana attacks the problem uniquely. With the amalgamation of machine learning and manual monitoring, AppTrana provides multiple layers of defence against DDOS attacks. With AppTrana built on AWS, it comes with in-built protection against Layer 3 DDOS.

Bot Management

AppTrana constantly monitors traffic for malicious BOTS and blocks them. AppTrana constantly updates its BOT management rules through crowd-sourcing keeping the rules up-to date. Based on the patterns observed, custom rules are also crafted by our security experts to avoid web scraping and protect against unwanted data loss.

Captcha Mode

As AppTrana constantly monitors the traffic to the application, it identifies variance in pattern of traffic (behaviour, location, rate etc..) and, as a first line of defense, kicks in the captcha challenges, showing captcha for traffic which is suspect.

Rate Control and Aggressive protection

As second line of defense, AppTrana does fingerprinting analysis on the traffic blocked by rules/captchas and kicks in rate control and other DDOS protection rule. By this time, our security experts are notified and they provide additional support to reinforce the application against DDOS attacks.

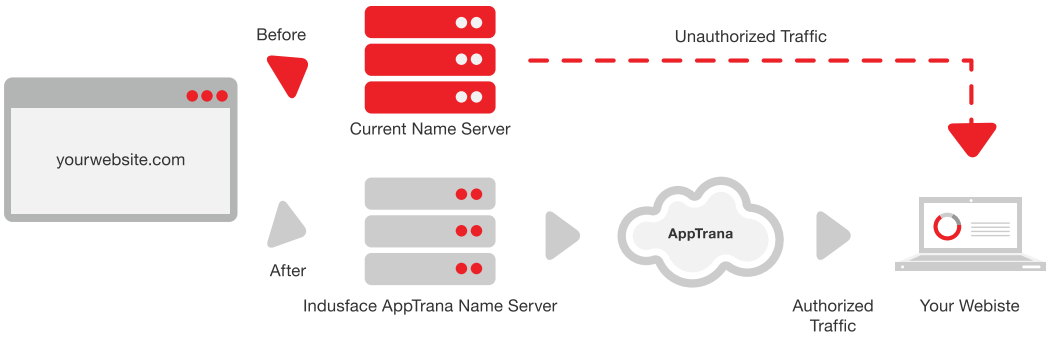
“Indusface has proved to be a valuable security partner with its AppTrana solution. Their ‘detect-protect-monitor’ package handles security worries so we can focus on improving services for our customers. Vulnerability detection, attack blocking and near real-time reports are some of the key differentiators that we enjoy with them. The web application scanning and web protection combination has ensured that we are protected from highly increasing threat vectors.”

Sharad Sadadekar, Chief Information Security Officer, HDFC Life

AppTrana security experts are available 24 x 7 to analyze DDoS and other attack patterns. Proactive false positive elimination as part of monitor module further ensuring that genuine visitors are not blocked.

Why AppTrana?

AppTrana is the industry's first fully managed solution, which completely takes ownership of all the security needs of your application, leaving the customers to concentrate on their business needs.



No Installation

Securing your website should be easy and that is what AppTrana provides. All you need to do is, make a CNAME change to point to Indusface AppTrana infra and AppTrana will now become your domain provider and protection will start instantly. The entire onboarding is done with zero downtime.

No Technology Expertise Required

You don't need a security expert/s to maintain the security posture of your application. AppTrana will completely take care of it. You don't have to worry about complex security jargons and evolving security threats you constantly keep hearing about. AppTrana is here to take care of all your security needs.

Completely Managed from Day Zero

We can't emphasize this enough. AppTrana provides you protection from day zero with 24*7 monitoring from emerging DDOS and other attack patterns.

Architecture Explained

Built bottom up on AWS, using all the latest resources available, Indusface AppTrana PCI compliant Infrastructure has been architected keeping security and performance in mind. Auto scaled SaaS setup built in AWS, scales seamlessly to handle Gigabytes of data with no visible impact to end user experience. The auto-scaled architecture spawn's machines based on the load making sure that users do not see any lag due to high traffic.

Network Design

- Secured using all of AWS Security best practice documents
- Security Zoning and Network segmentation
- SSL VPN
- Per Host Group Security Group

Host Design

- Bastion Host
- OS Level Hardening done
- App Stack Hardening done

Compliance

- Services used natively support PCI compliance

Why AWS?

Gartner estimated that the IaaS market size in 2014 was $13 billion, and growing fast. By 2018, it will be $42B (CAGR 35.6%). While there are many vendors offering IaaS today, AWS is the clear leader in this space and accounts for the majority of the business. Per Gartner, "AWS is the overwhelming market share leader, with 5x the Cloud IaaS compute capacity than the aggregate total of the [next] 14 vendors".

About Indusface

Indusface is an award-winning application security leader protecting 800+ global customers with its unique Total Application Security platform that detects, protects, and monitors applications. Indusface has not only won all major startup awards this year including the AWS Regional Innovation Partner - Technology Award but our security products have also been mentioned in the Gartner Magic Quadrants for Application Security Testing and Web Application Firewall.

INDUSFACE™

California
1001 Bayhill Drive
2nd Floor, San Bruno,
United States - 94066

www.indusface.com