WHITEPAPER

Real intelligence, not **just** virtual patching

SUMMARY

Finding a vulnerability in your application is an integral part of knowing your risks first. It also leads to an urgency within the organization to address and fix the problem quickly.

Despite organizations having strong intent for fixing the vulnerability, often it may not be practically possible to patch due to several reasons, such as lack of access to code with third-party dependency, developer availability, and/or lack of time.

Hence, virtual patching via web application firewall becomes a key value proposition for adopting WAF and providing time to fix benefits for security loopholes. The constraints faced by customers to fix the vulnerability quickly and the need for virtual patching are already well established. We are not going to be covering the time to fix benefits or the need for virtual patching in this whitepaper.

We at Indusface, with our AppTrana offering, use virtual patching as the starting point of our value proposition with our Managed WAF service in order to provide more value to the customer.

In this paper, we will examine how virtual patching can be used as the foundational block for gathering further intelligence on hackers and tracking their behavior.

With our collective experience of scanning and auditing 6000+ applications (whilst observing and preventing many millions of hackable risks), we have gained a deep understanding of a hacker's behavior. With continuous learning, we started using virtual patching policies to not just provide time to fix benefits to the customer but also to use it to track the hacker behavior- further enhancing the defense posture perpetually.

Our intent is to educate customers to not just look at virtual patching as a quick fix but also a key source to gather intelligence on hack attempts and the hacker identities and keep them off on a continuous basis. The ROI with this approach far exceeds the operational efficiencies and time to fix benefit of virtual patching, which is what the industry is currently looking at in isolation. We hope to change all that with our AppTrana offering.

HACKER BEHAVIOR

Before getting into the details of how virtual patching can become the source of intelligence to track hacker behavior, let's look at the steps a hacker will take before carrying out an exploit.

Hacker

1. Pray and Spray probes. They use crawlers and free tools to probe for gathering intelligence of what is running and where.
2. Use the output from those probes to build a list of targeted weak spots that they can go after with targeted attacks. Example: Site X is running a vulnerable web server, site Y is prone to-brute force logins, site Z has SQLi and XSS insertion possibilities.
3. Plan a targeted attack based on the intelligence of weak applications and their weakest link.

Application security prevention in use today

Every application owner or the security group (if you have one) should be doing the following:

1. Regular security scans of your application.
2. Periodic manual application penetration testing when application has gone through major changes.
3. Identifying the vulnerabilities and passing them on to the owner, who can patch them
4. Virtual patching in WAF if you have one and if necessary.

Challenges

1. The team in charge of the security scan will be different from the team performing the manual audit
2. Collecting this information and giving it to WAF vendors will provide you nothing more than just a signature (REGEX) and not a policy for defense and intelligence on hacker behavior.
3. Often WAF vendors do not take the ownership of identifying out-of-the-box risks and creating virtual patch policies for them - it is up to the customer.

SOLUTION

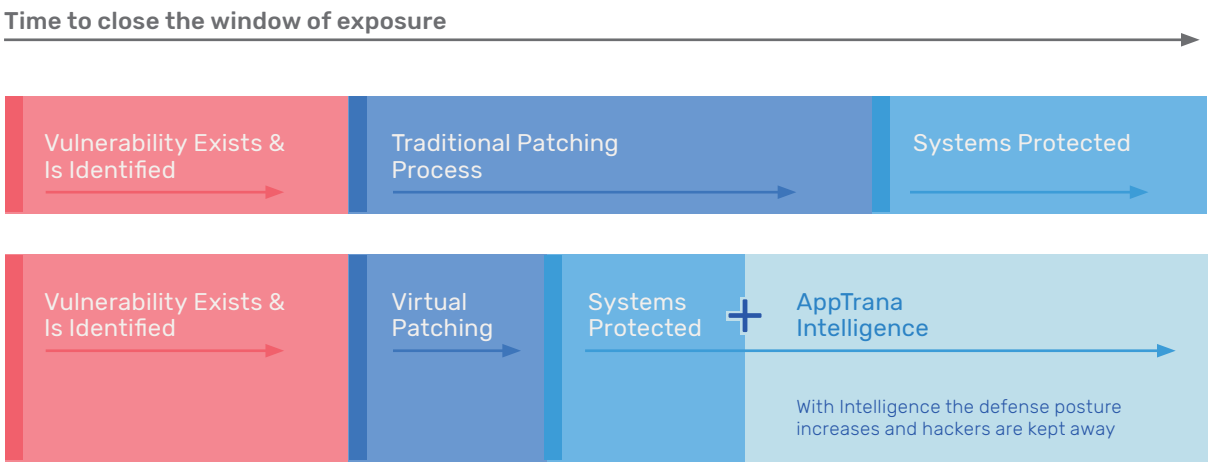
Map it to the hacker behavior. A hacker goes through the same cycle of what an application security team does, but instead of finding vulnerabilities and fixing them, a hacker will exploit it. It's important to have one solution that goes through the same lifecycle of a hacker attempt, but instead of finding and exploiting them, one can detect, protect and monitor. With AppTrana, we offer Scanning + WAF + Monitoring under one package so that the customer gets continuous hacking prevention against hackers, rather than just point-in-time virtual patching fixes resulting in a non-stop cat and mouse game with no advantage to the company.

The intelligence from vulnerabilities and associated exploited items, backed by real-time virtual patching policies (not just signatures), equip an AppTrana customer with a complete understanding of:

1. Vulnerabilities which exist in the application.
2. How many of them are patched via a virtual patching policy in WAF.
3. How many of the existing vulnerabilities were attempted to be exploited but blocked by WAF.

Point 3 is the most important piece, as for an evident attack, logging and analyzing information (such as machine fingerprint, IP, session ID or any additional application-specific custom info) is the foundation of developing security mechanisms. This data can be used to create hacker tracking profiles in order to further enhance the defense posture on subsequent requests originating from the flagged source. Upon any subsequent request from the hacker matching this profile, the policies will dynamically take a more aggressive stand against the requests without risking false positives.

The diagram below shows where the value proposition of virtual patching stops. With this approach, the benefit is continuous and ongoing by using the virtual patch policies to further enhance automated rules and policies (not just signatures) to enhance the defense posture once we know it's a hacker on the other side.



CONCLUSION

Web applications are business-critical systems that must be kept secure. It is not always possible or practical to fix vulnerabilities in these systems immediately. Organizations can use virtual patching in conjunction with vulnerability scanning solutions to quickly address vulnerabilities until permanent fixes can be deployed.

However, by combining scan intelligence and quick virtual patching policies in an integrated manner, companies can ensure improved security and operational efficiency. It also strengthens the process of dynamically and continuously improving security posture by tracking hacker behavior and improving security rules automatically.

ABOUT INDUSFACE

Indusface is an award-winning application security leader protecting 1000+ global customers with our unique Total Application Security platform that detects, protects, and monitors applications. Our Total Application Security solution is available On-Premise, As A Service and through the AWS Marketplace.

Mentioned in the Gartner Magic Quadrants for Application Security Testing and Web Application Firewall, Indusface has won all major startup awards in the last 12 months including the NASSCOM-DSCI 'Security Product Company' Award, iSpirit's 'InTech50 Most Innovative Products from India' and AWS 'Regional Innovation Partner: Technology Award'.

Bengaluru | Vadodara | Mumbai | New Delhi | San Francisco

Contact: marketing@indusface.com