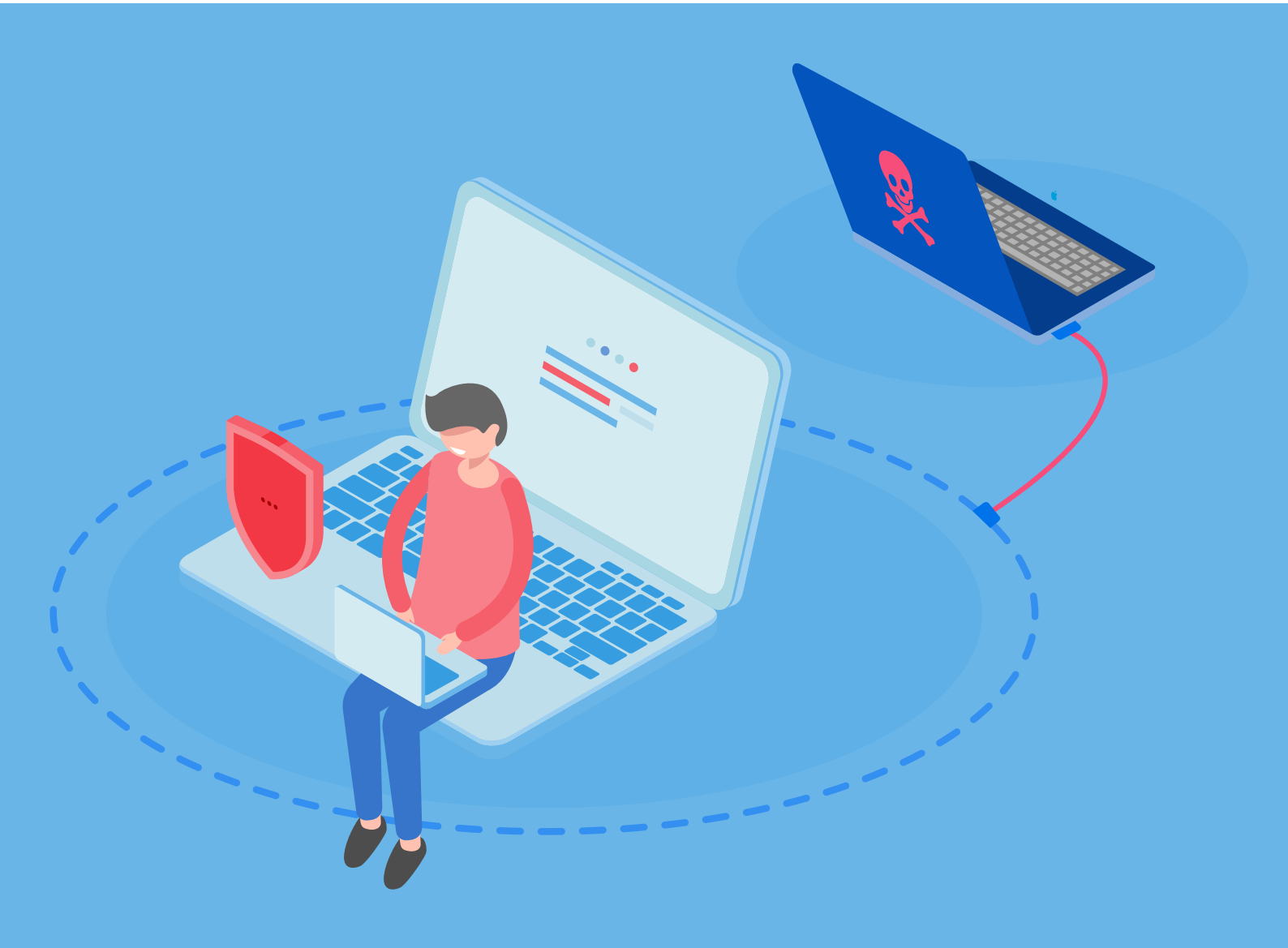
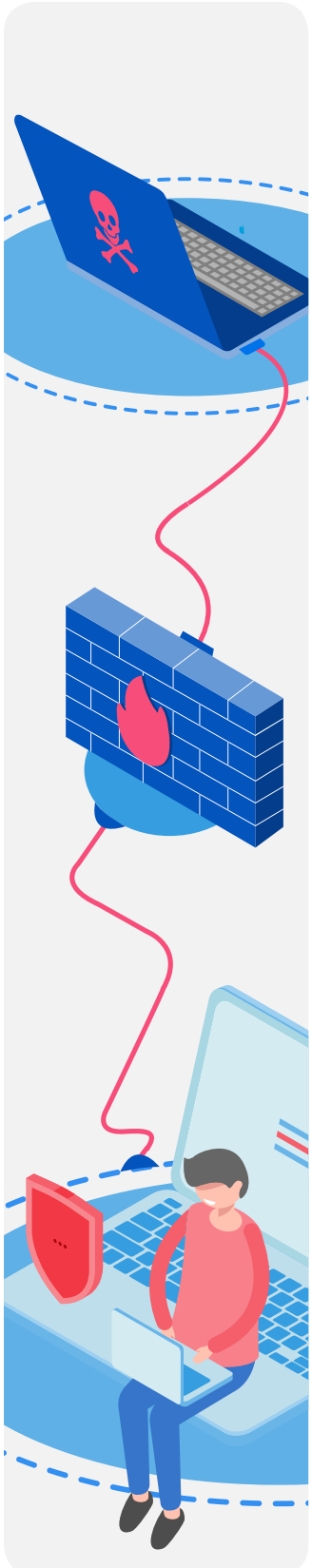
WHITEPAPER

Indusface and CARTA (Continuous Adaptive Risk & Trust Assessment)



AGENDA



INTRODUCTION

Gartner's CARTA (Continuous Adaptive Risk and Trust Assessment), which sets out their vision for security, is increasingly being adopted by a number of enterprises. Recently Gartner also called out CARTA strategic approach in the top 10 security projects for 2019. CARTA, being a strategic approach, covers a whole gamut of areas and multiple security products from end points, devices, IOT, procurement etc. contribute to different parts of CARTA.

VERY HIGH-LEVEL CARTA PRIMER

A couple of years back, Gartner introduced CARTA (Continuous Adaptive Risk and Trust Assessment) - a strategic approach to information security. With workloads increasingly moving to cloud, access being made from multiple devices and locations outside office boundaries, one-time gates are no longer sufficient and must change to be adaptive and context aware.

The CARTA approach suggests that both Risk (threat/attack) and Trust (access by entities) should not be made as a one-time gate of good/bad, allow/disallow but instead be continuously evaluated and actions taken in a dynamic, adaptive manner based on various factors like device, risk, asset value, incidents, behaviour, analysis etc. This strategy is applicable to Ops (production), Build (development) and Planning (business owners).

In this document, we talk about CARTA as it applies to Web Application Security and Indusface; applicable more to threat assessment and mitigation and not as much to trust. For this aspect, CARTA sets out a cycle of Predict – Prevent – Detect – Respond which resonates with the Detect-Protect-Monitor approach that Indusface provides.

CARTA: INDUSFACE TERMINOLOGY

PREDICT

Anticipate Threats & Exposure. (Detect)

Indusface Web Application Scanner automatically scans applications for vulnerabilities. Customers that need deeper business logic scanning will use our premium pen testing service.

PREVENT

Prevent Attacks (Protect)

Indusface WAF implements the Protect part and prevents attacks. The highly tuned advanced rule set is in block mode right from the start. Premium (custom) rules will be written and applied depending on specific customer scenarios.

Our security teams continually monitor the threat landscape and update detection and attack techniques as well as protection rules.

DETECT

Incident/breach (Protect, Monitor)

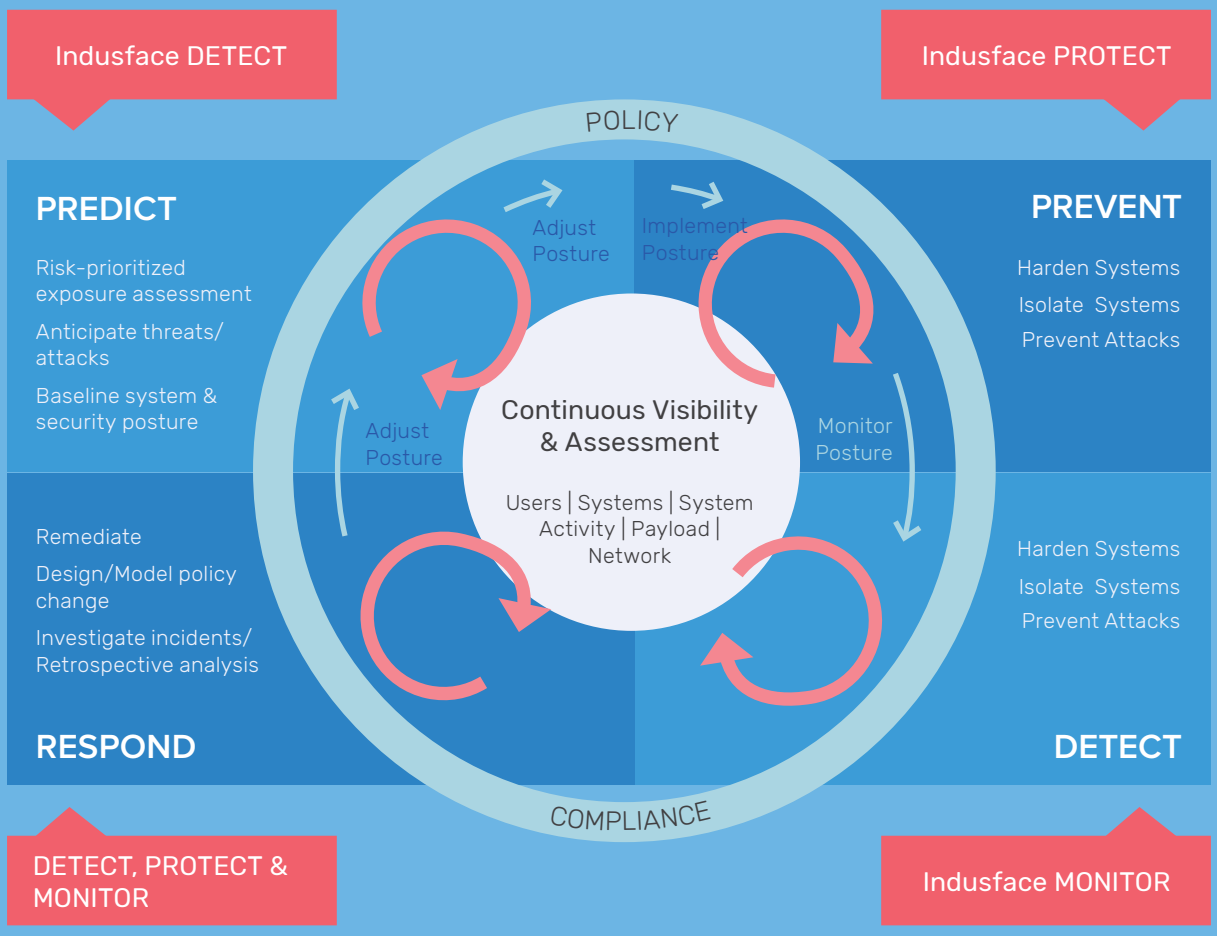
Indusface tools and teams will analyze and Monitor events to detect indicators of attempted attack and take appropriate action including automated response, alerting and getting security experts involved.

RESPOND

Remediate, analyze incidents (Detect, Protect, Monitor)

Raw and analyzed logs are stored so post facto analysis can be done by internal and customer teams. Internally, detection, prevention rules are adjusted, customized and new targeted rules written as needed in response to incidents.

CARTA RESULTS FROM THE GARTNER ADAPTIVE SECURITY ARCHITECTURE



Source: Gartner

HOW INDUSFACE USES CARTA IN ITS PRODUCT ETHOS

INTEGRATED WAS AND WAF

Vulnerabilities found by scanning have additional information associated with them that explains whether there is protection out of the box, additional rules have to be applied or a premium custom rule should be requested. Known vulnerabilities are tracked closely though they are mitigated by WAF – an attempt to attack is always interesting. Similarly, areas of the web application that are accessed in the real world but not yet scanned will be prioritized for scanning the next time a scan is performed.

DATA PIPELINE

Without data there is no analysis and timely data is required for quick response. Indusface has built a high volume, high speed data pipeline so that security and non-security events rapidly get to the backend for analysis. This augments longer term storage of raw data that can be used for post facto analysis by customers if needed.

ANALYTICS, AI, ML, AUTOMATION

"Use analytics, AI, automation, and orchestration to speed the time to detect and respond — and to scale our limited resources"

This has always been our philosophy. We use our years of experience with numerous web applications to drive what to automate like manual pen test cases -> automated scanning and automated rule generation. With the data pipeline, now we are adding more analytics and AI so our teams can focus on and prioritize security issues and incidents. This is the only scalable way to handle the sheer volume of data that is generated/collected.

ADAPTIVE PROTECTION

Allow more decisions than a simple block / allow eg. CAPTCHA, throttle, alert. These decisions are not static and depend on the behavior, context, threat assessment and vulnerability scans. This also means that IP as an identity is not sufficient, a more fine-grained knowledge of the session is needed. Sometimes this can be done by looking at the traffic while for others we need to integrate with IAM providers.

PLAY WELL WITH OTHERS

Along with the business cases like CDN integration, Let's Encrypt certificates, on a security specific basis, we are implementing API driven integration that can be used for things like getting events from Indusface (eg. SIEM), adjusting security posture, richer session identity etc.

WHAT ABOUT THE RECENT PAPER TOP 10 SECURITY PROJECTS FOR 2019?

Firstly, in Table 1 **"Foundational Security Projects and Capabilities"**: Server Protection Agents/ Security Infrastructure, WAF is one of the solutions for perimeter security controls. Of the specific 10 security projects that Gartner mentions, there are two that directly apply

CARTA-INSPIRED VULNERABILITY MANAGEMENT

1

WAF is specifically called out in the project advice as mitigating technology.

"Project Advice – Look at current threat and vulnerability management products and processes to accomplish this. Also consider mitigating technologies such as intrusion detection and prevention systems (IPDS) and web application firewalls (WAFs) that could be actively protecting for unpatched vulnerabilities."

DETECTION AND RESPONSE

2

Indusface Detect-Protect-Monitor and all the features relating to CARTA discussed above make Indusface an ideal MSSP partner.

"If you have taken a managed security services approach, consider a detection and response project that can feed valuable information into a managed detection and response (MDR) provider and/or a managed security service provider (MSSP)."

CONCLUSION

While Indusface has been doing much of this for years, using the CARTA framework to focus our approach helps us and our customers achieve Adaptive Attack Prevention.

ABOUT INDUSFACE

Indusface is an application security company protecting 1000+ global customers with its unique Total Application Security platform that detects, protects, monitors & accelerates applications. The solution is available On-Premise, As A Service (AppTrana) and through the AWS Marketplace. Mentioned in the Gartner Magic Quadrants for Application Security Testing and Web Application Firewall, Indusface has won major startup awards that include the NASSCOM-DSCI 'Security Product Company' Award, iSpirit's 'InTech50 Most Innovative Products from India' and AWS 'Regional Innovation Partner: Technology Award'. Visit Indusface and follow us on LinkedIn.