HCL **Application Security** with automated threat modeling & self-protection

An automated platform to design, build and manage application security

1. Overview

Nearly 84% of breaches occur in application software, making application security a critical business imperative. Enterprises understand that such data exploits erode stakeholder and shareholder trust, impacting brand reputation. This implicitly leads to loss of revenue as a result of decreased trust and regulatory penalties.

But an increased pace of development in enterprise security leads to business challenges such as:

Shorter product lifecycles that require constant updates to close vulnerabilities.

Multiple regulatory compliances requirements such as PCI, HIPAA, and GDPR.

Lack of skilled resources due to expensive and time consuming training process.

Uncertain resource allocation due to high degree of variability in the demand for application development.

2. What's driving changes in application security

Applications are the weakest link of an enterprise's security architecture. Despite layers of perimeter security, the applications are most susceptible to advanced, persistent threats leading to data breaches, placing the IT infrastructure at risk. Such vulnerabilities lead to significant setbacks for organizations across industries.

Enterprises need a resilient and dynamic solution to address the myriad of challenges that application security demands.

- Countering rising levels of automated, dynamic threats in the digital landscape
- Managing the scale and volume of vulnerabilities from legacy mission critical applications
- High volume of manual effort with imprecise results and large time investments
- Complexity of inter-app data exchanges makes threat discovery and identification difficult
- Lack of visibility to the application layer on a real-time basis
- Absence of any formal cloud and data based strategy for application security
- Lengthy compliance timeframes dependent on manual analytics and reporting

We at HCL understand an enterprises' needs and help tackle these challenges through:

1. Deep app forensics and automated threat modeling for app risk to combat operational errors and target a quick turnaround time by eliminating manual processes

2. Instant deployment with zero trust & workload security protection through smart cloud & data strategy by leveraging industry best practices
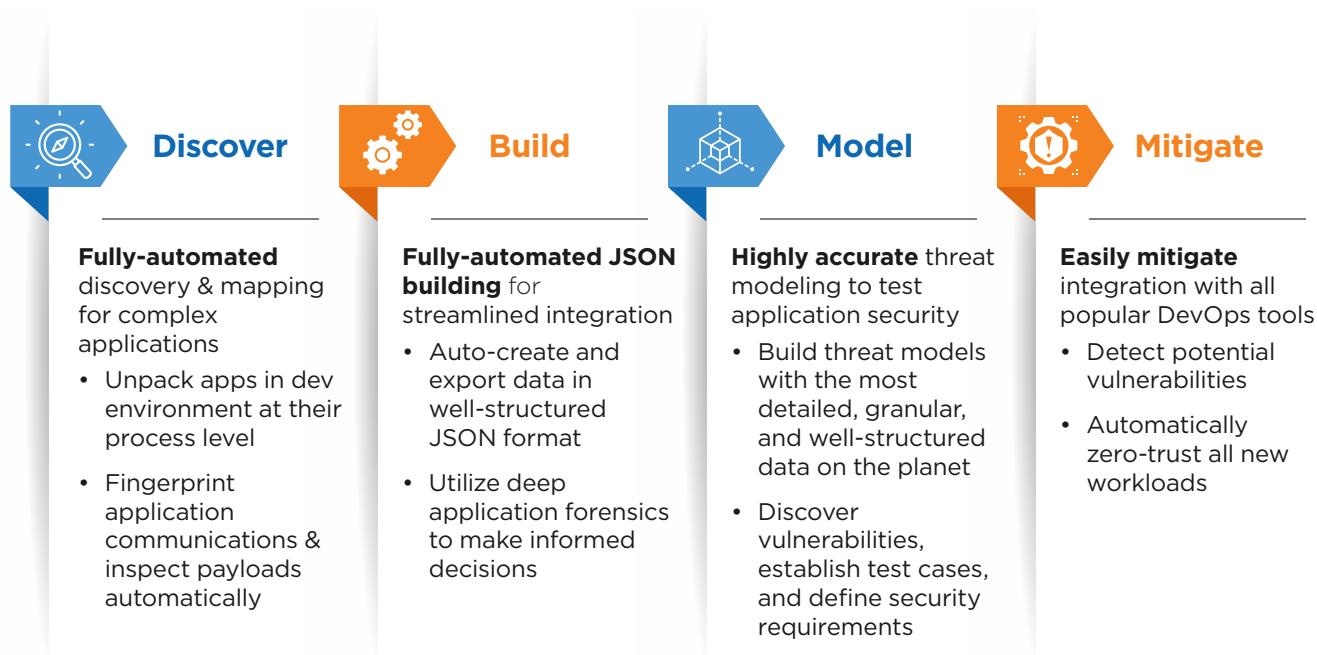
3. Automated and continuous application compliance to tackle lengthy compliance timeframes and provide cost-optimization through updated legacy applications

3. Solution overview

3.1 Comprehensive automated threat modeling

HCL helps organizations systematically process the identification, description, and documentation of the most common threats plaguing their application ecosystem. With the help of some of our partner solutions HCL is able to plug any gaps with an automated threat modeling solution that requires minimal involvement. By deploying a four-pronged automated solution, HCL enables organizations are to save time and money while also mitigating any vulnerabilities.

Discover	Build	Model	Mitigate
Fully-automated discovery & mapping for complex applications	**Fully-automated JSON building** for streamlined integration	**Highly accurate** threat modeling to test application security	**Easily mitigate** integration with all popular DevOps tools
• Unpack apps in dev environment at their process level	• Auto-create and export data in well-structured JSON format	• Build threat models with the most detailed, granular, and well-structured data on the planet	• Detect potential vulnerabilities
• Fingerprint application communications & inspect payloads automatically	• Utilize deep application forensics to make informed decisions	• Discover vulnerabilities, establish test cases, and define security requirements	• Automatically zero-trust all new workloads

3.2 Application self-protection and forensics

In addition to enabling an automated threat modeling service, HCL offers a comprehensive and automated "zero-trust" model for workloads with industry-leading AppSec solutions. This approach is designed to manage dynamic and unpredictable workloads by following a "trust nothing, verify all" paradigm. HCL's automated threat modelling application security platform can defend against threats from complex attacks, and takes advantage of enterprise IT gaps, such as misconfigured cloud, stolen credentials, and remote code injections by:

• Sanctioning and fingerprinting deep application attributes, communications, and payloads

• Deploying patented, Pico Segmentation-based zero-trust protection at runtime

• Leveraging automated software-defined controls and compliance of legacy and current-generation applications

• Using patented and self-learning Neuron function-based threat detection and protection

• Monitoring industry and IT compliance controls enforced for PCI DSS, PII, HIPAA, and NIST etc.

• Analyzing and visualizing with API integration into SIEM/SOAR and in-built reporting and dashboards

4. Automated protection for business-critical applications

Automated application threat modeling	Application self-protection with zero trust protection
Risk management: Threat modeling output used as risk assessment input	**In-depth coverage:** Deep application attributes, communications and payloads are sanctioned and fingerprinted
Alternate perspective: Provides security evaluation from the attacker's angle throughout the SDLC	**Secure complex apps:** Pico segmentation and visualization enables zero-trust protection at runtime and secures all attack surfaces
Threat list: Helps develop a prioritized threat list applicable in design and implementation	**Intelligent protection:** Threat detection based on patented self-learning neuron function
Countermeasure classification: Asset specific countermeasure selection adding relevant security controls	**Automation:** Software defined controls ensure compliance of legacy and current generation applications
Process guidance: Guides the secure code review and penetration testing process	**Compliance cover:** Enforces industry and IT compliances for PCI DSS, PII, HIPAA, NIST, and more
	Continuous monitoring: Visualized analytics from API integration into SIEM/SOAR to seamlessly built reporting and dashboards

5. Business benefits

The level of automation is a game changer with introduction of automated threat modeling into DevSecOps cycle. Automated threat modeling helps development teams to adopt an attacker's mindset, its assets and potential threats. This aids application developemnt teams in designing a more secure application system which can be more resilient to attacks.

The benefits of automated threat modeling include:

- Automated threat modeling complements other security activities such as code reviews and penetration testing when designing more secure system architecture.
- Deeply understanding the application functionality
- Create a security-focused visualization of the application's components
- Map the attacker perspective onto the architecture
- Identify vulnerabilities

- Indicate which attacks are most likely for each threat actor
- Map successful attacks to business impacts
- Real time detection & protection of known and unknown application security vulnerabilities
- Prevention from attacks evasive to network-based security solutions
- Faster vulnerability remediation with line –of-code detailing to aid developers

6. Why HCL

HCL's Cybersecurity and GRC services play a pivotal role in driving cybersecurity and risk-aligned digital transformation for global enterprises. Our proven expertise with application security across service domains enables us to provide global enterprises with automated solutions for a complete peace of mind. Powered by our "Dynamic Cybersecurity Framework", we are able to offer our customers with the tools and capabilities they need to achieve an optimized cybersecurity posture at every layer of their IT infrastructure.

Today, HCL manages the security needs of over 450 global enterprises, and has deployed over 4,500 skilled security professionals across the world who provide outcome-based, managed security services. Our key value propositions include:

Rich experience: A highly experienced team managing more than 200 customers globally in the domain of security monitoring and consulting

Industry expertise: Our application security services team provides constant remediation assistance on vulnerability fixing

Added capability: As the backbone of our managed security services, the Cybersecurity Fusion Centers (CSFCs) offer advanced security tools to run application event monitoring and threat intelligence service effectively with greater capability

End-to-end cybersecurity services: Comprehensive application security management support includes infrastructure, code scanning, monitoring, and data protection as managed services

Compliance ensured: Our services enable adherence to regulations such as HIPAA, PCI, SOX, and more with compliance scans

Seamless access: We provide a highly intuitive and customizable dashboard that provides a comprehensive application security status view

Recognition as a global leader in cybersecurity and GRC services by key analyst firms

A proprietary "Borderless Security Reference Framework" that helps clients manage their cloud security right from the foundation level to matured operations

TM

Dynamic Cybersecurity With HCL

To know more visit: **http://www.hcltech.com/cyber-security-grc-services**
or write to us at Cybersecurity-GRC@hcl.com