tCell Application Security

tCell Immunizes Web Applications and Services in Any Cloud

Securing the application is more important, but harder to do than ever. tCell was built to secure applications in the DevOps-first and cloud-first world, unlike traditional approaches, which struggle to keep pace. Uniquely architected, tCell offers rapid time to value.

SECURING THE APPLICATION IS A CHALLENGE

Security teams need to protect the application—after all, the application is the thing that delivers value to the business. But the bar is rising—the advent of DevOps, changes in application architectures (i.e., microservices) and adoption of cloud infrastructure means that application deployment velocity is rising, understanding how applications communicate is harder, and infrastructure is less predictable. For many organizations, protecting the application at the network level—which was never easy—is now becoming impossible.

TCELL APPLICATION SECURITY: VISIBILITY AND PROTECTION

Prior attempts at application security were partial pictures—either focused on dev-time vulnerabilities or production-time network traffic signatures. tCell re-defines key application security requirements:

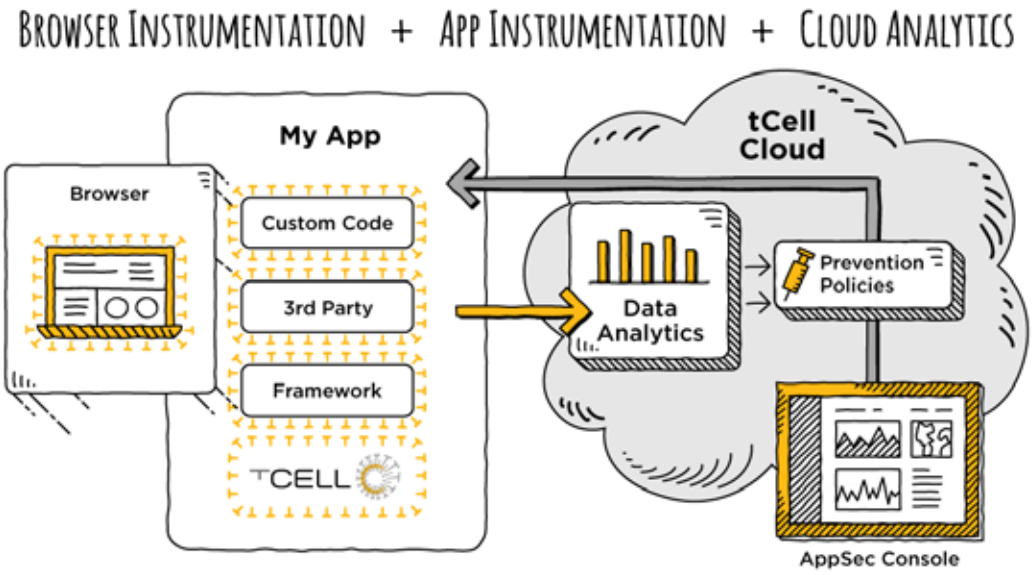
- Understand the application. Understanding the application means knowing your attack surface. tCell highlights application components (e.g, libraries, packages, API endpoints), their status, and how they communicate.
- Monitor the application. Monitoring the application means seeing how applications are being used in production, including attack attempts and actual breaches, as well as the data accessed by the application.
- Protect the application. Protecting the application means implementing policies that block threats at the application. Whether simple IP or user ID blocking, or effective content security policy deployment, tCell ensures that the application is protected.

TCELL: AN EASY DEPLOYMENT

Today's applications aren't easy to secure. With high-velocity application deployments, microservices architectures, and cloud infrastructures, organizations need flexible and portable solutions. tCell delivers.

- **DevOps:** tCell requires no change to application development, and no changes to application code.
- **Supported application environments:** tCell supports Java, .Net, Node.JS, Python, and Ruby.
- **Cloud infrastructure:** Because tCell in-app instrumentation communicates with tCell cloud-based analytics, and has no network or host dependencies, the solution is portable to any infrastructure.

tCell offers rapid time to value:
tCell begins providing insights almost immediately, requiring five minutes to install, one hour to deliver actionable information, and one day to enable active protection.



HOW IT WORKS: IN-APP INSTRUMENTATION AND CLOUD-BASED ANALYTICS

tCell uses an architecture that provides organizations both detailed application context and the big picture. tCell deploys in-app – both browser-side and server-side instrumentation which feeds cloud-based analytics. This results in app context feeding powerful analytics – resulting in low impact to the app, and actionable information for the security pro. So security teams get actionable information without lots of alerts or lots of tuning.

KEY FEATURES	HOW SECURITY TEAMS BENEFIT
Route/API Endpoint Discovery	See the API endpoints exposed by your application, which are getting traffic, which are being attacked, and which are orphaned.
Vulnerable Library Detection	Audit your 3rd party libraries. Identify vulnerable, out of date, or inconsistently deployed libraries in production.
Application Firewall	See OWASP Top 10 type attacks in real time.
Account Takeover Breach Detection	Detect and remediate stolen credential-based attacks that compromise your user accounts. For account takeover, we instrument the authentication framework.
XSS Breach Detection	Know when an XSS attack is successful. For our breach detection series of features, we monitor resources other technologies don't. For XSS, we look inside the browser, not just at server or network signatures.
Command Injection Breach Detection	Know when command injection attacks are successful. For command injection, we monitor and control the app's ability to shell out to the OS.
Suspicious Actor Blocking	Identify attackers across behaviors and shut them out before they get in.
Data Exfiltration Prevention	See and control which database columns are accessed by what API endpoints.
Content Security Policy Management and Reporting	Easily increase application security and active protection without management overhead.

TCELL ENABLES ORGANIZATIONS TO SECURE APPLICATIONS

With a simple deployment, a modern architecture, and support for the way organizations build apps and the infrastructures they build them on, tCell enables organizations to understand their applications and what's happening to them, as well as ensure that applications are protected.

TCELL

tCell
470 3rd Street, Suite 200
San Francisco, CA 94107

+1 415.326.4316 **TEL**
www.tcell.io