We have selected a handful of key software solutions that are leaders in the cybersecurity space. Our portfolio is curated to exhibit solutions that we believe are innovative and transformative to the California public sector. If you're interested in any of these solutions, please reach out to our team at sales@acuitytechnical.com

Invicti

Automation
Your security challenges grow faster than your team. That's why you need security testing automation built into every step of your SDLC.

- Automate security tasks and save your team hundreds of hours each month.
- Identify the vulnerabilities that really matter — then seamlessly assign them for remediation.
- Help security and development teams get ahead of their workloads — whether you run an AppSec, DevOps, or DevSecOps program.

Visibility
Without complete visibility into your apps, vulnerabilities, and remediation efforts, it's impossible to prove you're doing everything you can to reduce your company's risk.

- Find all your web assets — even ones that have been lost, forgotten, or created by rogue departments.
- Scan the corners of your apps that other tools miss with our unique dynamic + interactive (DAST + IAST) scanning approach.
- Always know the status of your remediation efforts, through Invicti or native integrations with your issue tracking and ticketing software.

Accuracy
Head-to-head tests by independent researchers show that Invicti consistently identifies more vulnerabilities than other scanning tools. And returns fewer false positives.

- Find more true vulnerabilities with our unique dynamic + interactive (DAST + IAST) scanning approach.
- Let no vulnerability go unnoticed with combined signature and behavior-based testing.
- Detect vulnerabilities quickly with comprehensive scanning that doesn't sacrifice speed or accuracy.

Scalability

- Reclaim the hundreds of hours your team spends chasing down false positives with features that confirm which vulnerabilities are real threats.
- Integrate security testing into your entire SDLC with powerful two-way integrations into the tools your development team already uses.
- Control permissions for unlimited users — no matter how complex your organization's structure.

Proactive
The longer a vulnerability lasts in your SDLC, the more costly it is to fix. Invicti helps you prevent vulnerabilities by showing your developers how to write more secure code in their existing environment. Because the easiest vulnerabilities to manage are the ones that never exist in the first place.

- Build security into your culture by integrating Invicti into the tools and workflows your developers use daily.

- Give developers access to actionable feedback that helps them produce more secure code — which means less work for your security team.
- Prevent delays with continuous scanning that stops risks from being introduced in the first place.

Dynatrace is a software-intelligence monitoring platform that reduces the complexity of enterprise cloud environments and speeds up digital transformation. Dynatrace provides information about your app performance, their infrastructure, and your end user's experience using AI and automation. Dynatrace can completely automate your enterprise cloud operations, and create software faster using:

Infrastructure Monitoring.
Dynatrace delivers simple and automated infrastructure monitoring that provides broad visibility across your hosts, VMs, containers, network, events, and logs. Dynatrace continuously auto-discovers your dynamic environment and pulls infrastructure metrics into their Davis® AI engine, so you can consolidate tools and cut MTTI.

Applications and Microservices.
Dynatrace provides automated, code-level visibility and root-cause answers for applications that span complex enterprise cloud environments.

Digital Experience Monitoring (DEM).
Dynatrace DEM provides Real User Monitoring (RUM) for every one of your customer's journeys, synthetic monitoring across a global network, and 4K movie-like Session Replay.How is Dynatrace Different From Other Cloud Monitoring Solutions?

Dynatrace is automated from deployment to instrumentation, discovery, dependency mapping, baselining, problem identification, and root-cause. All that is required is the installation of a single agent. While other solutions monitor and report on numerous metrics, Dynatrace provides context. This includes understanding and mapping all the relationships and interdependencies, top to bottom, from end-user experience all the way down to the infrastructure. Last, Dynatrace uses AI or AIOps. While some solutions have machine learning, Dynatrace uses Davis AI engine to process billions of dependencies in milliseconds.

CounterCraft provides a distributed Deception Platform that creates automated digital breadcrumbs to bait adversaries into thinking they are penetrating companies' networks. This innovative cybersecurity approach allows CounterCraft to get information on attackers and objectives while misdirecting them.

Their solution deploys deception-based campaigns and offers deep monitoring and complex response actions. The Cyber Deception Platform is currently used by governments, law enforcement agencies, and Fortune 500 companies – proving our craft and expertise in IT security. It runs automated counterintelligence to discover targeted attacks with a real-time active response and zero false positives.

OneTrust LLC provides provides privacy management software platforms that help organization comply with data privacy, governance, and security regulations. They have a tool specific to the California Consumer Privacy Act (CCPA). Their solution automates responses to consumer rights and Do Not Sell Requests.

Consumer rights requests - Automate consumer rights requests from intake through fulfillment.

Opt-Out of Sale - Enable opt-out of sale across web, mobile, and CTV, automating record keeping & communication to third-parties.

Data Mapping Automation - Automate the discovery, classification, and mapping of California consumer data.

Incident Management - Get guidance for California rules and streamline notifications for impacted parties.

Their solutions range from privacy management, data governance, consent/governance, and IT Risk/security management

SentinelOne is a comprehensive enterprise security platform that provides threat detection, hunting, and response features that enable organizations to discover vulnerabilities and protect IT operations. SentinelOne integrates static artificial intelligence (AI) to provide real-time

endpoint protection and reduce false positives that derail investigations or make threat detection a capital-intensive process.

Their platform includes:

Threat Detection
Detecting threats in real-time supports immediate response that mitigates discovered threats before they harm IT ecosystems. SentinelOne uses a patented Behavioral AI feature to recognize malicious actions and patterns. Threat detection is applied to detect file-less, zero-day, and nation-grade attacks. The integration of AI ensures threats are discovered in in a timely manner which reduces the effects of ransomware and phishing attacks.

Threat Hunting
Organizations should make it a goal to have a proactive process to discovering threats rather than a reactive one. Proactive threat hunting ensures attacks are sought out before they reach an enterprise network or infrastructure. SentinelOne delivers quick query times, and advanced actions when threat hunting. The advanced actions include pre-indexed forensic context to understand the motive behind attacks, full-native remote shell, and more.

AI Assisted Prevention
SentinelOne integrates Static AI on endpoints to prevent attacks in real-time. The integration of AI ensures threats are quickly culled and dealt with before they can affect network systems. The SentinelOne prevention model can be more efficient than legacy antivirus solutions as it produces low false positives while focusing on preventing real threats.

Automated Response
SentinelOne makes use of ActiveEDR to respond to issues within a network. ActiveEDR integrates behavioral AI and is capable of surgically reversing and removing malicious activities. Organizations can automate the response process to ensure it occurs in real-time. The AI-assisted response ensures devices connected to enterprise networks can individually respond to threats in real-time.

If you just opted in, you're consenting to receive marketing emails from: Acuity Technical Solutions, 9171 E Laguna Way, Elk Grove, CA 95758. You can revoke your consent to receive emails at any time by using the SafeUnsubscribe® link, found at the bottom of every email. Emails are serviced by Constant Contact