dynatrace

Keeping government applications secure

The role of application security in today's threat landscape

Dynatrace adds Application Security to the Dynatrace for Government platform

INTRODUCTION

A clarion call

Throughout the public sector, government leaders are sending a clear message: As we continue to pursue a cloud-enabled digital transformation, we must dramatically reduce the vulnerabilities of our expanding cyber ecosystem.

This arrives at a time when agencies everywhere — from those overseeing military weapon systems to IRS e-filing resources to school lunch programs to state budgets to agriculture initiatives — are increasingly dependent on applications as they invest in more cloud, analytics, artificial intelligence/machine learning (AI/ML) and internet of things (IoT) tools. Yet, in a rush to bring these products to market, developer teams may consider security as an afterthought.

Such thinking could expose agencies — a pattern that government leaders are seeking to stop in its tracks at a time when they are committing to zero trust.

In response, Dynatrace has significantly enhanced the Dynatrace for Government platform with Application Security, allowing organizations to gain visibility into pre-production and production vulnerabilities while securing applications at runtime for automatic and continuous protection.

With Dynatrace Application Security, agency IT teams — whether federal, state, local or education (SLED) — can acquire and deploy applications with confidence they will always have the context required to make informed, prioritized decisions about potential issues. Then, they proceed with rapid remediation regardless of whether vulnerabilities originate internally or via the supply chain.

This white paper will reveal what's at stake with the increasing need to acquire applications that are not only productive but safe — and how Dynatrace can help.

> **The security of software…is vital to the federal government's ability to perform its critical functions…**
>
> — May 2021 White House Executive Order on Improving the Nation's Cybersecurity

SECTION 1

IT modernization raises the bar for cybersecurity

Recent legislation and policies are driving agencies toward profound IT modernizations.

In January 2023, President Biden signed into law the FedRAMP Authorization Act as part of the National Defense Authorization Act for Fiscal Year (FY) 2023. The act includes what is called a "presumption of adequacy" provision, which directs agencies to presume that a cloud service has adequate security controls if it has already achieved FedRAMP authorization from another agency.

This means that the number of government-used applications will only continue to proliferate, making application security all the more mission-critical: In FY 2022, agencies reused FedRAMP-authorized cloud products more than 4,500 times, a 60 percent increase from the prior year.

However, most security tools today cannot address the threats these applications introduce, creating a cyber defense gap. Government leaders recognize this gap and have responded accordingly:

- The May 2021 White House Executive Order on Improving the Nation's Cybersecurity notes that the "security of software … is vital to the federal government's ability to perform its critical functions … There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended."
- In November 2021, the Cybersecurity and Infrastructure Security Agency (CISA) released its Binding Operational Directive 22-01, which presented a CISA-managed catalog of known exploited vulnerabilities carrying serious risks and required agencies to review and update their procedures to remediate the vulnerabilities.
- Most recently in March 2023, the White House published its National Cybersecurity Strategy, which seeks to hold technology companies more accountable for the safeguarding of their offerings while leveraging federal purchasing power to incentivize security.

Similarly, SLED agencies are facing their own threat-related challenges as they too invest in IT modernization, and are more determined than ever to reduce their attack exposure. With concerns rising about the growing presence of user applications everywhere, 67 percent of SLED security, IT and operations teams are allocating more than 10 percent of their technology edge investments on cybersecurity, notably more so than the healthcare, finance and manufacturing sectors. They are also seeking to accelerate their usage of applications with security as a top focus through StateRAMP.

These and other developments signify that agency IT purchasing decision-makers and their vendors realize they cannot afford to view security as an afterthought. They know they need to take a proactive, strategic approach to protecting applications from the very start to finish.

Dynatrace collaborates closely with government customers to help them achieve this goal by providing automated and intelligent application security capabilities. In the following sections of our white paper, we'll elaborate upon how we're making this possible.

SECTION 2

Dynatrace public sector platform gets major application security boost

Just one application security gap could jeopardize an entire mission, resulting in a wide range of consequences: Thousands of veterans may not receive benefits notifications. Traffic lights on a busy stretch of road could go dark. An Army unit may lose communications with an intelligence, surveillance and reconnaissance (ISR) drone tracking enemy movements.

At Dynatrace, we understand the critical nature of these and endless other real-life scenarios. To close security gaps, we have augmented our Dynatrace for Government platform with Dynatrace Application Security, which brings automatic, intelligent and highly scalable defense capabilities.

As a result, we're overcoming current limitations in application protection tools and processes: Traditionally, security or IT operations teams run security scans strictly in pre-production. But they end up with a static view at a single point in time, reducing the effectiveness of these efforts.

Container security and other modern tools provide runtime visibility. But they are still restricted in their ability to detect libraries that are actually in use, for example, as opposed to those that are present, but unused. What's more, they can't deliver deep insights if teams don't have source code access.

The software supply chain further complicates matters. In many cases, one public sector contractor will build the application, and then another will run it. But the latter contractor doesn't have everything needed to document what went into production, which means agency teams don't have this either. The White House executive order and cybersecurity strategy call out the lack of transparency and awareness in the software supply chain as a key area for improvement.

To release applications confidently in modern dynamic environments, it's essential to have full visibility into everything running on a continuous basis. The Dynatrace for Government platform reveals these insights down to individual transactions with code-level detail and almost no overhead, therefore supporting essential zero trust tenets.

Core Components of a Winning Platform

These innovative tools are the core technology components that power Application Security within the Dynatrace for Government platform

Our Davis AI engine powers the automation while continuously watching over entire pre-production and production environments. It identifies any changes and reveals precise answers about the source, nature and severity of vulnerabilities as they emerge in real-time. Davis automatically analyzes and prioritizes alerts and eliminates false positives, helping teams focus on what matters so they can understand risks in context.

OneAgent collects all monitoring data with leading technologies, as well as operational and performance metrics.

PurePath lends full insight into applications, including the entire dependency tree of open-source or third-party libraries.

SECTION 3

New platform features bring "total package" capabilities

As indicated, application security brings visibility into pre-production and production while enabling both runtime vulnerability analytics (RVA) and runtime application protection (RAP). Dynatrace recognizes that federal and SLED teams simply do not have the personnel resources required to manually address the growing complexities of application acquisition and protection. That's why we have positioned the automation of application security tasks as a primary driver of Dynatrace for Government.

Specifically, the platform's "total package" application security capabilities are made possible by the following:

Automatic and continuous vulnerability detection with 100 percent runtime visibility
The platform detects vulnerabilities in real-time at runtime. Even if checks are not integrated into the pipelines across all teams — or if the checks are bypassed deliberately — Dynatrace will pinpoint vulnerabilities instantly.

Vulnerability management from detection to closure
Automatic runtime detection and real-time visibility into the evolution of vulnerabilities. Because Dynatrace provides risk assessments, teams can prioritize which issues to address first.

Detection and blocking
Based on code-level insights and transaction analysis, Dynatrace identifies whenever user-generated inputs are sent to vulnerable application components without sanitization. With this, the module blocks SQL injections, command injections and attacks targeting zero-day vulnerabilities like Log4Shell automatically, without configuration.

Deep insights into production execution
This includes open-source components as well as closed-source software and Kubernetes workloads. We deliver absolute insights into applications — not only of development code and open-source libraries, but transactions that involve third-party/supply chain products for which teams have no source code access.

Complete coverage across production rollbacks and outdated releases, feature flags, canary and blue/green deployments
Unlike traditional approaches, agency teams identify vulnerabilities that are accidentally reintroduced in rollbacks or are — while known and even fixed — still posing a threat because of outdated components.

Security scores enriched with context

Teams too often rely solely on ratings from the Common Vulnerability Scoring System (CVSS), an open-industry standard for assessing the severity of these issues. But CVSS without context leads to incorrect or misidentified risk and prioritizations. The module goes beyond CVSS assessments with our Davis Security Score, which examines how vulnerabilities are impacting real-user sessions and whether they're connected to a database or reachable from the public internet.

This real-time awareness results in the rating of severities more fully, precisely and, again, automatically. In combining the gravity of the situation with exposure information, it allows teams to determine if they've loaded a vulnerable library, and how relevant this is within the context of the entire environment. Thus, teams recognize which potential exposures need immediate investigation.

Reduction of false positives

The platform reduces false positives and flags biggest risks with automatic and precise impact assessment. It analyzes attack vectors to discover if suspect libraries are called and used at runtime.

Automatic updates with real-time changes

Without any configuration required, Dynatrace auto-detects changes in application environments, such as container dynamics, elastic scaling, multi-version deployments, runtime container updates, rollbacks, A/B tests and blue/green deployments.

"Crown jewel" protection and comprehensive reporting

With service flow analysis from publicly available data, the platform automates the protection of mission-critical information assets. In addition, teams learn about the potential business impact of a vulnerability in context to support comprehensive risk reporting for their chief information security officers (CISOs).

Ideal collaboration

Teams collaborate more effectively using a single source of truth, including real-time vulnerability impact data and forensic analytics down to code level for developers and security specialists.

With Dynatrace observability monitoring all environments from pre-production to production and identifying vulnerabilities at runtime, teams benefit from full visibility into hybrid enterprise clouds, containers and workloads — with zero configuration. We understand that if applications are compromised, then the mission could be compromised as well.

To learn more about how our Dynatrace for Government platform and Application Security Module can support an optimal state of security for your agency, please contact us.

Dynatrace (NYSE: DT) exists to make the world's software work perfectly. Our unified software intelligence platform combines broad and deep observability and continuous runtime application security with the most advanced AIOps to provide answers and intelligent automation from data at enormous scale. This enables innovators to modernize and automate cloud operations, deliver software faster and more securely, and ensure flawless digital experiences. That's why the world's largest organizations trust Dynatrace® to accelerate digital transformation.

Curious to see how you can simplify your cloud and maximize the impact of your digital teams? Let us show you. Sign up for a free 15-day Dynatrace trial.

dynatrace

dynatrace.com blog @dynatrace

05.03.23_BAE4615.WP.USLet_cs