Reveal security

Solution Brief

TrackerIQ for ServiceNow

Continuous threat detection combats data leakage and malicious actors

servicenow

Benefits

- Detect malicious insider activity such as changes to workflow automation and security settings
- Enable faster mean-time-to-detection (MTTD) of insider threats
- High-fidelity alerts enable focus on real threats and improves response times
- Stop leakage of sensitive data managed by ServiceNow, such as CMDB
- Deploy compensating controls to monitor human and machine access

Overview

ServiceNow, a global workflow automation leader, streamlines enterprise operations with ticketing, reporting, and integrations. Improving ServiceNow security is crucial for risk reduction. Despite proactive posture management, continuous threat detection is vital to detect breaches and insider threats. Persistent bad actors targeting SaaS applications emphasizes the need for a holistic security approach, combining posture management and vigilant threat detection to safeguard ServiceNow and uphold digital workflow integrity.

TrackerIQ, by RevealSecurity, enhances security by continuously monitoring user activity, identifying potential threats like unauthorized data export from tables such as CMDB. TrackerIQ also provides compensating controls by monitoring API usage, and changes to ServiceNow workflows and security settings, quickly detecting anomalous activity that could be indicative of a compromise or a malicious insider.

Data Leakage Creates Exploitable Attack Vectors

ServiceNow manages critical enterprise information, notably in Configuration Management Database (CMDB) tables, housing hardware and software details and their interdependencies. Leakage on this information can provide an attacker (internal or external) very valuable reconnaissance information, including IP addresses, OS versions, applications and patch levels. But despite ServiceNow granular permission model for access control, locking down user permissions is extremely challenging due to the variety of external users accessing the ServiceNow tenant.

TrackerIQ enables critical compensating controls that monitor user activity in ServiceNow. This enables the accurate identification of concerning or malicious behavior, such as the export of sensitive information from tables like CMDB, Incidents, and Tasks. These behaviors can be strong indicators of system misconfiguration, broken access control, or impersonation.

API Connectivity Can Put ServiceNow Data at Risk

ServiceNow integrates with various API-enabled systems, allowing connections to third-party applications and data sources. While enhancing operational efficiency, poorly configured integrations pose a risk to ServiceNow data.

TrackerIQ enables continuous monitoring of API connections to ServiceNow, heavily scrutinizing all connections - even trusted connections - for unusual activity. The result is the identification of anomalies that indicate potential compromises and allowing the security team to fully understand what data is being accessed.

Control Modification of Workflows and Security Policy

ServiceNow enables workflow automation, allowing attackers or insiders with the right credentials to make real changes in IT infrastructure and workflows, potentially leveraging these alterations to achieve malicious goals.

In addition, ServiceNow provides security configuration options to fortify its platform. Tightening these settings is an important step in minimizing opportunities for risky or malicious activity. However, this is only an initial first step and continuous monitoring is necessary to ensure that these settings are not changed by a ServiceNow administrator or an external attacker.

TrackerIQ uses sophisticated behavioral analytics to monitor how users - including privileged users such as administrators - interact with ServiceNow, enabling detection and alerts when suspicious behavior such as changes to workflow automation or security settings is detected.

About TrackerIQ

TrackerIQ uses patented user journey analytics to model how users interact with ServiceNow and delivers detailed alerts when suspicious behavior is detected. TrackerIQ operates out-of-band using log data integrations, so it's completely non-disruptive to your critical business applications.

TrackerIQ's application-independent approach translates the often cryptic logging terminology of individual applications into a normalized format for analysis. From there, user journey analytics, based on unsupervised machine learning, develops micro-personas representing your trusted users and establishes baselines of their normal behavior. This includes user journeys that span multiple applications for maximum context and accuracy. Ongoing application usage of trusted identities is compared to past journeys by the same individual and comparable peers, and information-risk alerts are generated when high-risk anomalies are detected.

About RevealSecurity

Reveal Security is an identity threat detection company that delivers accurate behavior-based user analytics without rules. This allows organizations to cost effectively detect, alert and quickly respond to the abuse and misuse of trusted identities operating inside and across the mission-critical applications that drive their business.

For more information,
visit www.reveal.security