Essential Guide

Continuous Asset and Identity Intelligence

Reduce enterprise risk, accelerate investigations, and uncover compliance gaps in security controls with continuous asset and identity discovery.

splunk>

As organizations extend their digital presence across cloud, hybrid, on-premises, OT, and IoT systems, security operations teams struggle with accurately and efficiently identifying their extensive array of network assets — encompassing devices, users, and applications. Despite deploying numerous systems to manage different asset types, security teams continue to grapple with:

- Inaccurate asset data.
- Slower investigations due to a lack of asset and identity context.
- Measuring compliance against security controls.

Security teams spend valuable time and resources on basic asset management due to fragmented, outdated, or inaccurate data provided by asset management tools and Configuration Management Databases (CMDBs). Tracking down necessary asset data, and collecting and reconciling asset information is a time-consuming, manual process. Security analysts often spend excessive time correlating alert data with assets and identities during investigations. Without a comprehensive, up-to-date view of all unique assets, security operations teams must cross-reference multiple tools and make assumptions about the relationships between devices and users. Security teams struggle to measure compliance against security controls and spend countless hours each quarter preparing asset inventories and compliance reports for internal and external audits.

Asset and identity visibility is a critical need that continues to be a problem for many organizations; you can't protect what you can't see. As security compliance regulations become increasingly stringent and cyber insurers demand greater transparency into an organization's security posture, the significance of asset visibility can't be overstated.

What is continuous asset and identity intelligence?

Continuous asset and identity Intelligence is a transformative approach to managing and securing the vast array of assets within an organization. By drawing from diverse data sources, it continuously discovers, monitors, and builds an accurate inventory of assets and identities, including endpoints, servers, users, applications, cloud, OT/IoT systems, and more. This ensures that teams have a real-time, comprehensive view of the entire network asset landscape.

This approach goes beyond mere discovery by continuously updating the inventory of assets and identities. It correlates data across multiple sources — including network, endpoint, cloud, and vulnerability scanning tools — eliminating stale data to ensure that the asset inventory remains accurate and comprehensive. This foundational insight is crucial to reduce risk exposure and eliminate blind spots.

Limitations of traditional asset management tools

There are many tools that attempt to solve the asset visibility problem, but they often create additional issues. These tools are typically siloed, each with its own capabilities and use cases, leading to fragmented and inconsistent asset data. So, while there are numerous tools attempting to solve the asset visibility problem, the reality is that these tools are simply falling short. Let's explore why:

Configuration Management Database (CMDB)

CMDBs are designed to maintain an inventory of IT assets and their relationships. They aim to provide a single source of truth for configuration data. However, they often fall short because they rely heavily on manual updates, leading to incomplete and outdated information. Moreover, they usually lack real-time data integration and fail to reflect the dynamic nature of modern IT environments.

IT Operations Management (ITOM)

ITOM tools focus on the administration of the IT infrastructure, including hardware, software, and network components. They help monitor and manage those assets' performance. While ITOM tools provide valuable operational insights, they often don't integrate well with security tools, resulting in siloed information that is not easily accessible for security teams.

Cyber Asset Attack Surface Management (CAASM)

Geared towards identifying and managing the attack surface of an organization, CAASM tools help discover unknown assets and assess vulnerabilities. However, these tools typically lack comprehensive asset management capabilities and don't integrate deeply with compliance or IT operations systems. This makes it difficult to get a complete picture of the asset landscape.

Cloud Security Posture Management (CSPM)

CSPM tools are designed to manage and improve the security posture of cloud environments. They focus on detecting misconfigurations and compliance issues in cloud settings. While CSPM tools are essential for cloud security, they often don't cover on-premises or hybrid environments, leading to gaps in asset visibility and management.

Each of these tools addresses only a part of the problem, so security teams have to juggle multiple systems to get a comprehensive view. This is where the challenge lies: The more tools you use, the more fragmented your asset visibility becomes. Security teams end up with disconnected data, making it difficult to get a unified, accurate, and up-to-date picture of their assets and identities.

5 essential capabilities of continuous asset and identity intelligence

1. Continuously updated asset inventory

For security teams, the value of maintaining a continuously updated asset inventory cannot be overstated. This practice makes sure devices, users, applications, and user identities are accounted for, updated, and monitored in real time, helping teams detect and respond to potential vulnerabilities and threats quickly.

An up-to-date inventory also allows for more precise risk assessments and better allocation of security resources. By minimizing gaps in security coverage and reducing the challenge of oversight, it also ensures all assets are protected according to the latest security protocols and compliance requirements.

2. Asset data enrichment

By supplementing basic asset and identity information with additional context such as network activity, asset associations, and asset health, security teams gain a deeper understanding of their assets' security posture. Enriched asset data allows for more nuanced risk assessments and more informed decision making, helping security teams prioritize vulnerabilities and respond to threats with greater precision and speed. Enriched asset data also helps detect anomalies and patterns that might indicate a security breach, facilitating faster and more accurate incident response.

3. Out-of-the-box (OOTB) and custom compliance metrics frameworks

The integration of both OOTB and customizable compliance metrics frameworks within asset and identity intelligence are essential for organizations to measure compliance against common security frameworks, identify gaps in security controls, and drive improvements in overall security posture. OOTB frameworks provide immediate, standardized compliance assessments based on widely recognized regulations and standards like CIS Critical Security Controls, ISO 27001, NIST, PCI DSS, and HIPAA — allowing security teams to quickly align with industry best practices.

Customizable frameworks allow organizations to tailor their compliance and security measures to fit unique operational needs or to address specific risks. This flexibility is crucial for adapting to evolving threats, changing regulations, and the specific risk landscape of your organization.

4. Seamless integration with security information and event management (SIEM)

Integrating continuous asset and identity intelligence into a SIEM solution brings invaluable benefits. By enriching SIEM capabilities and providing detailed and contextual data about every asset and user identity within the organization, the SIEM can more effectively correlate security events with specific assets and identities, detect patterns of abnormal behavior, and flag potential threats with greater accuracy. The integration also facilitates automated responses and streamlined workflows, enabling faster and more effective incident response.

5. Bidirectional integration with CMDB

A key capability of continuous asset and identity intelligence is its bidirectional integration with CMDBs. This integration enhances both the asset discovery process and the accuracy of the asset inventory. Asset and identity intelligence pulls data from the CMDB to enrich the asset discovery process. Using existing data within the CMDB, ensures that asset discovery is more comprehensive and accurate. This process also allows for reporting compliance with the CMDB by identifying all discovered assets that are not currently recorded, highlighting gaps and discrepancies.

In addition, pushing enriched, accurate, and complete asset data back to the CMDB ensures that the CMDB is continually updated with the most current asset information.

This bidirectional integration not only enhances the accuracy and completeness of asset data but ensures security operations are based on the most reliable information available.

Top use cases for continuous asset and identity intelligence

Continuous asset and identity intelligence provides organizations with the ability to effectively safeguard their digital environments. By integrating continuous asset and identity intelligence into security workflows, businesses gain valuable insights to drive security operations and risk management. Key use cases for enhancing security and overall digital resilience include:

Asset and identity discovery

In today's complex environments, organizations face significant challenges in accurately discovering and managing an ever-expanding array of assets and identities. Continuous asset and identity intelligence addresses these challenges by providing comprehensive visibility into digital resources.

It enables real-time discovery of assets and identities, ensuring every device, user, and application is accounted for and monitored. This gives organizations an up-to-date inventory, enhances security by ensuring all assets are under governance and compliant with security policies, and reduces the risk associated with unauthorized access and data breaches.

Compliance reporting

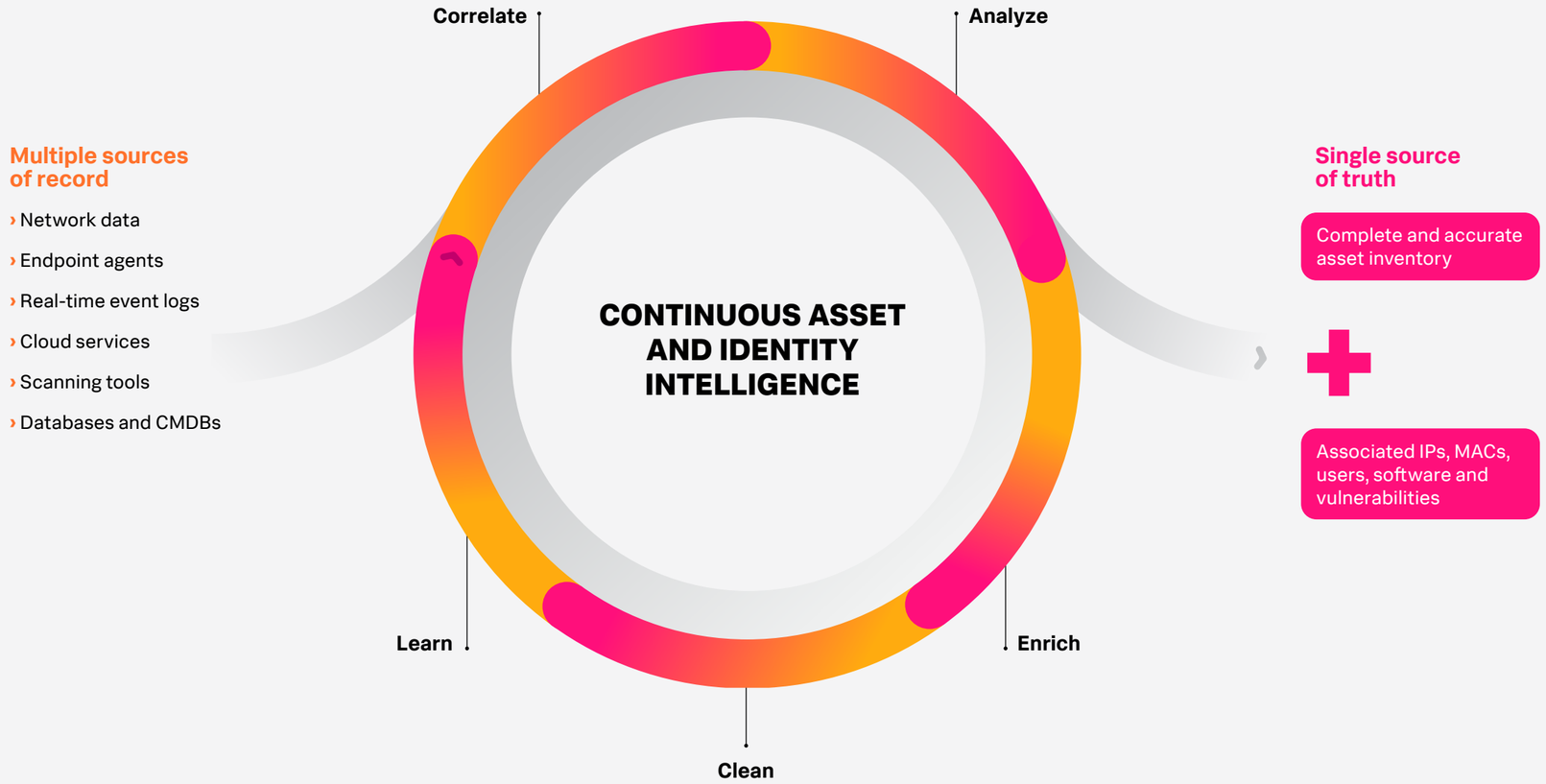
Security and risk teams often spend considerable time preparing asset inventories for audits. One of the most common challenges in asset management for compliance and audits is accurately tracking and accounting for in-scope assets in their environment, and identifying when assets lack critical security controls.

Continuous asset and identity Intelligence mitigates these challenges by providing a unified view of all assets, measuring compliance against common security frameworks such as CIS Critical Security Controls, ISO 27001, NIST, PCI DSS, and HIPAA. With continuous asset and identity intelligence, security teams can proactively identify and close security control gaps in compliance as they occur. Additionally, they can demonstrate improvements in compliance over time, making the audit process more efficient and less time consuming.

Asset investigation

Sprawling digital landscapes and the complexity of tracking assets' interactions and dependencies can obscure visibility and make it difficult for security teams to pinpoint and respond to threats efficiently. Asset and identity intelligence provides deep, contextual insights into every asset.

An up-to-date, comprehensive asset inventory helps security analysts correlate alerts, understand the relationship between devices and users and view an asset's current and historical state. This helps teams quickly gather the context and detail needed to inform and accelerate investigation and response.



Enter Splunk

Splunk offers a robust continuous asset and identity intelligence solution for businesses to gain accurate asset inventories and a single source of truth for assets and identities. Splunk Asset and Risk Intelligence (ARI) is designed to help security teams conduct faster and more thorough security investigations with accurate asset and identity context, identify gaps in compliance, and reduce risk exposure.

Comprehensive and continuous asset visibility to reduce risk exposure

With information fragmented across silos, SecOps teams can struggle to get asset visibility into potential attack surfaces, ask asset-related questions, get answers, and take action.

With Splunk Asset and Risk Intelligence, teams leverage the rich data in Splunk to gain a continuously updated inventory of assets and identities by correlating data across multiple sources — including network, endpoint, cloud, and scanning tools. This eliminates stale data, ensuring that your asset inventory is always accurate and comprehensive.

The solution analyzes asset information from multiple sources, finds pattern similarities, and identifies when different systems report the same asset to provide a single view of the asset and identity. This ensures accurate recognition and reconciliation of the data as one asset and identity, not multiple, maintaining accuracy and consistency in asset inventory.

Splunk Asset and Risk Intelligence also enhances asset visibility across IT and SecOps with a bi-directional CMDB integration. ServiceNow asset records are updated with asset and identity intelligence, which allows teams to identify devices that are not in the CMDB solution to make sure they are properly managed. An automated ticketing integration sends non-compliant assets from Splunk Asset and Risk Intelligence to the CMDB to close gaps in security controls.

The level of detail and immediacy provided by Splunk Asset and Risk Intelligence greatly enhances an organization's ability to manage risk effectively, ensuring that security postures are robust and proactive rather than reactive.

Accelerate security investigations with accurate asset and identity context

Correlating alert data with specific assets and identities during investigations can be difficult when there's a lack of contextualized, accurate asset data available to teams. Security teams often lack a real-time, comprehensive overview of assets and, as a result, need to cross-reference multiple tools and make assumptions. This slows down the investigation process and delays alert triage and incident response. Splunk Asset and Risk Intelligence provides accurate asset and identity context to focus and shorten investigations.

Through contextual asset insights and user identity and application relationship mapping, the solution helps security teams quickly identify who is associated with what asset and when. This reduces the time spent pivoting to other systems to understand the assets involved in an attack and the potential risk to the organization. Security teams can easily interpret the data and get the information needed.

Splunk Asset and Risk Intelligence enriches and adds more context to the assets that are continuously discovered. It pulls together data from vulnerability and software scanning tools to inform teams about what software and vulnerabilities exist on their systems. It also accurately attributes IP addresses to assets and identities to reduce the laborious, manual searches through logs that teams need to do to try and correlate what assets or identities were associated with what IP addresses and when. With Splunk Asset and Risk Intelligence, security teams have a simple, convenient, and fast way to enrich investigations with accurate asset and identity information to quickly understand the asset at risk.

Integrating seamlessly with Splunk Enterprise Security (ES), Splunk Asset and Risk Intelligence continuously updates and populates the ES Assets & Identities framework with the latest asset information, and provides comprehensive asset context for ES notable event enrichment. This added asset context and visibility reduces investigation times through better detection and focus.

Uncover compliance gaps in security controls

Many organizations struggle to get visibility of all necessary assets, putting them at risk of compliance violations and potential cyberattacks. Security and risk teams spend considerable time preparing asset inventories for audits, but the lack of effective tools for asset discovery and endpoint compliance makes it difficult to manage known and unknown network endpoints. This creates gaps and risks non-compliance, elevating overall organizational risk exposure. With Splunk Asset and Risk Intelligence, organizations can understand and improve their compliance and security posture with out-of-the-box and customizable dashboards and metrics. By leveraging compliance framework controls, the solution provides a clear lens to proactively address assets that are missing critical security controls.

Users can validate compliance status using OOTB dashboards and metrics to quickly understand their compliance posture. Additionally, custom compliance metrics (laptop encryption, vulnerability scanning coverage, application enforcement, malware protection, etc.) can be built for reporting on real-time compliance against security controls. Splunk Asset and Risk Intelligence provides comprehensive endpoint compliance reporting across assets to identify and reduce risk exposure. By proactively identifying compliance gaps as they occur and demonstrating improvements over time, teams can better keep up with security and compliance requirements.

With Splunk Asset and Risk Intelligence, teams have an unparalleled advantage in safeguarding their digital environments. Continuous and comprehensive visibility into all assets and identities equips organizations with the necessary tools to preemptively identify their vulnerabilities, conduct faster and more thorough investigations, and respond swiftly to emerging threats.

Get Started

Are you ready to learn how continuous asset and identity intelligence can help modernize your SOC? Speak with a Splunk expert now.

splunk>

24-CMP.eGuide.continuous-asset-and-identity-intelligence-v5