Splunk Asset and Risk Intelligence

Continuous asset discovery and compliance monitoring for proactive risk mitigation

Product Benefits

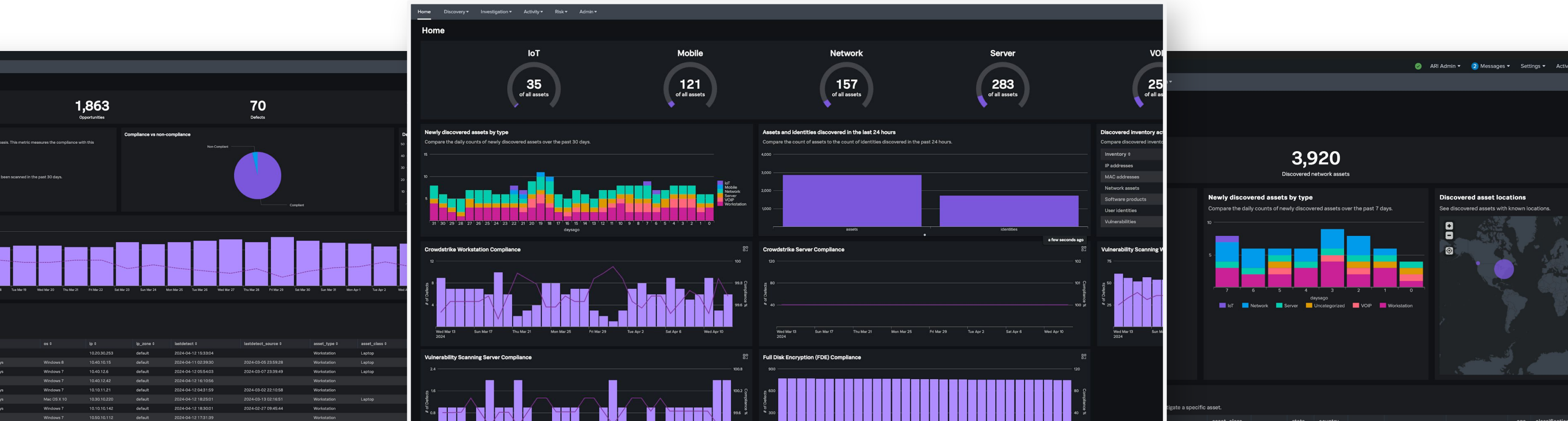
Gain accurate asset and identity context to enhance visibility and shorten investigations

Understand and improve compliance and security by proactively addressing assets lacking essential controls

Continuously update asset and identity inventory to reduce risk and eliminate blind spots

As organizations navigate increasing infrastructure complexity, they face the pressing need to effectively manage their expanding attack surface to uphold compliance standards. Businesses are broadening their digital footprint across cloud, hybrid, on-premises, and operational technology (OT) and internet of things (IoT). Security operations teams are not only struggling with the daunting task of accurately and efficiently mapping out a vast array of assets, including devices, users and applications, but they are also grappling with the repercussions of incomplete and inaccurate asset data. These data discrepancies contribute to lengthy security investigations and create substantial gaps in compliance, putting the business at risk and creating a barrier to regulatory adherence.

Splunk Asset and Risk Intelligence continuously discovers assets and identifies compliance violations and gaps in security controls. It uses both established out-of-the-box and custom frameworks to accelerate security and compliance investigations and reduce risk exposure. Leveraging existing data sources in the Splunk platform, Splunk Asset and Risk Intelligence correlates, analyzes and enriches the data with advanced, customizable pattern-matching rules to provide a comprehensive and accurate asset inventory. Splunk Asset and Risk Intelligence discovers all associated IP addresses, MAC addresses, users, software, and vulnerabilities for more powerful asset investigations. It is pivotal in proactively identifying and remediating endpoint compliance gaps, tracking asset activities, identifying asset relationships, and setting a new standard in asset discovery and risk mitigation.


Home
Discovery
Investigation
Activity
Risk
Admin
IoT
35
Mobile
121
Network
157
Server
283
1,863
Opportunities
70
Defects
Compliance vs non-compliance
Newly discovered assets by type
Compare the daily counts of newly discovered assets over the past 30 days.
Assets and identities discovered in the last 24 hours
Discovered inventory
Crowdstrike Workstation Compliance
Crowdstrike Server Compliance
Vulnerability Scanning Server Compliance
Full Disk Encryption (FDE) Compliance
3,920
Discovered network assets
Newly discovered assets by type
Compare the daily counts of newly discovered assets over the past 7 days.
Discovered asset locations
See discovered assets with known locations.

Gain comprehensive and continuous asset intelligence to reduce risk exposure

Without an accurate view of all the assets within their organization, security teams struggle to maintain visibility of their attack surface, answer asset-related questions, and take action when necessary – ultimately putting the business at risk. Splunk Asset and Risk Intelligence delivers a continuously updated view of assets and identities by correlating data from network, endpoint, cloud and scanning tools. It removes duplicate and outdated data to ensure precision and completeness of your asset inventory. Advanced, customizable pattern-matching rules enrich assets for increased accuracy and completeness, and complete and accurate activity history adds context to your security events. All of this offers essential insights that are fundamental to minimizing risk exposure and eliminating attack surface blind spots.

Accelerate security investigations with accurate asset and identity context

Security teams are challenged with correlating alert data with specific assets and identities during investigations. Splunk Asset and Risk Intelligence enhances this process by providing accurate asset and identity context, which sharpens the focus and shortens investigations. By mapping relationships between assets and identities, security teams can swiftly identify who is associated with what assets and when.

The solution incorporates data from vulnerability and software scanning tools to inform teams about the software and vulnerabilities that exist on their systems. Contextual asset insights combined with user identity and application relationship mapping allow teams to better understand the potential impact of an incident.

Accurate attribution of IP addresses to assets and identities removes the manual effort required to trace the association of IP addresses with specific assets or identities over time. Equipped with extensive asset and identity context, including network activity, asset associations and asset health, security teams can conduct faster, more thorough investigations.

Uncover compliance gaps in security controls

Accurate asset management is crucial for compliance and audits, and organizations who struggle to gain visibility of all necessary assets put themselves at risk of compliance violations and potential cyberattacks. Splunk Asset and Risk Intelligence empowers organizations to understand and improve their compliance and security posture with dashboards and metrics. The out-of-the-box compliance metrics framework allows businesses to report real-time compliance against several security controls. Teams can also build custom compliance metrics for things like laptop encryption, vulnerability scanning coverage, application enforcement, malware protection and more. By leveraging compliance frameworks, the solution provides a clear lens to proactively address assets that are missing critical security controls to improve both security and compliance posture.

Seamlessly integrate with Splunk Enterprise Security to enrich notable events

Splunk Asset and Risk Intelligence can be deployed within an on-premises Splunk Enterprise or Splunk Cloud environment, and by enriching Splunk Enterprise Security with detailed asset information, security teams can reduce investigation times. The solution continuously updates and populates the Splunk Enterprise Security Assets & Identities framework with the latest asset information, and provides comprehensive asset context for Enterprise Security notable event enrichment to establish accurate attribution of assets during investigations.

splunk>

Contact us: splunk.com/asksales

splunk.com