

Analyst1 Releases Version 2.16.0

Release Includes Centralized Credential Management, HashiCorp Vault Support, and a New SentinelOne Integration

RESTON, VA, UNITED STATES, September 25, 2026 /EINPresswire.com/ -- [Analyst1](#), a leading cyber

“

With 2.16.0, every credential across every source and integration is managed in one place, visible to administrators and governed on their terms, including in the vaults they already trust.”

Michael Wenger

threat intelligence platform, today announced the general availability of version 2.16.0. The release gives administrators one place to manage the credentials behind every source and integration, lets teams authenticate through HashiCorp Vault, and extends endpoint coverage with a new SentinelOne integration.

One Home for Every Credential

Connecting threat intelligence to a security stack means giving the platform credentials for each tool it touches. In 2.16.0, administrators manage credentials for all sources

and integrations in a single location, increasing visibility into what is configured across the platform and making rotation easier. Existing source and integration credentials migrate automatically to Analyst1’s credential storage during the upgrade.

HashiCorp Vault Support Keeps Secrets Where They Already Live

Teams that manage secrets in HashiCorp Vault can now authenticate sources and integrations through Vault instead of storing integration credentials in Analyst1. When an integration connects, Analyst1 retrieves the current credentials from Vault and does not store them. Analyst1 keeps only the credentials it needs to reach Vault itself, so it can retrieve integration credentials again after a services restart. Key capabilities include:

- Configure one or more credential management providers, including multiple providers of the same type, such as two separate HashiCorp Vault providers
- Map Vault storage objects to Analyst1 credential fields using path notation
- Retrieve current credentials from Vault each time an integration authenticates

SentinelOne Joins the Endpoint Lineup

Version 2.16.0 adds SentinelOne Endpoint Security as an endpoint detection and response (EDR)

integration, joining the CrowdStrike Endpoint Security integration introduced in 2.15.0 and Microsoft Defender for Endpoint from 2.13.0. Analyst1 sends indicators out to SentinelOne and brings sightings back, so analysts can see which intelligence is showing up in their environment. Key capabilities include:

- Export domain, IPv4, IPv6, file hash (MD5, SHA1, and SHA256), and URL indicators to SentinelOne IOC Management at the Site level, with configurable risk score, severity, and description
- Export SHA1 and SHA256 file hashes to a Site-level SentinelOne Blocklist, scoped to macOS, Windows, or Linux
- Keep indicators active in SentinelOne for as long as they meet the criteria defined in Analyst1, and remove them automatically when they stop
- Poll SentinelOne Threats and Alerts on a configurable schedule and look-back window, recording hit statistics for indicators Analyst1 already tracks

Bring Your Own AI with Microsoft Foundry

Analyst1 now supports Microsoft Foundry as a Bring Your Own AI ([BYO AI](#)) provider. Teams configure their Foundry connection and credentials in Analyst1, then use the models available in their own Foundry environment for Analyst1 AI capabilities.

"Every integration you connect means handing a platform the keys to another tool; security teams deserve to see exactly where those keys live and how they're used," said Michael Wenger, Director of Product at Analyst1. "With 2.16.0, every credential across every source and integration is managed in one place, visible to administrators and governed on their terms, including in the vaults they already trust. That foundation lets us connect intelligence to the tools that act on it with confidence. With SentinelOne, analysts can now push intelligence to the endpoint and see exactly what it catches."

Additional Platform Improvements

Version 2.16.0 also includes enhancements across the platform:

- Censys Reputation Labels (MALICIOUS, SUSPICIOUS, BENIGN, INACTIVE, and HONEYPOT) are now available as Vendor Attributes, so analysts can filter indicators created from Censys collections by label
- Updates for MITRE ATT&CK v19.2 and ATLAS v2026.08 are available
- Security updates include Chromium and several third-party libraries, addressing multiple CVEs, along with stability fixes for Recorded Future API requests, custom evidence source retrieval, and indicator extraction from uploaded email messages

Availability

Analyst1 version 2.16.0 is available now. Existing customers can access full release notes and documentation at docs.analyst1.com, including upgrade details for credential migration and MITRE ATT&CK mappings. For questions, contact your account manager or reach out to support@analyst1.com.

About Analyst1

Threat intelligence often gets stuck between insight and action. Analyst1 is the Operationalized Threat Intelligence Platform built to close that gap. It automatically structures data, links it to assets and vulnerabilities, and tailors views for each role. Integrated with SIEM, ticketing, and vulnerability systems, Analyst1 orchestrates workflows and automates trusted actions, helping organizations reduce response time from days to minutes. For more information, visit analyst1.com.

Media Contact

Marketing@analyst1.com

Scott Messick

Analyst1

[email us here](#)

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/945068057>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.