monad

Monad Makes Security Data Available at Scale

The typical enterprise has all the data they need to secure their organization better, yet that data is typically hidden, and its value locked within discrete data silos. Monad unleashes this security data so that security, DevOps and cloud engineering teams finally have the insights they need to improve security and to build applications using this data on the fly.

The pressure on security operations teams just won't let up. It's not just that the number of attacks that target enterprise data and systems are on the rise, it's also the velocity and the complexity of digital transformation efforts underway. As businesses digitize their customer interactions, evolve their business models, and accelerate their ability to deliver new software features and applications, security teams find themselves struggling just to keep up with the pace of change.

As part of this evolution, security teams find themselves working ever more closely with DevOps teams. This means that they need to move as quickly as the applications and infrastructure within their organizations advance. The challenge with this relatively new DevOps focus means that these teams need to get their security data immediately so they can build new applications and workflows that support business objectives. Yet, this data has been historically siloed and difficult to reach and extract in order to obtain its insights.

> "Staying on top of security data is about constantly grooming your entire fleet of systems for the few rotten apples buried in it and the work needs to restart every week. Monad is set to solve this problem with their scalable security data platform that we can easily bring into our SecDevOps toolset."
>
> Alex Eiser - Security lead at a mid-sized biotech company

Today's Big Security Challenge: Unleashing Value Hidden Within Existing Security Data Silos

Simply throwing more resources at the security challenge, such as adding additional security tools or staff, doesn't solve the problem. If it did, cybersecurity would have become much more manageable a long time ago. Enterprises have invested tens of billions during the past twenty years in network firewalls, application security, anti-malware, vulnerability management, identity management, intrusion prevention, and more.

Why hasn't cybersecurity become more manageable? Because the complexity of today's business-technology environments make cybersecurity fundamentally a data management challenge.

Enterprise cybersecurity is a data management challenge because every security product deployed in the environment generates its own security information. This data remains siloed within the database or logs created by each discrete toolset. These data islands obscure the view that security operations teams must see if they are to understand the actual security posture within their organization.

This situation exists not because of, but despite, the best efforts of security teams.

Despite their best efforts, security teams can't obtain the actionable insights they need

This data security challenge only keeps growing. Today, each enterprise relies upon, on average, 130 separate security tools. This means that security teams must manually rush to gather much of the data they need whenever there is an incident. This slows down response and increases the risk that attackers will slide through defenses, or that systems will fall out of compliance to internal or external regulatory mandates, because of the inadequate information at hand. If teams had access to insights about these systems, these vulnerabilities would have been addressed and the systems made secure and compliant, before an attack occurs.

There's been no easy fix for security teams. For instance, if a new business initiative requires input on risk from the security team, it becomes a significant task for that team to simply collect the data they need and then extract value from that data necessary to assess the actual business risks comprehensively.

What does this look like in practice? Because there's rarely any clarity regarding what team member owns the management of what tool, work tickets are created in service management systems such as Jira or ServiceNow to track the ad hoc initiative. Additionally, since the security data is siloed in each tool, the teams will often manually collect the data they need. They will then assemble it in spreadsheets and distribute it to various groups within email or file shares.

The data is then manually parsed, correlated, and prioritized. And, following all of these efforts, there's no straightforward way to present the necessary information to executives, such as with visualization tools or dashboards they help communicate to business leaders with clarity.

Some organizations attempt to be proactive and get ahead of the challenge by building customized connectors to dedicated security data lakes. When the people who worked on building the APIs leave the company or switch job roles, the entire endeavor becomes unmanageable and falls apart. Others turn to security information and event managers, but these lack the specific information modern security and DevOps teams seek.

All of these build-it-yourself approaches prove hard to maintain and more costly than anticipated. Additionally, they don't provide the insights into risk necessary to solve the business problems these teams face.

Building homegrown tools is also a costly and an unproductive utilization of highly-skilled security staff. Should a similar request for security data come in the next quarter, most of the work completed must be conducted repeatedly. These efforts are also a distraction that places organizations at greater risk than they need be.

What enterprises need is a persistent, manageable, and scalable way to interconnect the data pipelines between their security tools so that this data can be streamed consistently, cleansed, enriched and stored within any data warehouse. That's how to make this necessary data accessible, searchable, and ready for analysis by business intelligence tools.

> At Monad, we see security as fundamentally a big data problem. DevOps and cloud engineering teams today are unable to access their security data in the streamlined way that they need in order to swiftly address their most pressing security and compliance challenges."

Christian Almenar
Co-Founder and CEO

Jacolon Walker
Co-Founder and CTO

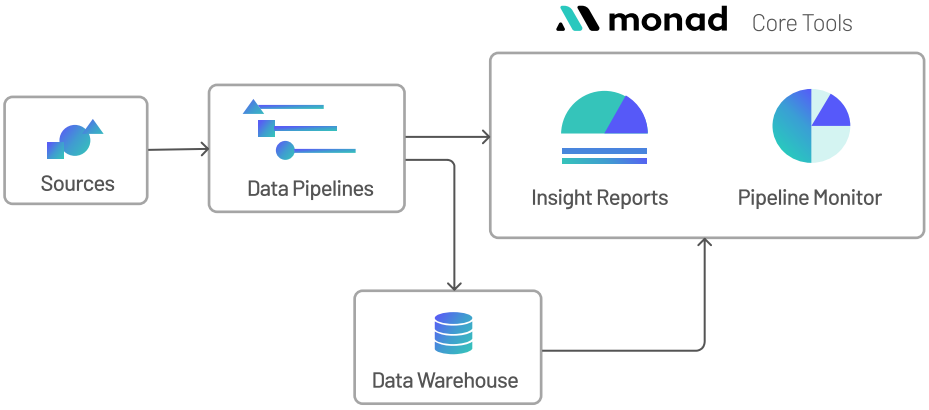
> We started Monad to build the first cloud native data platform for security. What we really want to do is to unlock the security and development teams with their security centric data so they can search it easily and find powerful and valuable insights from it."

Security teams need a way to unlock the value hidden within their existing security data

Solving this security data challenge is why we founded Monad. The Monad Platform enables teams to extract and connect the data from their essential security tools, centralize that data within a data warehouse of choice, normalize and enrich that data so that teams are provided with the precise insights they need to secure their systems and data effectively. All of this data is also now SQL searchable, so security and DevOps teams can finally access this data directly via their analytics tools.

Monad makes these security insights readily available, accurate, comprehensive, and reproducible.

Finally, security operations teams can more completely utilize the full capabilities of their security toolsets based upon the actual status of their environment.



Because Monad provides security and DevOps teams a "single source of truth" for all of their asset and vulnerability data for IT, application security and cloud services, these teams can swiftly solve challenges that previously took considerable manual effort to aggregate the data.

By unleashing the security data trapped within each discrete security tool, Monad provides enterprise security operations teams, DevOps teams, and cloud engineers these insights. It saves them an incredible amount of time and cost.

In-depth: The Monad Data Security Platform

The Monad data security cloud platform will initially focus on helping enterprises to extract value from data sources within vulnerability and asset management. Monad's out-of-the-box connectors enable enterprises to consistently stream, cleanse, and store their vulnerability management data within any data warehouse. With this single source of truth across desperate security tools, security data is now fully accessible, searchable, and ready for analysis.

Monad's vulnerability and asset management connectors are available for the entire relevant technology stack, including asset discovery and management, vulnerability management, configuration management databases, and more.

Soon, Monad will add additional security use cases, such as EDR, XDR, identity management, threat intelligence, among others.

Monad's data-centric connectors and APIs work across security tools and provide the flexibility to unleash value from your existing security tools seamlessly.

Following the extraction of security data and establishing a continuous data pipeline, the Monad security data platform transforms that data by creating a unique star schema, the Monad Object Model or MoM. MoM works with any data warehouse. This way, security teams, DevOps teams, and cloud engineering teams can interact directly with the data through SQL, third-party business intelligence tools, as well as Monad's visualization capabilities, Insights which is delivered as part of the platform to address various security and compliance best practices and workflows. With this new knowledge in hand, security teams can now build effective security and compliance applications on the fly.

MoM offers a standardized schema for security data that:

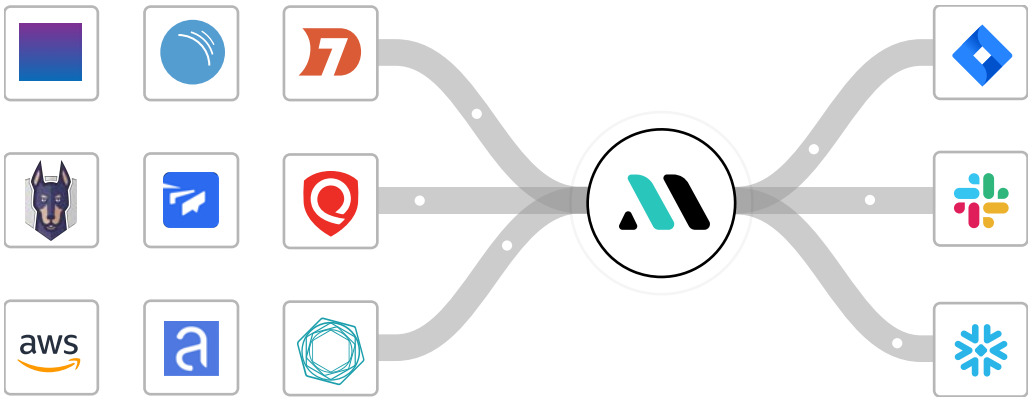
With security data enriched and normalized by Monad, security, DevOps, and cloud engineering teams can set their spreadsheets and manual data aggregation methods away, and swiftly build accurate and persistent data pipelines so that they can:

- Quickly build the security and compliance best practices they need to create and meet service level agreements, pass security and regulatory audits, conduct comprehensive and information incident postmortems, and more.
- Create a continuous single source of truth and data coverage for all IT, product, cloud, and application assets.
- Obtain accurate, comprehensive dashboards and reports for insights into team performance views, return on investments and return on risk reduction, aggregate vulnerability details, and much more.

- Provides a consistent and normalized schema across a variety of sources
- It is built using dimensional modeling (Star Schema)
- Creates fact tables with dimensional tables for attributes
- Creates a unique workflow and data pipeline manager
- Injects, collects, eliminates data noise, and transform enterprise security data into a unified schema

How does Monad help enterprises unleash their security data? Monad guides the user through the credential setup and connects directly to the APIs of the security tool. Once that authentication is complete, Monad prepares the data for

availability within the data warehouse of choice. Teams can also choose to export their security data from Monad into a variety of SQL-like data platforms.



Through its integration with common service management platforms, such as Jira and ServiceNow, Monad helps enterprise security teams move from data insights to prioritize and act quickly. Finally, through its open API, the Monad security data platform enables these teams to develop integrations for, and therefore garner more value from, their custom in-house security toolsets.

Conclusion

Security teams don't necessarily need more security tools, but they certainly need to unlock the data within the tools they already have. The Monad Platform enables security teams to do exactly that. Monad was founded to help enterprise security teams, DevOps teams, and cloud engineering teams to connect and extract the data they need from their essential security tools. Monad enables the centralized storage of that data within a data warehouse of choice and normalizes and enriches that data. This way, teams are provided with the precise insights they need to secure their systems and data effectively. Monad makes these security insights readily available, accurate, comprehensive, and reproducible. For more information, visit www.trymonad.co.