CONTEXTAL

Technology Overview

 | contextal.com

About Contextal

Founded in 2022 by cybersecurity veterans with a history of creating industry-leading technologies safeguarding the International Space Station and billions of users worldwide.

Contextal develops technology, which analyzes thousands of relationships, anomalies, past events and other indicators to connect the dots and **understand the complexity** of threat surfaces.

The solutions provided by the company offer unique threat detection and intelligence capabilities through a seamless **contextual approach**, significantly improving cybersecurity efforts.

Led by Proven Experts

Contextal is founded by the creators of ClamAV, one of the **world's most widely used** anti-malware solutions.

Tomasz and Alberto have cooperated with leading **global organizations**.

AV integration in macOS 10.4.

Built the first solution utilizing EPSec, presented at VMworld.

AV integration with Cisco Security Agent & FireAMP.

Developed advanced detection, sandboxing and Browser Isolation technologies.

Why Existing Security Solutions Fall Short

Lack of Broader Context

They usually analyze threats in isolation, **missing complex relationships** and signals that indicate sophisticated attacks.

Detection Mechanisms Are Rigid And Limited

Most systems **can’t adapt** to new or evolving threats without manual updates or reconfiguration.

Pattern-based systems **can be easily evaded** and have a poor, **short-lived efficacy.**

Security & Scalability Issues

Legacy security solutions **weren't built for the cloud**, often leading to gaps in protection, performance, and reliability.

Most popular industry solutions were **created decades ago**, using unsecure frameworks and their core technology has only been maintained over time.

Our Approach

Context is Everything

Contextual Threat Detection

Focused from the ground-up on a broader perspective by analyzing and **correlating relationships, metadata, time, past events, and anomalies** across the entire attack surface.

ContexQL

Customizable Scenarios with ContexQL

Enables precise, flexible detection through a **powerful domain-specific language** designed for contextual operations.

Dramatically improves the efficacy posture with future-proof generic detections.

Built for Security and Scalability

Developed in Rust with isolated, containerized components and **modular architecture** for secure, high-performance, and horizontally scalable deployments.

Introducing

Contextal Platform

The most comprehensive and advanced contextual detection system available today!

Designed from the ground up as a **cloud-native solution**, ensuring scalability, performance, and security in modern cloud environments.

27+

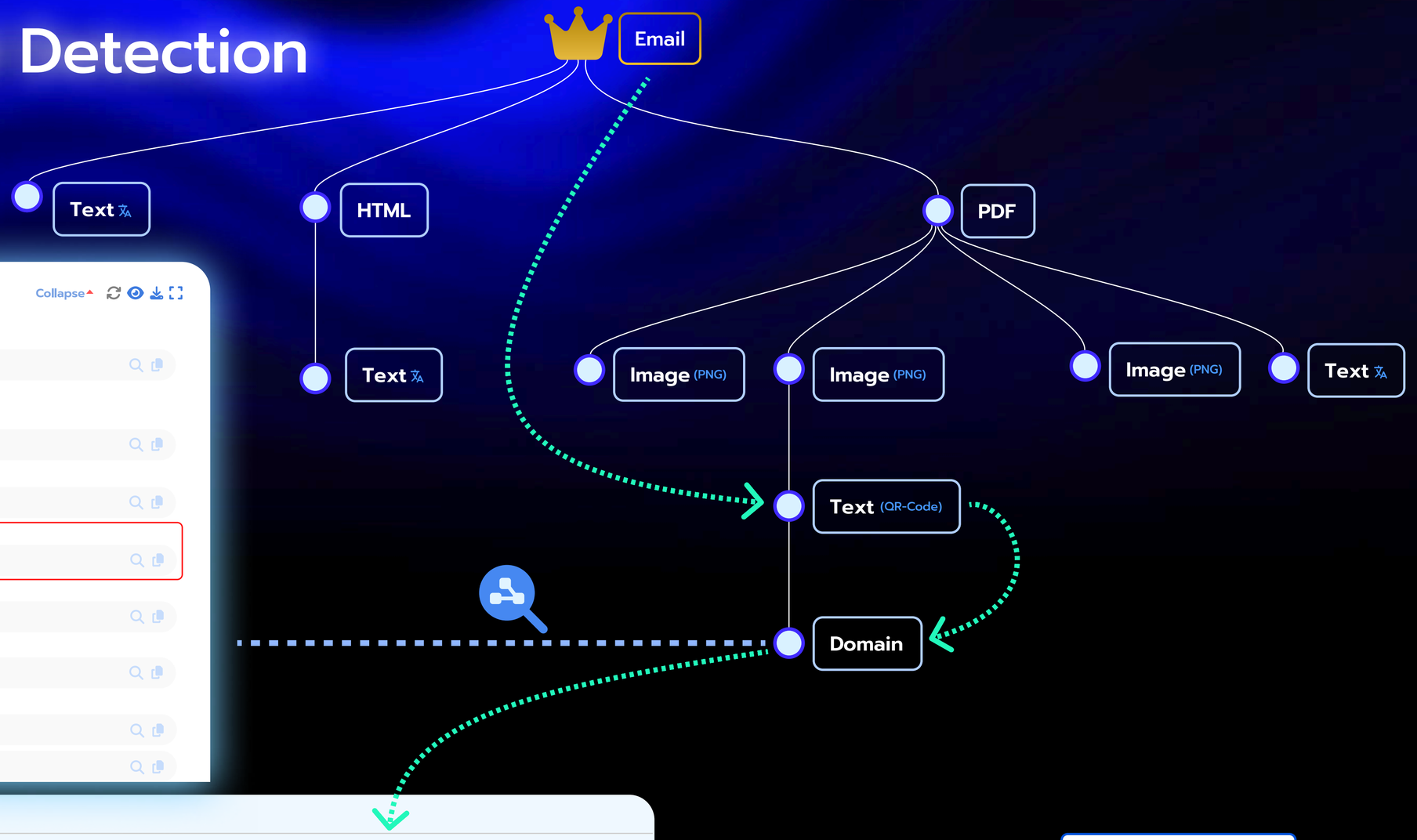
Broad data coverage with 27+ dedicated processors capable of handling **all popular data formats.**

AI

AI Powered & Optimized: AI-driven image classification and text processing run locally, ensuring complete **data privacy.**

See it in Action

Contextual Detection



ContexQL

```
object_type = "Email" and @has_descendant(
  @has_symbol("QRCODE") and @has_child(
    object_type = "Domain" and @match_object_meta($age_days < 30)
  )
)
```

Actions

BLOCK

ContexQL & Scenarios

Our powerful ContexQL language can be used to perform data searches and create actionable detection scenarios operating in real-time.

ContexQL

Scenario Name*

Suspicious LNK in Email/HTML/URL

Scenario Description*

Block potentially suspicious LNK files found in Email/HTML/URL.

Local Query*

```
(object_type = "Email" or object_type = "HTML" or object_type = "URL")
and
@has_descendant (
  object_type = "LNK"
  and (
    @match_object_meta($string_data.relative_path iregex("powershell"))
    or
    @match_object_meta($string_data.command_line_arguments iregex("powershell"))
    or
    @match_object_meta($string_data.command_line_arguments.len() > 260)
  )
)
```

Action*

BLOCK

- Provide scenario name & description.
- Write a query with ContexQL.
- Dictate actions such as BLOCK, ALERT, ALLOW, QUARANTINE.
- Optionally extend your scenario with more advanced settings.
- Deploy & trigger actions!

Local Context vs Global Context

Contextal Platform uniquely correlates insights across **multiple contextual layers,** enabling precise, situational threat detection.

Local Context

- Focused on current input objects.
- Captures all information and relationships within these objects.
- Represented as a graph of inner-object connections.

VS

Global Context

- “Common Knowledge”
- Aggregates graphs over a specifed time window into a graph database.
- Enables cross-object correlation and threat pattern recognition with the current local context.

See it in Action

Detecting Campaigns with Global Context

Scenario Name*

ENCRYPTED CAMPAIGN

Scenario Description*

Detect e-mail campaigns with encrypted attachments that can't be inspected.

Local Query*

```
1  object_type = "Email" and @has_descendant(
2    @has_symbol("ENCRYPTED") and !@has_symbol("DECRYPTED")
3  )
```

Show Results →

☑ **Global Context** (optional)

Global Query

```
1  MATCHES: >8;
2  TIME_WINDOW: 15 minutes;
3
4  // text sentiment from the local context
5  ${sentiment}=LOCAL.filter(object_type = "Text")
6    .get_object_meta($natural_language_sentiment.compound);
7
8  object_type = "Email" and @has_child(
9    object_type = "Text" and @match_object_meta($natural_language_sentiment.compound in ${sentiment})
10 ) and @has_descendant(
11   @has_symbol("ENCRYPTED") and !@has_symbol("DECRYPTED")
12 )
```

Action*

ALERT

Challenges with Encrypted Threats

The Problem

- Some threat campaigns rely on encrypted content to evade detection.
- Passwords may be shared in the same message or via external channels.
- Traditional security solutions are often unable to analyze encrypted content.

The Contextual Way

Contextual Auto-Decryption

- While processing data objects, Contextal Platform extracts a list of potential passwords from textual elements.
- At the final stage of processing, the platform checks for encrypted content (e.g., PDFs, Office documents, archives).
- If present, the encrypted content is reprocessed using the collected passwords, which are best suited for a given object. Upon successful decryption, the data is inspected and the **DECRYPTED** symbol is added.
- As shown in the previous example, the **absence** of the DECRYPTED symbol can also indicate an anomaly or evasive behavior!

Contextal Benefits

Threat Detection

	Problem Solved	Benefit
Contextual Threat Detection	Traditional systems analyze files or events in isolation, missing broader patterns and correlations.	Detects sophisticated threats through local and global context analysis across time, content, and relationships.
Metadata-Driven Global Intelligence	Siloed systems can't utilize shared knowledge for detection or correlation.	Enables cross-event analysis and "common knowledge" detection through a unified metadata graph database.
Threat Intelligence Console	Analysts often lack visibility into processing details, results, and decision rationale.	Provides an intuitive interface for investigation, trend analysis, deep threat insight, and detection automation.

Contextal Benefits

Future Proof

	Problem Solved	Benefit
Secure by Design	Legacy tools require constant maintenance and security updates, often disrupting production environments.	Built in Rust with containerized modules for maximum memory safety, isolation, and minimal attack surface.
Flexible & Powerful Detection Mechanisms	Traditional solutions require engine updates or redesigns to handle new threat types.	Uses ContexQL to build reusable, generic detection logic covering entire threat classes.
AI Optimized	Most solutions don’t provide any valuable output for AI training, wasting precious data.	Provides vast amount of metadata in a standardized JSON form, ready to feed into AI models.

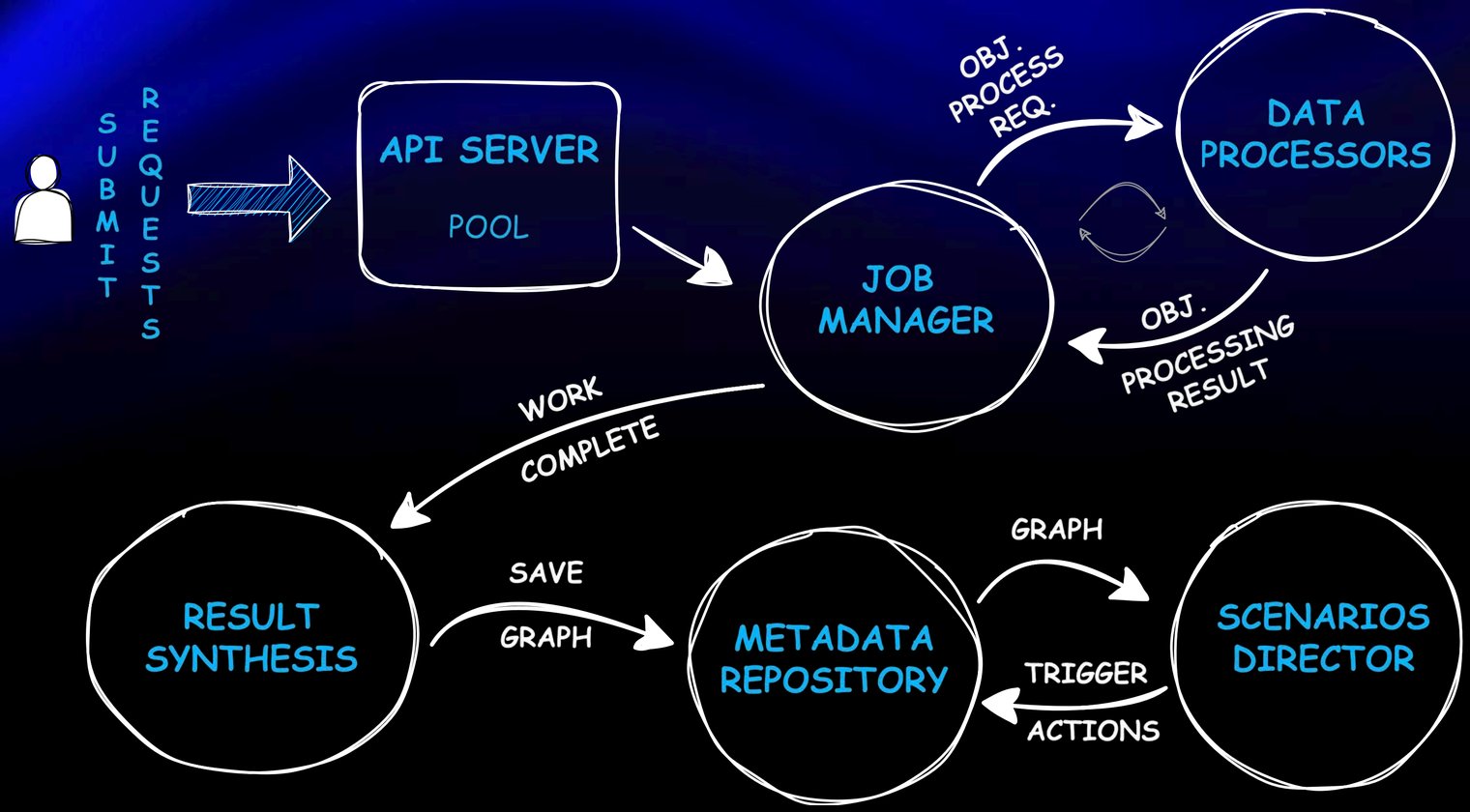
Contextal Benefits

Architecture

	Problem Solved	Benefit
Customizable Data Processing Pipelines	Most security solutions function as black boxes that can't be tuned or extended.	Modular processing architecture lets you adapt pipelines for different content types or workflows.
Ready for Integration	Black-box security solutions often use custom protocols and have specific environment requirements.	Uses modern industry standards, can be easily plugged into existing environments or be the core processing platform for organisations.
Modular, Scalable & Cloud-Native Architecture	Traditional tools struggle with cloud-native deployments and horizontal scalability.	Deploys flexibly on-prem or in cloud environments, scaling automatically with demand.

See it in Action

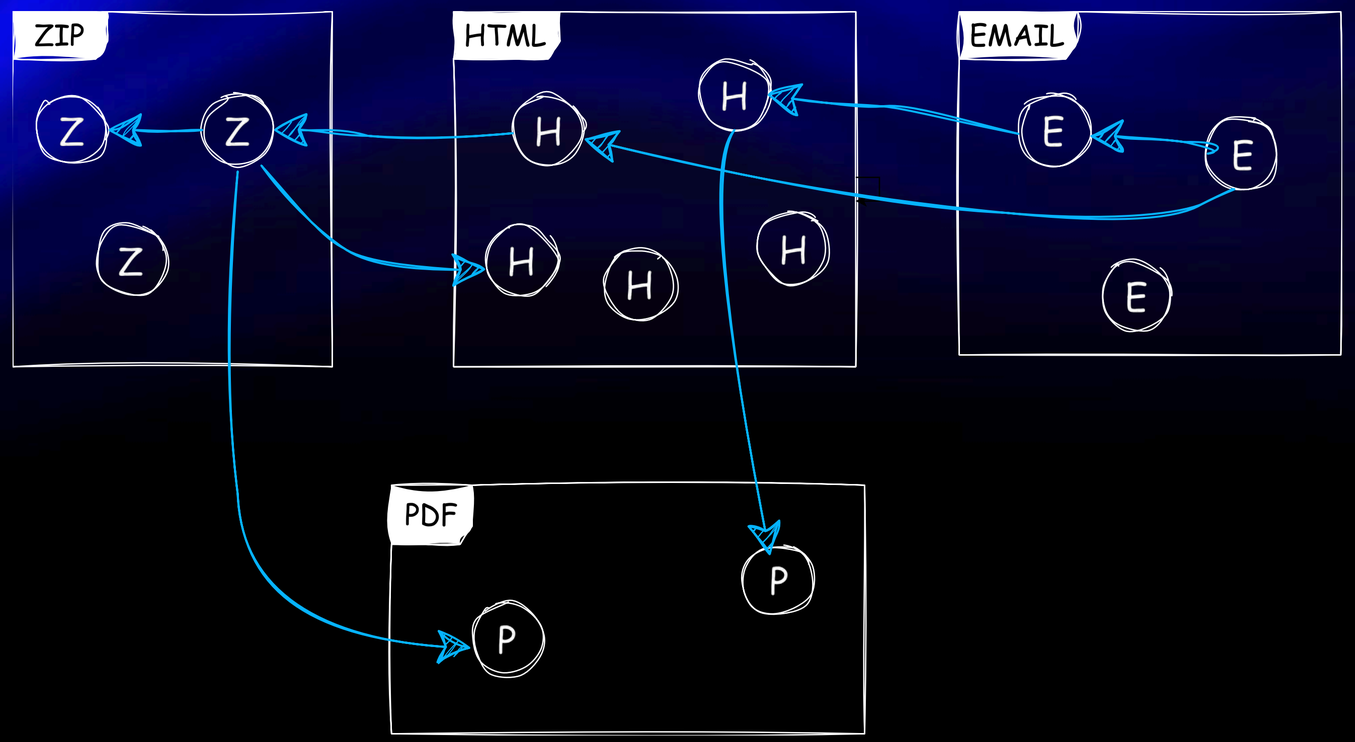
Anatomy of the Platform



- The client submits a raw data object for contextual analysis.
- Additional metadata can be provided to **enrich the context**, including:
  - Origin
  - Name or identifier
  - Associated user
  - Organization name
  - Time of arrival
- Processing is fully automated and aimed at **real-time submissions.**
- After processing, the client receives a verdict, consisting of one or more actions triggered by matching detection scenarios.

See it in Action

Data Processing in Detail



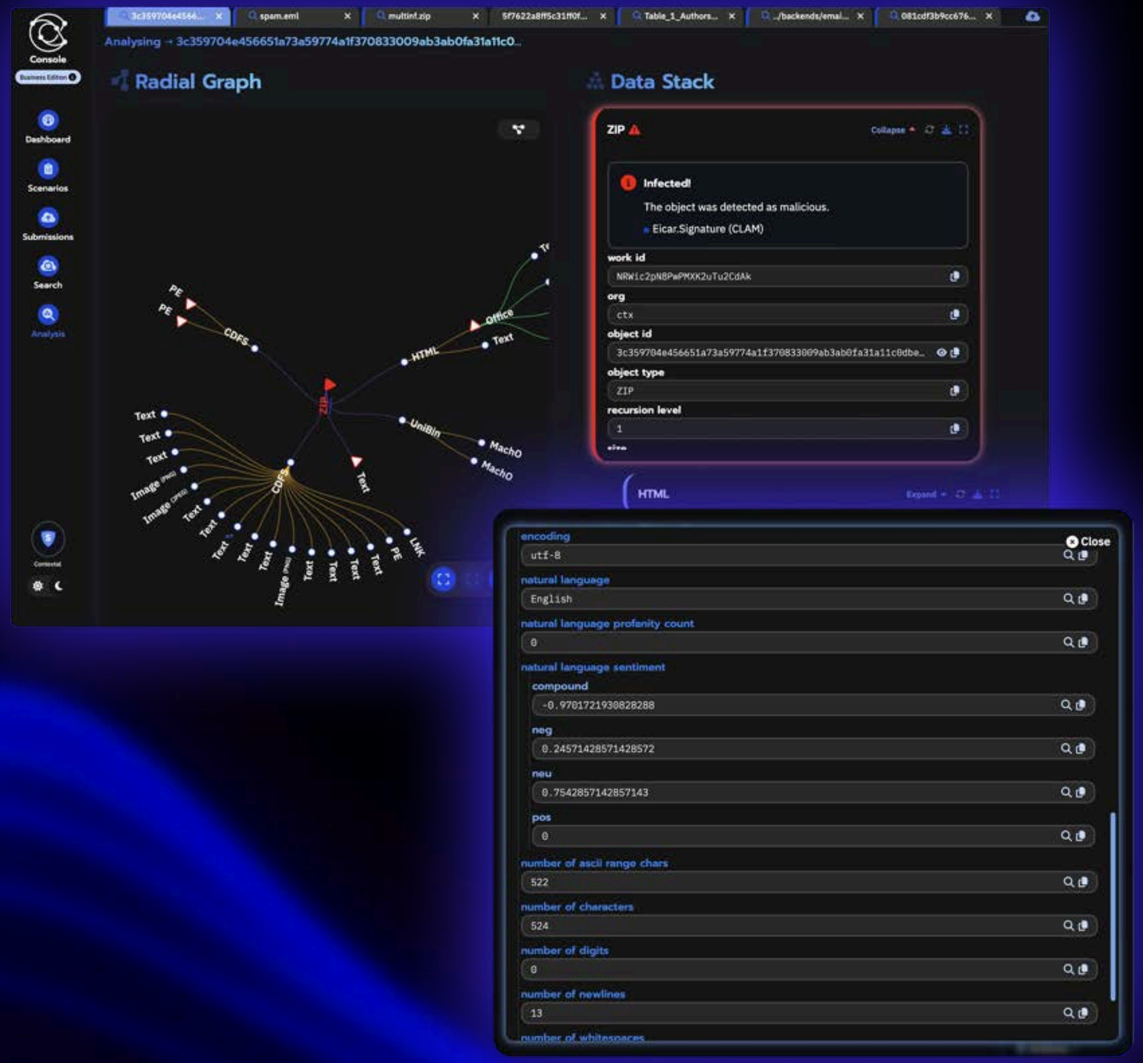
- Pools of containerized workers are **automatically scaled** based on current cluster load.
- Each pool handles a specific type of input (e.g., Email, PDF, HTML) and scales independently for **optimal efficiency.**
- Processing an item generates **detailed metadata** and may extract **child objects,** which are recursively analyzed.
- All processing is **fully parallelized** across available compute resources for maximum performance.

Result Synthesis

- The output of data processing - including that of child objects - consists of **metadata, relations, and symbols** that highlight significant characteristics or anomalies.
- **Raw input data** is no longer analyzed after this stage and may be discarded or retained, depending on needs (e.g., for debugging or reprocessing).
- Final results are consolidated into a **graph-like JSON structure** and stored according to the configured retention policy.

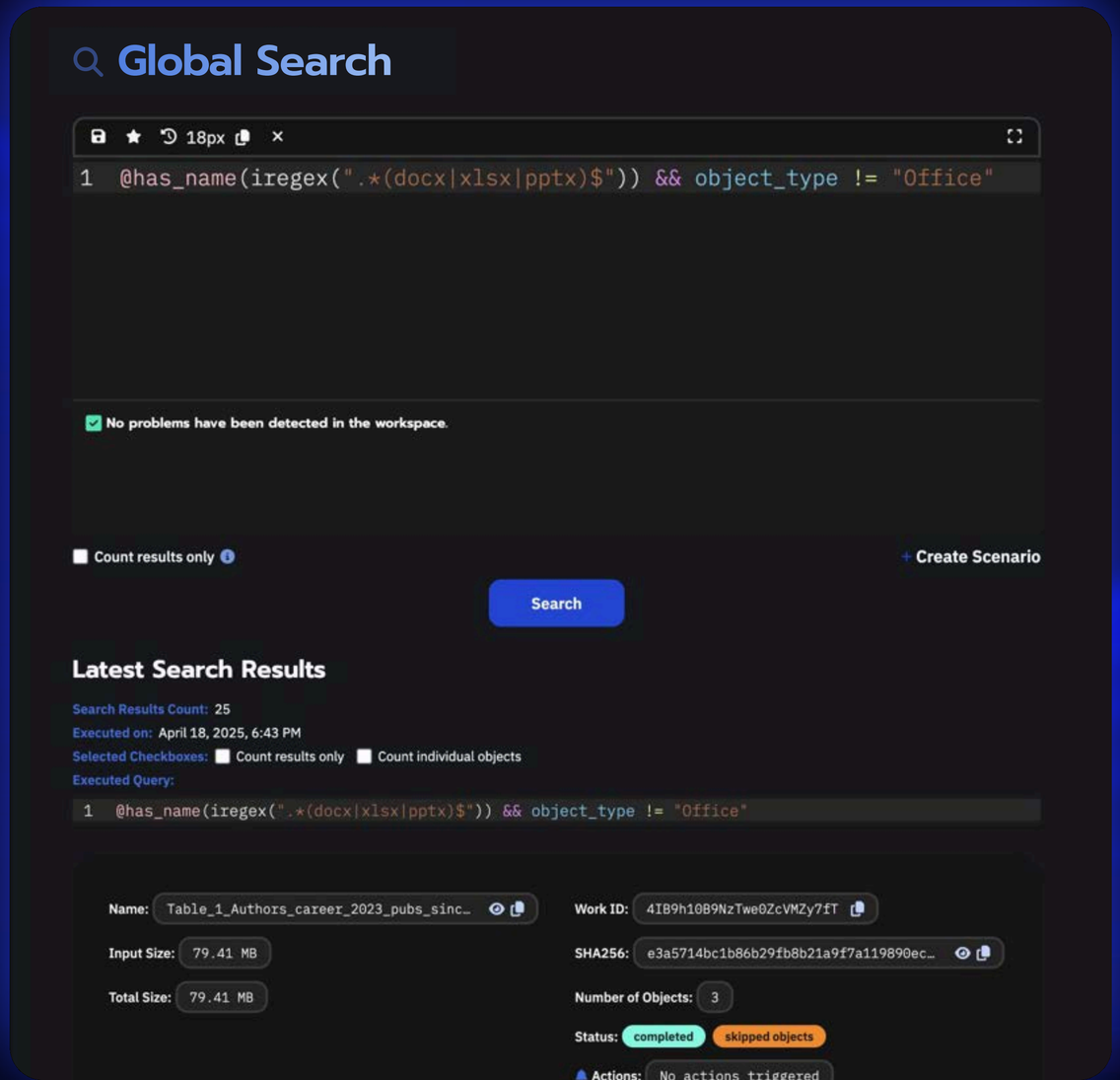
Metadata Repository

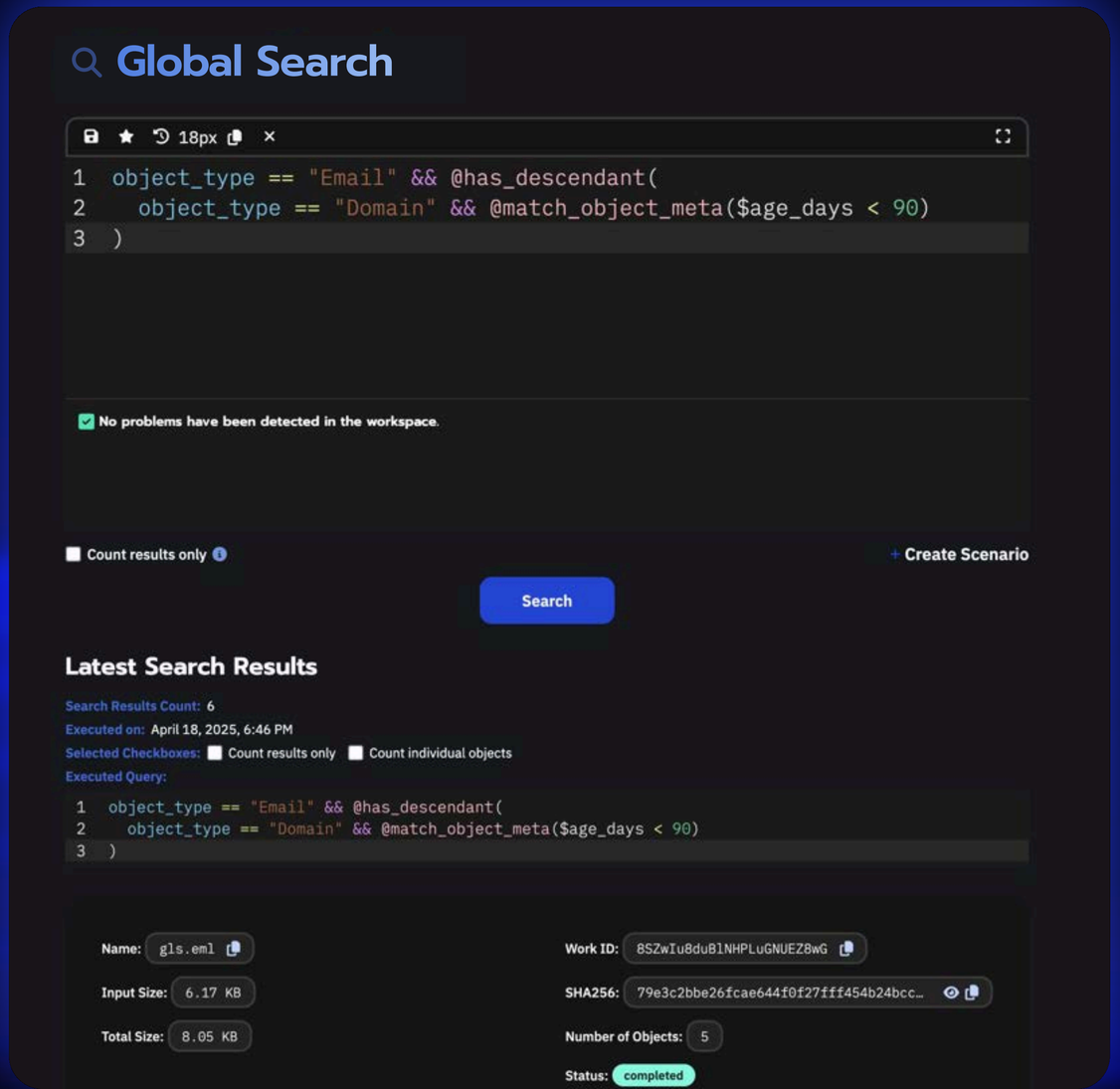
- Collected metadata can be searched, visualized, and analyzed using **Contextal Console** or accessed via API.
- Enables **global context** operations, serving as a foundation for “common knowledge” across all processed inputs.
- Supports training and fine-tuning of **AI/ML models** by providing rich, labeled, real-world data.
- Facilitates historical correlation and long-term **threat trend analysis.**
- Provides a foundation for custom **threat intelligence** feeds customized to specific organizational environments.



See it in Action

Example Data Search





Scenarios & Actions

- **Scenarios** are compact programs written in ContexQL that perform logical and statistical operations on graph data.
- Each scenario is evaluated against the local result graph, and optionally against global context graphs for broader correlation.
- **Actions** are free-form strings reported by matching scenarios and interpreted by platform clients.
- The presence, absence, or combination of actions delivers a straightforward yet **powerful mechanism** for generating actionable results.

Scenario Name*

NSFW Graphics

Scenario Description*

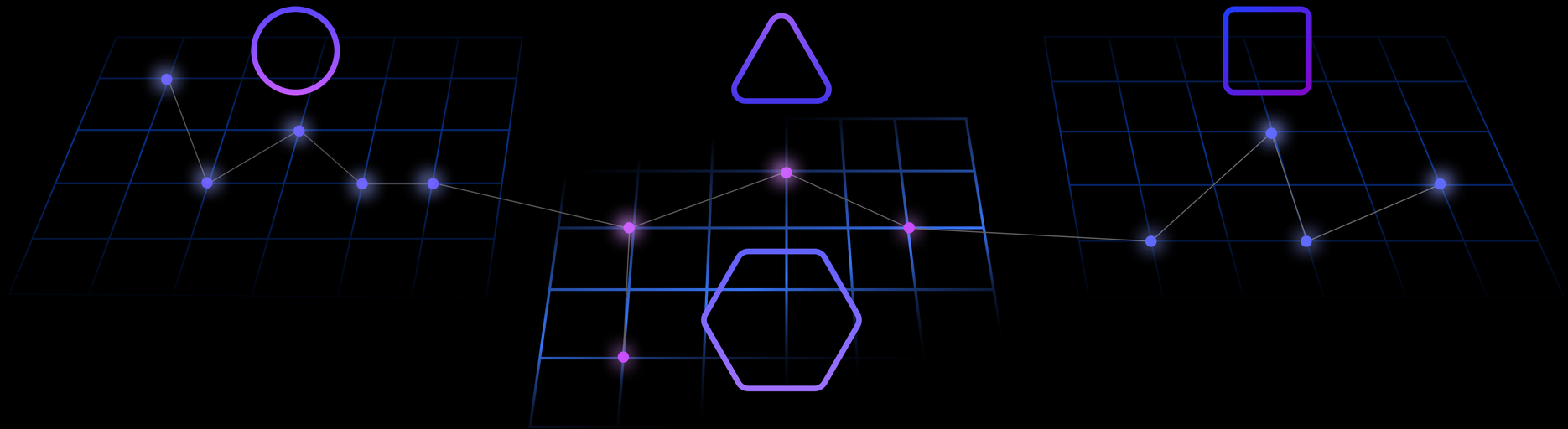
Alert on NSFW images.

Local Query*

```
1  object_type = "Image" and
2    (@match_object_meta($nsfw_verdict = "Hentai")
3    or @match_object_meta($nsfw_verdict = "Sexy")
4    or @match_object_meta($nsfw_verdict = "Porn"))
```

Action*

ALERT



Integration

Designed for Cloud

Cloud-native architecture, deployable both on-premises (via Kubernetes) and in public cloud environments

API-Driven

Modern, REST API-based integration model.

Speak JSON

Portable and standardized data exchange format using JSON.

Monitor Everything

Observability and Monitoring via standard metrics.

SSO Ready

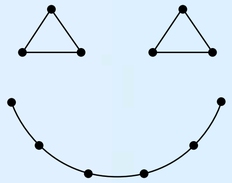
Contextal Console supports Single Sign-On (SSO) with granular user roles and permissions.

Plug & Play

Optional client libraries available for integration with popular platforms and languages.

Reach out for more information.

info@contextal.com | contextal.com | platform.contextal.com



Thank You!