

Trust & Safety

Sensitive Online Research — On & Off the Platform

When following up on suspicious activity, Trust and Safety investigators typically start by reviewing users' or groups' behavior and actions on the company's online platform. A hospitality business' T&S team, for instance, will first look at how certain users interact with the online reservations system or property hosts, while a social media platform's analysts will first look at the user's posts and discussions. If the findings warrant further research, T&S investigators will continue by digging into the users' other online activities and affiliations. Both types of web research – within their own digital platform or service and outside of it, require analysts to exercise caution, protecting their identity, mission, and organization from compromise.

Within a Trust & Safety organization, enforcement operations teams are tasked with recommending and/or taking actions to keep users safe from abuse. Various systems, algorithms, as well as community self-policing alert this team of potentially nefarious activities, content, and offers on the platform that they must investigate, such as:

- **Acceptable Use Enforcement** - Content moderation and site integrity maintenance, including activities such as review of harmful assets from hate groups and criminal enterprises, and phishing and malware-driven posts targeting the community.
- **Marketplace Surveillance** - Identifying, removing and potentially reporting to law enforcement counterfeit, stolen, or fake digital and physical goods for sale.
- **Fraud Investigations** - Inquiries into compromised accounts (i.e, account takeover and fake accounts), created using stolen credit cards and identities to make purchases or otherwise engage fraudulently on the platform.

All of these Trust & Safety scenarios require the ability to closely monitor and research the actions of suspicious users and groups. And in order to gather enough evidence to complete a picture of the perpetrators' activities and motives, researchers need to track them across many different sites and platforms, including the dark web.

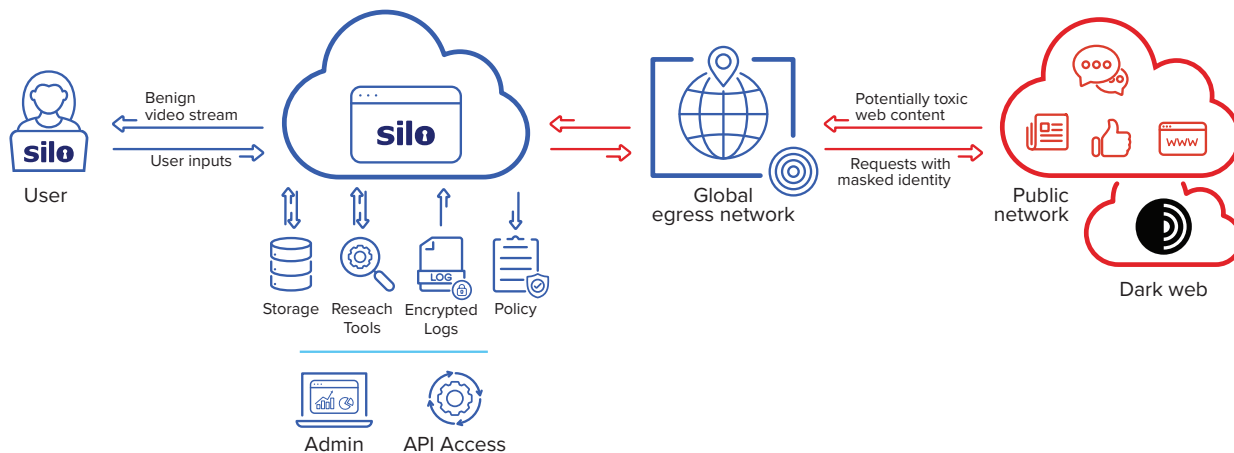
Investigators who do this type of sensitive research need to be able to blend in and maintain anonymity, in order to protect their identity and their organizations. When dealing with criminal elements and the broader web, online research needs to be isolated from malicious content and toxic sites to protect the corporate infrastructure. And with time always being of the essence, online researchers need to be equipped with the right tools for quick and safe evidence collection, collaboration and analysis.

“*[F]ocus needs to shift to wherever the customer meets the brand (think of it as “the B2C perimeter”) – whether that’s on your infrastructure (your website, your app, your contact centre) or not (copycat domains, social media, marketplace sites selling counterfeits etc).”*

<https://blogs.gartner.com/akif-khan/what-is-trust-and-safety/>

Silo for Research

Silo for Research is designed to help Trust and Safety teams conduct secure and anonymous online investigations across the open, deep and dark web. It's built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code away from your network in a secure, isolated environment that you manage by policy, providing 100% protection and oversight of all research activity.



When analysts don't conceal their identities and affiliations, their research targets can get suspicious, block the investigators from accessing needed resources, change their location or disappear altogether, or even threaten retribution against the analyst and their organizations.

Silo for Research allows you to manage your digital fingerprint. Beyond anonymity, the platform empowers analysts to blend in with the crowd including altering the attributes of their physical location, user agent string (i.e., device, OS, and browser type), timezone, and language.

In addition to the security of complete isolation from all web-borne threats and full web anonymity, Silo for Research provides analysts with an integrated suite of workflow productivity tools -- from analyzing page content, links and source data, to a safe way of manipulating and storing toxic files and inappropriate content off-network, and web page translation, capture and annotation capabilities.

The world's most at-risk enterprises and government agencies rely on Silo for Research to conduct their secure and anonymous online investigations.



CONNECT WITH US

+1 877-659-6535
www.Authentic8.com



PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.