NSIGHT SERIES

Issue 1

Managed Attribution

The foundation for effective online operations

What is managed attribution? Why should you care? What can you do about it? The answers to these questions will determine how successful—and secure—you are online

Controlling Your Online Identity

Managed attribution (MA) is the process of controlling the technical and behavioral indicators that comprise your online identity (or attribution). By managing their attribution, operators, investigators, analysts, and researchers can construct an online identity that is consistent with their mission and may persist over time, allowing them to access social media platforms, dark web markets, and other online operational domains. This MA-enabled access allows users to pursue a variety of online missions without revealing their identity or organization. In short, effective MA is the foundation for effective online operations—it's operational security for cyberspace.

Managed attribution is critical because the internet is optimized for communication, not security or privacy. When we're online, we're constantly communicating information about our digital fingerprint (technical indicators like our operating system or IP address) and our behavioral footprint (the pages we visit or people with whom we engage). Consequently, we can never truly be anonymous or non-attributed online. The digital and behavioral information we are constantly communicating makes up our online attribution, and social media providers, websites, dark web forums, advertising networks, and others can use this information to deny us access to platforms, manipulate the content we see, or expose our actual identity.

Yet, while achieving online anonymity may be virtually impossible, we can manage what information we communicate online and how we communicate it. MA solutions allow users to control their technical and behavioral indicators to create an online identity that is misattributed, or different from their actual identity and affiliation.

Defeating the Gatekeepers

Effective MA provides misattributed access to online operational domains, such as social media platforms or dark web markets, and enables a variety of online missions. This access can either be discrete or persistent, but does not tie back to the user. This is particularly important as online platforms and forums continue to raise the barrier of entry by requiring more and more identifying information. These entities are the gatekeepers to many operational domains, and effective managed attribution is critical to overcoming their challenges. Without proper MA solutions, users risk

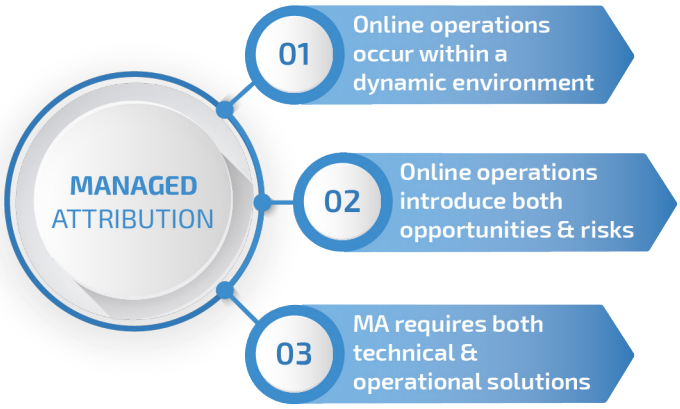
losing access, exposing their mission, and wasting the time and resources used to establish an online identity in the first place.

There is a wealth of publicly available information (PAI) online, but much of it increasingly resides on these protected platforms. At minimum, for example, social media platforms require an email address to create an account. Increasingly, however, these sites require authentic phone numbers, secondary emails, pictures, extensive social networks, and/or an authentic online pattern of life for users to access and operate on their platform. The gatekeepers use the information they collect about users' digital fingerprint and behavioral footprint to determine their authenticity. If the user is suspected to be false, they will be denied access to critical operational domains.

Discrete and Persistent Access

MA solutions can provide either discrete or persistent online access depending on users' mission requirements and resources. Discrete access manages users' IP addresses, cookie history, and other digital artifacts to provide basic access to these operational domains. In contrast, persistent access against sophisticated gatekeepers provides users with a more comprehensive MA solution that can include browsing target websites to collect trackers, egressing from a specific location, and managing other indicators to create an online identity that is consistent and may appeal to specific audiences (e.g., users on a dark web forum).

Without this access, users cannot collect PAI, create content, or engage with others. Further, by employing a limited MA solution, users heighten their risk of online exposure. This can include inadvertently revealing information about your true location, identity, affiliation, or reason for being online. Even partial exposure can suggest to platforms or other users that you are not who you say you are, which can lead to increased scrutiny.



Ntrepid's MA Framework

Ntrepid has developed an MA framework to help users make decisions about how to manage their online attribution and efficiently allocate resources for their operations. The framework consists of three primary principles.

First , online operations occur within a dynamic environment. Cyberspace can change rapidly, and managed attribution is an ongoing process of identifying these changes and assessing how they may impact your mission or ability to access PAI. Effective MA solutions must constantly anticipate, adapt, and overcome the new challenges that will inevitably arise in this dynamic environment.

Second, online operations introduce both opportunities and risks. No online activity is without consequence. Navigating

social media, for example, comes at the expense of providing a lot of identifying information. Operating on the dark web increases the risk of malware exposure. It's important to continually evaluate every opportunity—to access PAI or acquire new capabilities, for example—against its risks, and to consider how your MA solution accounts for those risks.

Finally, effective managed attribution requires both technical and operational solutions. There is no technological silver bullet for online operations—people matter, and mission success is dependent on users' ability to fuse MA solutions with operational best practices.

Effective managed attribution is the foundation for effective online operations. It is operational security for cyber operations and allows users to pursue their mission and allocate resources efficiently. The Ntrepid MA framework can help users understand how to manage their online attribution to gain misattributed access to critical operational domains. However, you need sophisticated technical solutions and proper training on how to use them to compete—and ultimately win—in a dynamic operational environment.

About Ntrepid

Ntrepid is a mission-driven provider of cutting-edge managed attribution technology solutions for national security to discreetly and safely conduct sophisticated online operations in the most demanding environments. We leverage our deep experience in the national security community to anticipate our customers' needs and provide solutions before the requirements are expressed. Our heavy investment in R&D allows us to stay ahead of the rapidly changing internet landscape. Ntrepid's innovative solutions enable advanced operational and technical capabilities while protecting your organization, mission, and operators.

Contact us to learn more about the full spectrum of Ntrepid solutions.

www.ntrepidcorp.com
1.800.921.2414
solutions@ntrepidcorp.com

Ntrepid's Nsight Series analyzes emerging trends, challenges, and technologies that impact your online operations—all from the perspective of better managing your online attribution.

NTREPID®