Authentication service for digital fraud detection and prevention

APPLICATIONS

Advanced client authentication capabilities for web and mobile based applications

- Detect and mitigate digital ad fraud
- Protect against financial account fraud, such as account takeover/ credential stuffing
- Inspect all transactions/events for bots and unauthorized users that are attempting to access your web and mobile applications
- Enrich both wire-data and end-point data with additional information (geolocation, DNS, etc.) for robust fraud detection

BENEFITS

- Increased integrity of decisioning based on both end-point AND wire-data
- Increased agility in deployment via lightweight snippet installation
- Provide the ability to programmatically monitor and deliver real-time, standardized network intelligence regarding clients in question
- Integrate with new and existing network security frameworks,

PRODUCT OVERVIEW

The MantisNet authentication solution is a cloud-native client service that continuously monitors your digital systems for fraudulent and malicious activity. Whether you are looking at access to internal service portals, verifying that advertising dollars are being spent on actual human clicks and not bot clicks, or looking to determine if external accesss to your public facing systems are origionating from legitimate sources, MantisNet authentication services provides unparalleled insights to help make informed decisions in real-time.

Upon deployment, the MantisNet authentication service continuously inspects traffic from clients that are attempting to access or transact with your systems to determine if they are legitimate, suspect, compromised, counterfeit, or otherwise invalid. This concept can be summed up as "fraud prevention"- a well known concept in the realm of cybersecurity. However, the MantisNet authentication service brings an innovative approach to fraud detection and prevention...an approach that provides deeper visibility in to these client devices by utilizing continuous real-time traffic inspection of network traffic, a source of valuable intelligence that has been previously untapped in the marketplace.

PRODUCT DESCRIPTION

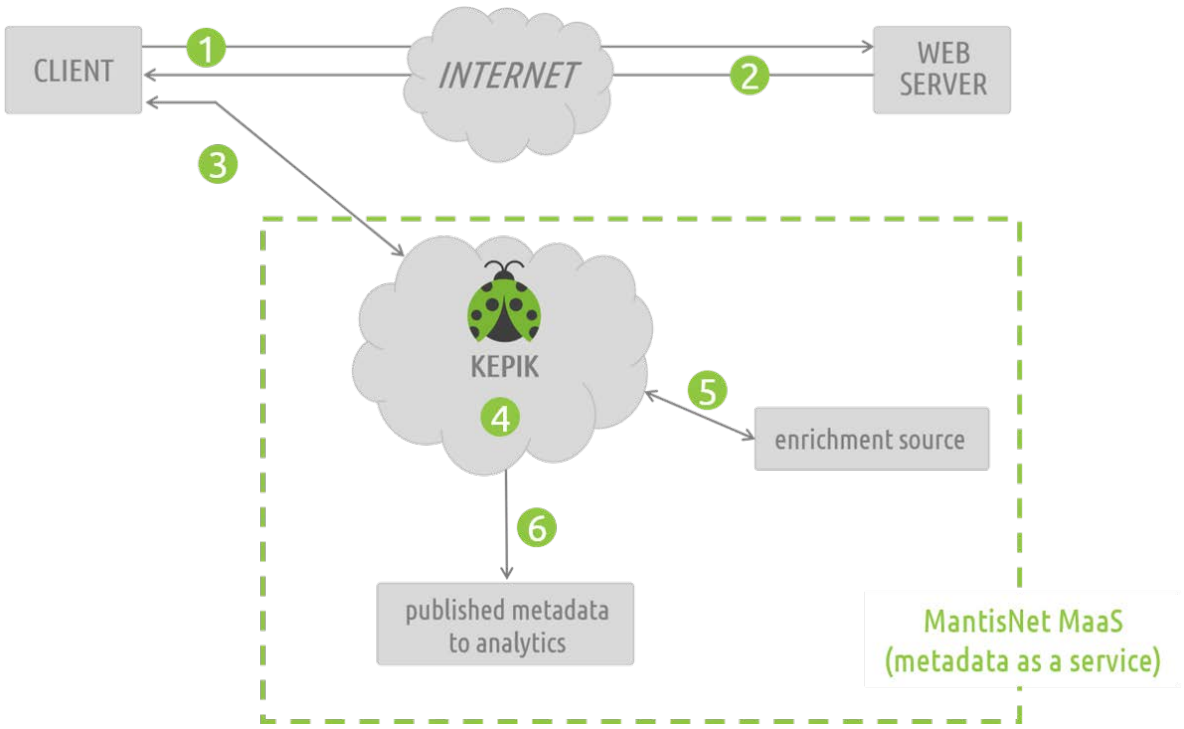
Core to the MantisNet authentication service is the ability to analyze wire-data, or network data. Wire-data is a data source that has not typically been leveraged by fraud prevention solutions. Most systems rely on end-point data which has been the de facto data source for client authentication within fraud prevention systems. While end-point data can be a useful source of information to help determine the integrity of a client/application, there are significant blind spots that nefarious actors can exploit if a client authentication system solely relies on end-point data analysis. The main problem is that bots (or humans) can spoof/mimic end-point data- they can misrepresent the application(s) they are using for connecting in to digital systems, and mislead fraud prevention systems so as to avoid detection.

The MantisNet authentication service closes the gap on these blind spots by leveraging wire-data, which is an immutable source of information. Wire-data, in its most simple form, is defined as digital information transiting network infrastructure in the form of packets. Network packets provide a "ground source" of truth that cannot be altered, hacked, or modified. By leveraging both end-point data AND wire-data as data sources for client authentication, the MantisNet solution provides organizations a new option for fraud prevention that stands above the rest.

DEPLOYMENT OVERVIEW

The MantisNet authentication solution, and underlying metadata technology, are delivered to clients as a cloud-based service. This approach provides clients with a fraud prevention environment that can tie in to any existing tools, with a rich set of both end-point information and wire-data on every client/transaction occurring within their systems.

Deploying MantisNet authentication services is straightforward. Organizations need to simply load a "code Snippet" on to the desired website or application they would like to protect in order to tie in to the MantisNet authentication service offering. The following diagram provides a high-level overview of this architecture:

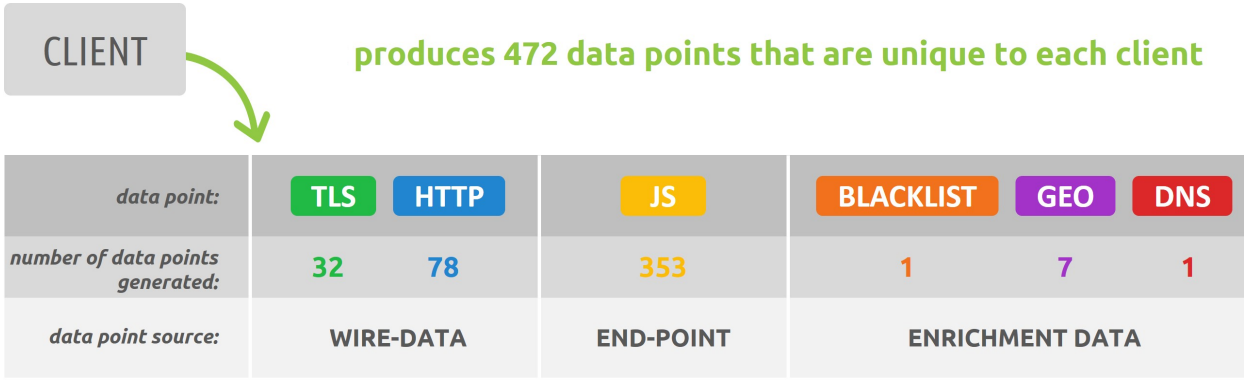


1. Client browsers to company website
2. Company web server serves up homepage with link to embedded snippet
3. Client reaches out to the server to load the web beacon
4. The server decodes TLS/HTTP protocols and generates client metadata
5. The server enriches client metadata with geolocation, IP reputation and DNS
6. The server publishes enriched metadata in to streaming analytic workflow i.e. Kafka

**note: the above figure depicts the standard cloud based service offering. On-prem solutions are available*

CLIENT FEATURE CHARACTERISTICS

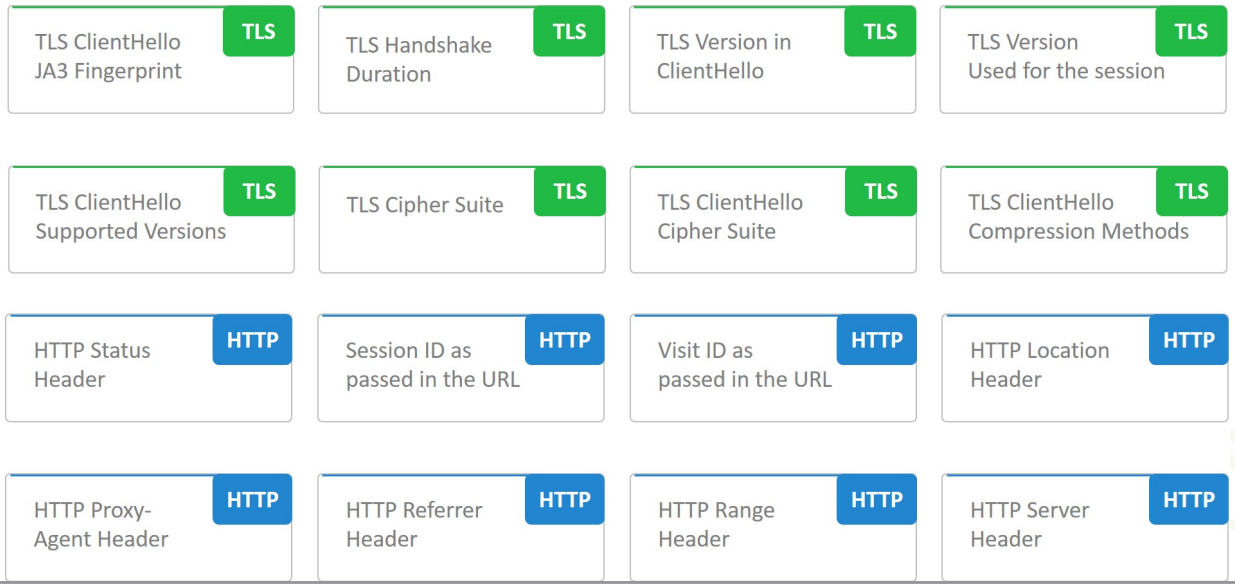
For any transaction involving client and host interactions, MantisNet's authentication solution provides authentication of the client, or more specifically- the application being used by the client. The solution generates and processes over 400 unique feature characteristics of the client application that is requesting/processing each transaction in order to determine the validity of the client. The MantisNet authentication solution works with a wide range of fraud detection, authentication, and enrichment sources to provide users with a thorough understanding of all clients attempting to gain access to, or transact within, your digital systems.



CLIENT SPECIFIC WIRE-DATA

As outlined in the above chart, the MantisNet authentication service generates 110 unique data points that are sourced from wire-data for each client. The wire data points being generated are structured as serialized key,value pairs- an open-standard format ideal for feeding machine learning and artificial intelligence systems.

By analyzing and generating metadata associated with TLS and HTTP network packets, the service provides users with a new and orthogonal source of intelligence to help better determine the integrity of clients attempting to access digital systems. See below for a few examples of these data points:



ABOUT MANTISNET

MantisNet develops Software Defined Network (SDN) and Network Function Virtualization (NFV) network intelligence solutions that provide businesses and governments real-time network monitoring solutions, for 100G speeds and beyond. MantisNet's solutions better enable network teams to monitor, manage and engineer the increase in network traffic flows they're experiencing compared to the preceding generation of packet brokers, firewalls, load balancers and event management solutions.

MantisNet combines end-to-end visibility, wire-speed network monitoring and protocol analysis (from L2 to L7) with the ability to perform real-time traffic engineering and remediation against operational issues, security threats, fraud, and malicious activities, either manually or autonomously. Our solutions are deployed at leading telecom, service providers, NEM labs and government sites. We work to make network intelligence actionable for a broad range of DevOps, network and application performance testing, streaming analytics, and cyber security applications.

For more information, visit www.MantisNet.com

11160 C1 SOUTH LAKES DRIVE, SUITE 190 RESTON, VA 20191
(571)306-1234
INFO@MANTISNET.COM