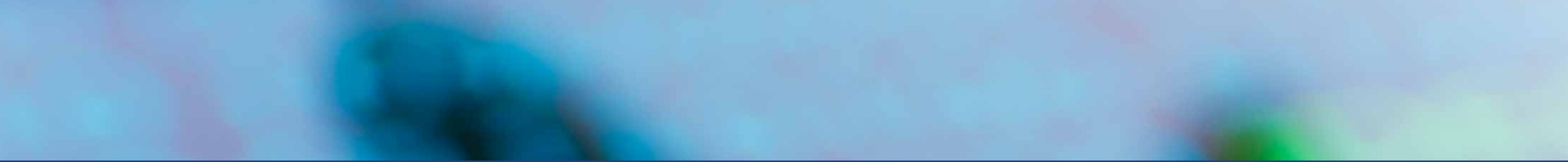
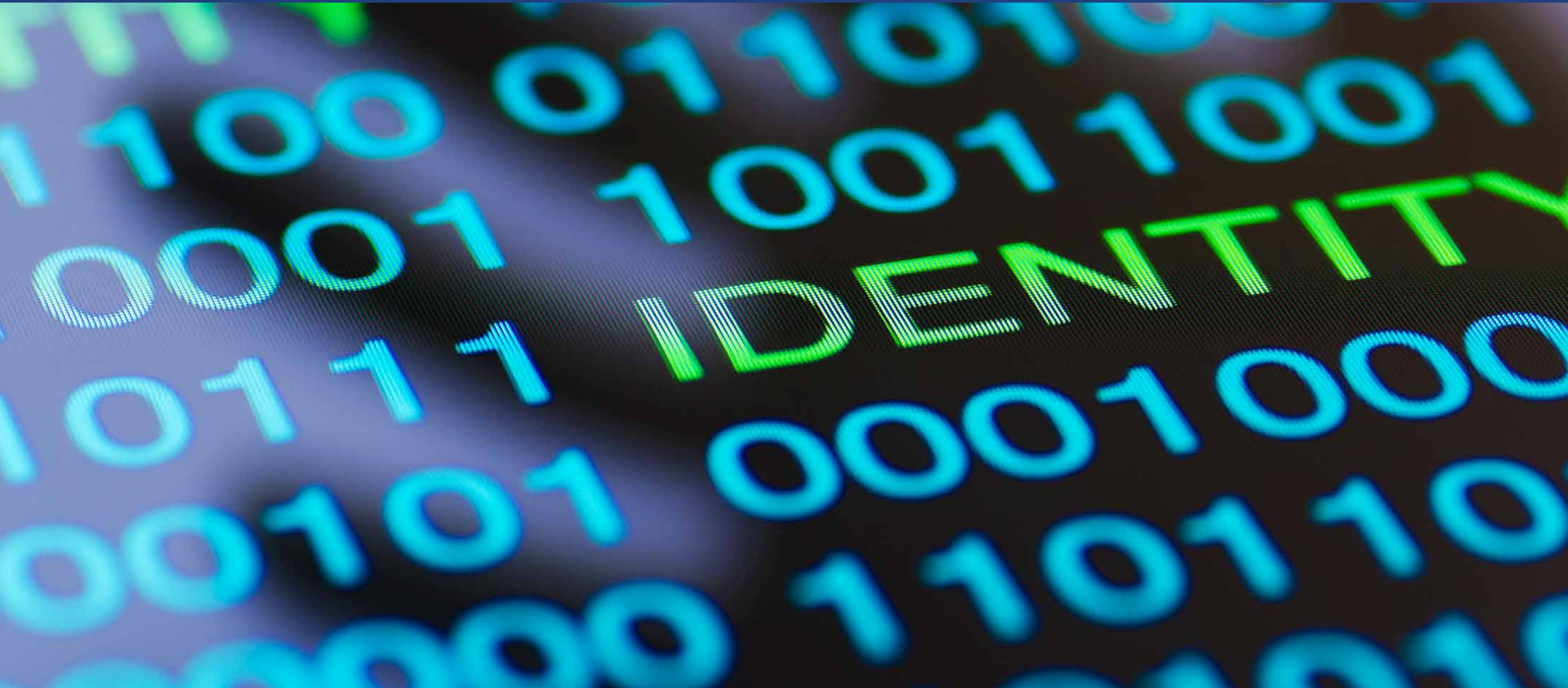


digital element®
Location is Elemental ™

How IP Intelligence Is Used to Detect and Prevent Online Fraud

An Industry Brief for Latin America



Latin America Experiences Explosive Growth in Online Fraud

Global e-commerce sales are predicted to reach $4 trillion in 2020, making up 14.6 percent of total retail spending, according to eMarketer.[I] In Latin America, the e-commerce market is expected to exceed $118 billion by the end of 2021. In fact, two of the three fastest-growing e-commerce markets in the world are in Latin America: Colombia and Argentina.[II]

> A downside of this explosive growth is the increased opportunity for online fraud. Recent research showed that cyber frauds grew 88 percent year over year in Latin America in the First Quarter 2018. Regional trends in cybercrime, such as that of new-account origination fraud, are having a strong impact on the volume of attacks seen coming from key Latin American countries, for example Brazil.[III]

South America continues to be at the epicenter of new-account origination fraud:

- 34 percent of all new-account origination fraud comes from South America.
- 54 percent of all new-account origination fraud targeting media companies comes from South America.
- Most attacks target e-commerce merchants as well as sign-ups for new media accounts associated with free trials (that can then be fraudulently resold for a profit).

Source: Q1 2018 CyberCrime Report

Not only does the actual fraud hurt, but making inadvertently wrong decisions to avoid fraud costs also impacts merchants. The Merchant Risk Council's 2017 Global Fraud Survey showed that the average online store declined 2.6 percent of all incoming orders due to fear of fraud, including 3.1 percent of all orders worth more than $100.[IV] For a $10-million business, this means a loss of nearly $300,000 annually. But the true cost of declines is actually far higher than just the lost sales revenue.

South America continues to be at the epicenter of new-account origination fraud:

34%

34% of all new-account origination fraud comes from South America.

54%

54% of all new-account origination fraud targeting media companies comes from South America.

Most attacks target e-commerce merchants as well as sign-ups for new media accounts associated with free trials (that can then be fraudulently resold for a profit).

Source: Q1 2018 CyberCrime Report

Online retailers in Latin America are definitely paying a price in turning away more legitimate customers and manually reviewing more orders:

82%

82% of merchants conduct manual reviews

9.2%

9.2% of orders are rejected due to suspicion of fraud

57%

57% of orders are accepted post review

1.7%

1.7% of sales become chargebacks

Source: 2017 Online Fraud Report for Latin America

Online retailers in Latin America are definitely paying a price in turning away more legitimate customers and manually reviewing more orders:

- 82 percent of merchants conduct manual reviews
- 9.2 percent of orders are rejected due to suspicion of fraud
- 57 percent of orders are accepted post review
- 1.7 percent of sales become chargebacks

Source: 2017 Online Fraud Report for Latin America

These are substantial numbers, yet careful management of the authentication process and deployment of the right tools can yield significant results in terms of online fraud reduction.

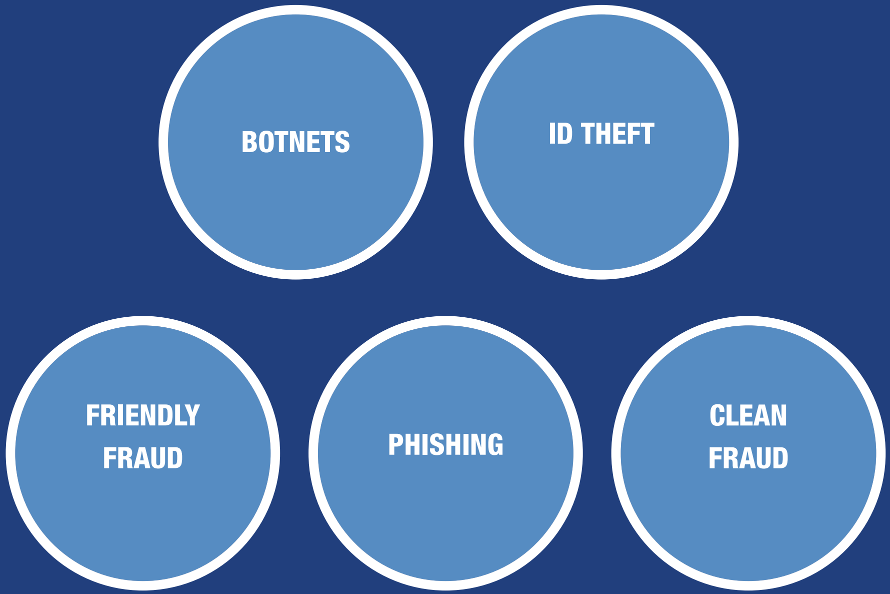
IP Intelligence Is a Top-Five Fraud Tool

The most effective fraud prevention involves multiple technology solutions that work in tandem to identify who real customers are and how they perform activities and transactions online. Accurately recognizing a user's digital identity can be based on a variety of data parameters (i.e. location, device type, etc.) and combined with behavioral analytics to help merchants more successfully distinguish between legitimate consumers and potential fraudsters, blocking high-risk activities in real time.

Not All IP Vendors Are Created Equal

> Implementing IP information ranks in the top five of all tools deployed by merchants using automated screening systems, but not all IP solutions are created equal. There is a vast chasm between those who simply repackage publicly-available data and premium providers who deploy multiple methodologies to analyze IP-routing infrastructure.

Five Key Fraud Types That Can Impact Your Business


BOTNETS

ID THEFT

FRIENDLY FRAUD

PHISHING

CLEAN FRAUD

digital element®
Location is Elemental ™

There are several suppliers and systems available that can determine where an IP is and for a small investment an answer can be provided, but is it the right one? Determining the correct location of an IP address and discovering other critical fraud-prevention data, such as proxies, requires advanced infrastructure analysis, as opposed to simply scraping Internet registries or repackaging publically available free data.

Digital Element's premium IP data, at its most granular level, can accurately locate a user down to the city/postal code sector level without becoming personally-identifiable. The coverage is global, accuracy is 99.99 percent at a country level, and the data is refreshed regularly. Importantly, it can also determine how a user connects; enabling the identification of data that merchants need to effectively combat fraud such as proxies, virtual private networks (VPNs), satellites, anonymisers, tors, mobiles, Internet Service Providers (ISPs), domains and hosting centers.

This is achieved by combining IP routing infrastructure analysis with anonymous location insight gleaned from a network of global commercial partners.

NetAcuity® is an effective one-source solution that is simple to integrate into merchant systems and manage in house. Conversely, publically available data has patchy global coverage, is rarely updated, is limited in terms of data parameters identified and is inherently inaccurate.

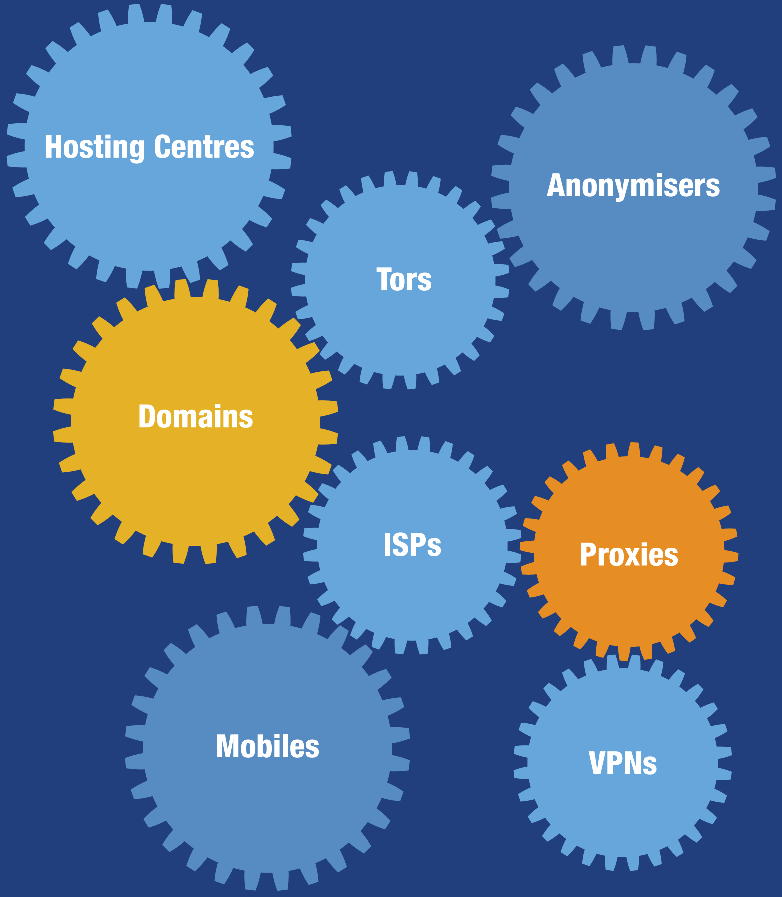
What Are the Fraud Types?

The greatest threats for Latin American digital merchants are clean fraud, ID theft, friendly fraud, phishing and botnets. Digital Element's NetAcuity IP Intelligence delivers technology that can expose the anonymity or lift the cloak of the fraudster.

Invest in Smarter Rules

Building smarter rules around fraud detection and automating the process is proven to increase detection rates, reduce false positives and improve the visitor experience. IP Intelligence can be used to automatically block suspect traffic, request verification (via email or SMS), or flag suspect activity for further internal review.

Building Smarter Rules Around Fraud Detection and Automating The Process is Proven To Increase Detection Rates, Reduce False Positives and Improve Visitor Experience.



digital element
Location is Elemental ™

Geography is part of the fraud-detection landscape and smart merchants take it further than just location, by using NetAcuity's advanced intelligence parameters to identify proxies, VPNs, anonymisers, Tors, mobiles, ISPs, domains and hosting centers. By providing more than just geography, NetAcuity IP Intelligence can identify greater numbers of suspicious connections.

What Rules Should be Employed?

Check IP Address for Country of Origin

A company trading internationally will often block common high-risk fraud countries such as Nigeria, India, Pakistan, Russia and even Brazil. Additionally, if a user is known to reside in a specific country, access to an account from another country could be deemed suspect. A basic "registry scraped" system will not be able to accurately determine the location of a user. Also, free IP data cannot identify if visitors are masking the country they are accessing the internet from (via a proxy or anonymiser), allowing potentially fraudulent activity to take place.

Bill-to/Ship-to IP Address Locations

If the bill-to/ship-to IP addresses do not match, an automated red flag can be passed for further review, or the account holder could be asked for verification via an email or text.

Domain Names

Reviews of known fraud domains and risky internet locations, such as public Wi-Fi hotspots, internet cafes and university/colleges, should be regularly conducted.

Proxies

Understanding the type of proxy a visitor is connecting to the internet with, such as anonymous, transparent, corporate, public, education or blackberries, can trigger fraud alerts. Responses to the type of proxy can vary depending on what type of proxy it is—for example, an anonymous proxy may warrant a higher fraud score than a corporate one. By identifying connections that obscure the end-user location or those that seek to portray a connection from an "acceptable" city or country can now be easily identified and categorized.

When should rules be employed?

- ► SIGN UP
- ► LOGIN
- ► PURCHASE
- ► FUNDS DEPOSIT
- ► WITHDRAWAL

Hosting

End-user traffic should generally not be seen from hosting or data centers as these types of facilities are designed for traffic to pass through, not originate from. Some cloud browsers do use these centers, but services are patchy and not widely developed. Reviewing these with other CRM data is highly recommended before order acceptance is confirmed.

Home, Business and ISP

Additional layers of intelligence can be added that identify whether a connection is a home or business as well as which ISP is being used. The data can be used to build profiles of previous connectivity to assess differences or anomalies over time.

When Should Rules be Employed?

The critical points of any authentication or payments system are during sign up, login, purchase, funds deposit or withdrawal.

Ideally, continually check at every stage of the purchase process to ensure the session has not been hijacked.

Mobile Transactions

The global mobile payments market is estimated to reach $3.38 billion by 2022.[V] While 84 percent of Latin American merchants operate mobile commerce websites and apps, almost 30 percent are not using a fraud-management tool in their mobile channels.[VI]

Using a mobile device for ecommerce and completing the purchase still creates an IP connection. Users are 80 percent more likely to be on a Wi-Fi network due to speed, convenience or cost—only 20 percent connect via 3G, 4G or LTE.

A Wi-Fi connection is just the same as a desktop setup in that NetAcuity can accurately determine the Wi-Fi location and the type of proxy being used so the same rules apply. If the connection is via 3G, 4G or LTE, then network characteristics identifying the service provider and its connection hub are seen.

Compelling reasons to know more about your traffic

Reduce Fraudulent Activity by 90%

Deploy on a Server in less than 20 minutes

digital element®
Location is Elemental ™

Compelling Reasons To Know More About Your Traffic

Understanding where and how visitors connect to a site can result in more accepted orders, less false positives and reduced fraud. Automation is key and NetAcuity's IP Intelligence provides a simple one-source solution to enable digital business to reduce fraudulent activity by as much as 90 percent.

Easy to deploy on an internal server in less than 20 minutes and queried by various supplied APIs, NetAcuity has a response time that is fast and reliable at less than 0.03 milliseconds—allowing it to handle up to 30,000 requests per second.

Some of the Data We Provide to Protect Our Clients

Proxy Type	
• Anonymous	Actual IP address of the end users is not available which often includes the use of services that change location to circumvent digital rights management, TOR points (free software for enabling anonymous communications), temporary proxies and other masking services.
• Transparent	Actual IP address of the end user is available via HTTP headers, although the value is not necessarily reliable (i.e. it can be spoofed).
• Hosting	Addresses belong to a hosting facility, and end users are not typically located in a hosting facility.
• Corporate	Generally considered harmless, but their location can occasionally be a concern. Multiple users proxied through a central location or locations, and thus sharing a single network-apparent IP address, are not reliable.
• Public	Multiple users are proxied from a location allowing public internet access (i.e. libraries).
• Edu	End users come from an educational institution with the .edu extension.
• AOL	AOL proxy
• Blackberry	All Blackberry users go through a centralized proxy location and thus cannot be accurately geotargeted.
• "?"	A return that indicates there is no evidence to support proxy activity for a given IP address (used to initially parse proxy vs. non-proxy online traffic).
Proxy Identification	
• Tor Exit	The gateway nodes where encrypted/anonymous Tor traffic hits the internet.
• Tor Relay	Where the Tor network receives traffic and passes it along. Also referred to as a "router."
• Cloud	Enables ubiquitous network access to a shared pool of configurable computing resources.
• VPN	The virtual private network encrypts and routes all traffic through the VPN server, including programs and applications.

NetAcuity Global Client Base

emailage™
The Global Hub of Email Intelligence

Symantec.

BBVA

LogRhythm™

inter
BANCO

experian.™

globo
.com

JPMorgan Chase & Co

Televisa

Contact us to learn more about how we can help protect your online initiatives from fraud.

www.digitalelement.com

North American Headquarters
155 Technology Parkway Suite 800
Norcross, GA 30092, USA
+1 678.258.6300

European Headquarters
8 Northumberland Avenue
London WC2N 5BY, United Kingdom
+44 (0) 2035 142 663

digital element®
Location is Elemental ™

There is significant value in investing in a multi-layered approach for fraud mitigation. Findings show that the right multi-layered approach can justify upfront costs of the solution investment as greater accuracy yields more positive results on the bottom line.[VII]

Knowing more about where your customer is coming from as well as how they connect will deliver many of the improvements needed in merchant payment systems.

Digital Element is the only dedicated global provider of IP Intelligence. With nearly two decades of experience and knowledge, specialized Latin American teams can advise on how to defend against online fraud.

NetAcuity Tidbits and Some Techie Stuff

- Client Platform – Integrates with most operating systems and applications
- Support – 24/7 technical support
- Latency – As low as .03 milliseconds
- Database updates happen weekly
- Provides support for a variety of popular 64-bit computing platforms: Red Hat Enterprise Linux 5, Solaris 10-Intel, Solaris 10-SPARC,Windows 2003/2008 Server
- Processing – Capable of over 30,000 IP resolutions per second
- Restful Interface
- Up-and-running in as little as 20 minutes
- Application Programming Interface (API) – C, C++, C#, Perl, Java, PHP, .NET, Ruby, Python, Node.js, Apache Module, Go, Nginx or custom support available for a wide array of programming languages and client platforms

[I] eMarketer, “Retail Ecommerce Sales Worldwide 2015-2020, August 2016.

[II] Dowd, Miriam, FocusEconomics, “Latin America Is the World Leader in Ecommerce Growth Despite Serious Challenges,” Mar. 22, 2018.

[III] Q1 2018 CyberCrime Report, 2018.

[IV] Merchant Risk Council, 2017 Global Fraud Survey, 2017.

[V] Allied Market Research, “Mobile Payments Market Global Opportunity Analysis and Industry Forecast, 2014-2022,” Jan. 11, 2017.

[VI] Visa, 2017 Online Fraud Report for Latin America, 2017.

[VII] LexisNexis, “The True Cost of Fraud Study,” 2016.

Latin America Contact:

Jorgelina Striedinger, Vice President, Latin America

jstriedinger@digitalelement.com
www.digitalelement.com

Mobile: +1 404-409-3055 **Office:** +1 678-258-6343 **Skype:** Jorgie11