CSC

2022

DOMAIN SECURITY REPORT

SUMMARY OF KEY FINDINGS—WHAT'S NEW IN 2022?

CSC has been reporting on the domain security posture of the Forbes Global 2000 companies annually for the last three years. This year, we're seeing some companies becoming more secure, but there are still a portion of companies with considerable domain security risk. It's our intent to elevate the awareness of these threats and share domain security best practices to improve all organizations' domain security posture.

NEARLY 3/4

OF GLOBAL 2000 COMPANIES HAVE AN ALARMINGLY HIGH RISK OF EXPOSURE TO SECURITY THREATS

Nearly three quarters of the Global 2000 companies have implemented less than half of all domain security measures. CSC looked at eight key security measures and derived an average score for each company. The higher the score, the stronger the security posture.

45%

OF COMPANIES THAT USE ENTERPRISE-CLASS REGISTRARS ALSO USE REGISTRY LOCK

A registry lock enables end-to-end domain name transaction security to mitigate human error and third-party risk. It's a highly cost-effective means to protect domain names against accidental or unauthorized modifications or deletions. Only 5% of companies that use consumer-grade registrars have registry lock deployed. Unlocked domains are vulnerable to social engineering tactics, which can lead to unauthorized DNS changes and domain name hijacking.

75%

OF THE REGISTERED DOMAINS THAT RESEMBLED THE GLOBAL 2000 BRANDS (HOMOGLYPHS) ARE OWNED BY THIRD PARTIES

Of the 75% of homoglyph (fake) domains owned by third parties other than the Global 2000 brand owner, 82% have their WHOIS or ownership details masked in 2022, compared to 77% in 2021, showing that more are using WHOIS privacy protection.

<5%

GROWTH IN IMPLEMENTING OTHER PROACTIVE DOMAIN SECURITY MEASURES

Companies are struggling to qualify for cyber insurance rates they can afford, and domain security is one area where the fix is a relatively low cost compared to other cyber expenses. With the risks of not having domain security in place potentially leading to phishing or ransomware attacks, and many other cyber threats, we hoped to see a higher implementation of some of these security measures, such as registry lock, domain name system (DNS) redundancy, DNS security extensions (DNSSEC), and certificate authority authorization (CAA) records.

23%

GROWTH IN DMARC WITH HIGHEST GROWTH RATE

The most recent figures from the Anti-Phishing Working Group (APWG) show the numbers of phishing attacks are higher than ever before, growing tenfold since 2020—so it's not surprising this has helped increase the adoption of domain-based message authentication, reporting, and conformance (DMARC)—an email validation system designed to protect a company's email domain from being used for spoofing, phishing scams, and other cybercrime.

AS ZERO TRUST SECURITY MODELS BECOME A TOP DEFENSIVE SECURITY STRATEGY, 2022 HAS SHOWN HOW CRITICAL IT IS TO INCLUDE DOMAIN SECURITY

Zero Trust models must extend beyond business systems, applications, and devices, and include a company's domain ecosystem as a real vulnerability to the attacks noted in Figure 1. The following two domain security threats are used to enable all of the attacks listed below.

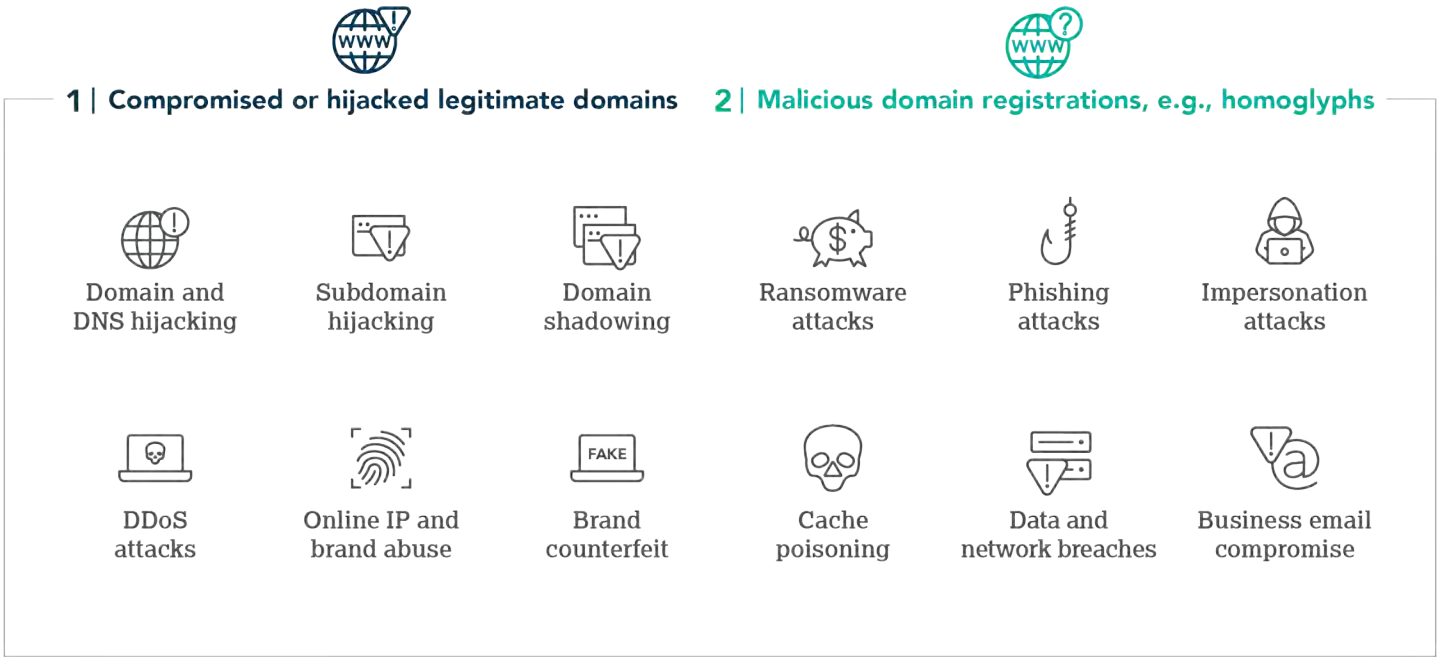


Figure 1

Global businesses rely on the internet for everything—websites, email, authentication, voice over IP (VoIP), and more. It's part of an organization's external attack surface and needs to be continuously monitored for cybercrime attacks and fraud. As cyber risks continue to increase, organizations and cyber insurers face greater challenges in quantifying them and addressing their capacity for harm. Seemingly every day, we learn about new developments involving supply chain attacks, ransomware, and phishing attacks, along with additional layers of complexity in terms of what coverage they require and how to stop them.

DOMAIN SECURITY DEFINED

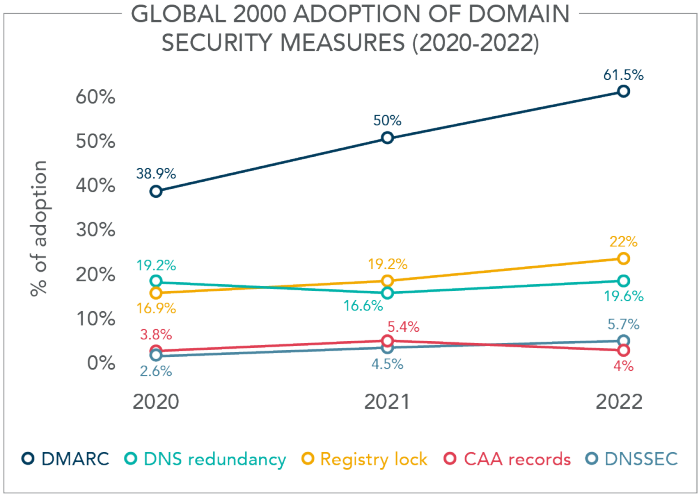
CSC administers domain security with a layered approach. First and foremost, it involves securing a brand's online presence by securing the domain portfolio—which may consist of multiple brands through acquisitions—and an online DNS footprint. Secondly, we monitor, analyze, and enforce on threat vectors targeting online brands. And lastly, we complement these other two data sets with the internal data sets behind the firewall to give a fully comprehensive picture of a brand's security posture.

This report looks at the security posture of the Global 2000 companies, a list that is refreshed by Forbes each year (i.e., each year new companies make it to the list, and a few companies that were previously listed may not rank in the top 2000). The insights shared in this report are based exclusively on publicly available data sets that are managed via a one-of-a-kind proprietary data lake powered by machine learning, artificial intelligence, and deep search technology.

FINDINGS AND ANALYSIS

In this analysis, CSC looked at the adoption of the domain security measures outlined below across the Global 2000 list, and then we performed a deep dive into the industry groups and regions.

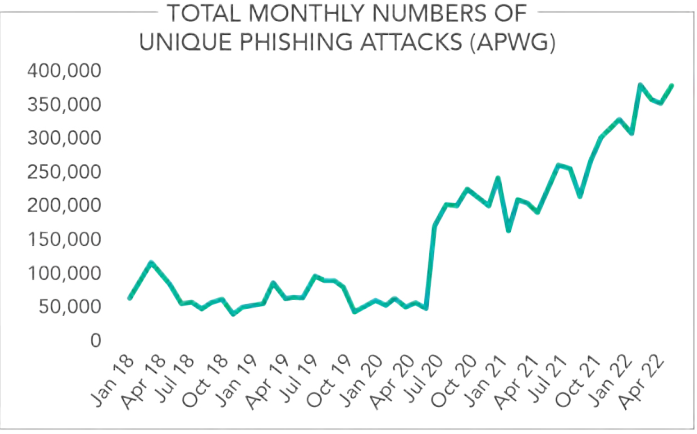
TRENDS IN ADOPTION OF DOMAIN SECURITY MEASURES (2020-2022)



DMARC USE HAS NEARLY DOUBLED IN TWO YEARS

It's no surprise given all the news about phishing attacks—including their increase in volume and complexity—that DMARC use has risen quite quickly from 39% in 2020 to 62% in 2022.

The most recent figures from APWG show the numbers of phishing attacks are higher than ever before, with the quarterly total of identified unique phishing attacks exceeding 1 million for the first time in Q1 2022, and over 600 distinct brands attacked each month.



Also, driving growth in DMARC is that Verified Mark Certificates (VMC) are now requiring DMARC to be set up to ascertain the secure sockets layer (SSL) certificate. Additionally, Apple announced Brand Indicators for Message Identification (BIMI) in September and stated that its email clients for iOS 16 and macOS will support a broad industry effort to combat brand spoofing and impersonation. Senders that support BIMI must meet a strong standard of email authentication and this includes using the DMARC security standard.

It's very easy to spoof email and make it look like it's being sent from a legitimate source when it really isn't. Yet while authenticating the email channel with DMARC minimizes the incidence of email spoofing and potential phishing, we also know that even with this control in place, not having a DMARC reject policy still poses phishing risks and needs to be included in the implementation.

GROWTH OF SECURITY MEASURES SUCH AS REGISTRY LOCK, DNS REDUNDANCY, DNSSEC, AND CAA RECORDS HAS BEEN CONSISTENT, BUT SLOW

Companies having registry lock turned on went from 17% adoption in 2020 to 19% in 2021 and 22% in 2022. A registry lock enables end-to-end domain name transaction security to mitigate human error and third-party risk. It's a highly cost-effective means to protect domain names against accidental or unauthorized modifications or deletions. However, some domains may remain unlocked, as not every registry around the world offers lock services.

Companies deploying DNS redundancy and DNSSEC have gone up slightly over the past three years. More government agencies are calling for resilience in the DNS, as a it makes a critical component in any organization's core infrastructure, and so while the increase in adoption aligns with increasing pressure for organizations to step up, we have yet to see greater rates of adoption that could be attributed to companies needing to plan for increasing cost and resource allocation.

Lastly, the use of CAA records went up slightly from 2020 to 2021, but back down slightly again in 2022. CAA records allow companies to designate a specific certificate authority (CA) to be the sole issuer of certificates for their company's domains. This prevents cybercriminals from using a non-appointed certificate authority to get a new certificate. Their request will fail, and the company will receive an alert. However, many companies still don't fully use this security control, as it's often difficult for them to navigate the requirements, especially when they use multiple providers for their domains, DNS, and SSLs.

2022 DOMAIN SECURITY MEASURES BY REGISTRAR TYPE

For this report, we analyzed the trend of domain security adoption with respect to the type of domain registrar used by the companies that make up the Global 2000.

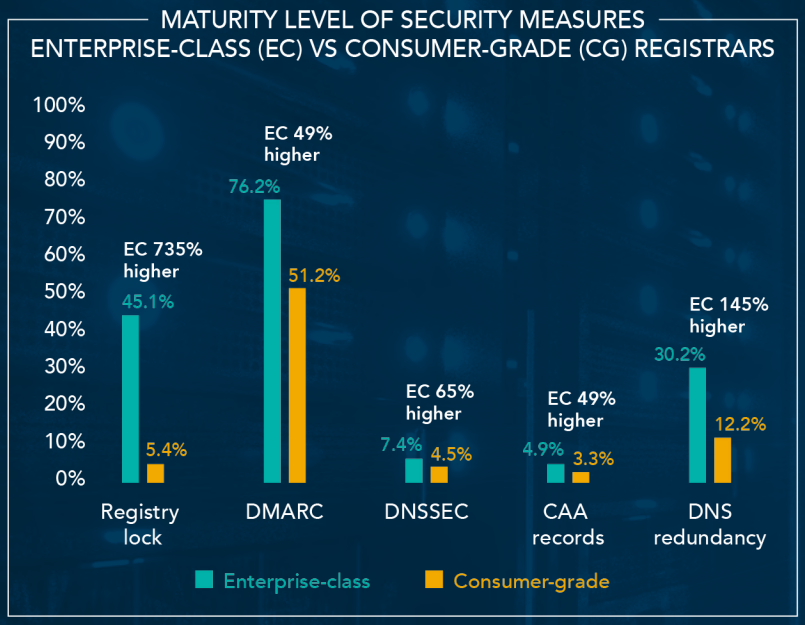
CONSUMER-GRADE REGISTRARS:

A consumer-grade registrar is geared for domain services, websites, and email for personal use, entrepreneurs, and small businesses that are just getting started.

ENTERPRISE-CLASS REGISTRARS:

An enterprise-class registrar specializes in working with corporations and brand owners that require advanced business practices, capabilities, expertise, and support staff in relation to domain and DNS management as well as security, brand and fraud protection, data governance, and cybersecurity.

Companies that rely on enterprise-class capabilities have a higher adoption of the domain security measures.



Many companies have a misconception that all registrars are the same. There's misplaced trust put into consumer-grade registrars that may not have been designed for domain security that can impact a company's overall security posture. This is especially apparent for the adoption of registry locks, as most consumer-grade registrars do not support them.

IN LATE 2021, SecurityScorecard researched the cyber ratings of companies that used enterprise-class registrars versus consumer grade. Their findings showed that companies that have their domains managed by enterprise-class domain registrars have one-half to a full letter grade higher overall cybersecurity rating.

TO LEARN MORE:

- Domain Security Starts with Your Registrar
- Your Cybersecurity is Only as Strong as Your Weakest Vendor
- Vendor Selection Matters in the Domain Registrar Ecosystem

OVERALL DOMAIN SECURITY POSTURE

Looking at the importance of eight key security measures that we grouped according to a company's **domain security risk level,** CSC derived an average score for each company. This average makes up the company's security score with a higher score denoting a stronger security posture—meaning companies are at less risk of domain security threats.

KEY DOMAIN SECURITY MEASURES

- Enterprise-class registrar
- Registry lock (MultiLock)
- CAA records
- DNS redundancy
- DNSSEC
- SPF
- DKIM
- DMARC

NEARLY 3/4 OF COMPANIES HAVE IMPLEMENTED LESS THAN HALF OF ALL DOMAIN SECURITY MEASURES

TOP FIVE PERFORMING INDUSTRIES

- IT software and services
- Business services and supplies
- Hotels, restaurants, and leisure
- Media
- Aerospace and defense

HIGHEST PERFORMING COMPANIES

6 companies had the highest security score with the most adoption of domain security measures.

2/3 of these are U.S. companies.

BOTTOM FIVE PERFORMING INDUSTRIES

- Consumer durables
- Food markets
- Construction
- Trading companies
- Materials

LOWEST PERFORMING COMPANIES

137 companies have a domain security score of zero

These companies are primarily from the APAC region, making up **82%** of the zero-scoring companies

The lowest performing industries, namely food markets, materials, and construction, are at the highest risk for a cyberattack due to a lack of domain portfolio security measures. Supply chain issues coincide with myriad materials, labor, and distribution issues these three industries are already tackling, causing more problems. Consumer durables is also in the bottom five industries including automotive companies. It's important to note, there has been a shift with these companies to have stronger cybersecurity postures now that the Internet of Things (IoT) is such a big part of the more personalized features within new cars. These companies will need to mitigate more potential threats.

RELATIONSHIP BETWEEN DOMAIN SECURITY SCORE AND THE GLOBAL 2000 RANKING

The better a company's rank on the Global 2000, the better domain security posture a company has.

SUSPICIOUS OR MALICIOUS DOMAIN ACTIVITY TARGETING THE GLOBAL 2000

We identified and analyzed domains containing the brand names with more than six characters from the Global 2000 companies that were not owned by the brands themselves. The intent of these fake domain registrations is to leverage the trust placed on the targeted brand to launch phishing attacks or other forms of digital brand abuse or IP infringement that leads to revenue loss, traffic diversion, and a diminished brand reputation.

There are endless domain spoofing tactics and permutations that can be used by phishers and malicious third parties.

WE INTENTIONALLY FOCUS ON COMMON HOMOGLYPHS AS THEY ARE ONE OF THE MOST EGREGIOUS ATTACK METHODS USED BY THREAT ACTORS.

DOMAIN SPOOFING TACTICS

Fuzzy matches

cscg1obal.com cscgl0bal.com

Homoglyphs–IDNs

ćscglobal.com csçglobal.com

Cousin domains

cscglobal.jp cscglobal.ec

Keyword match

cscglobalcovid.com covidcscglobal.ar covid19.com

Homophones (Soundex)

siesiglobal.com cscclobol.com

COMMON HOMOGLYPHS (FUZZY MATCHES) IN .COM DOMAINS

Based on frequent observation of use in phishing domains, our analysis included common Latin-character substitutions, for example, using C0rnpanyName.com to look like CompanyName.com

C0rnpanyNarne.com

Most popular character substitutions

i → l	m → rn	i → 1
s → 5	o → 0	e → 3
l → 1	l → i	w → vv

75% Over 75% of homoglyph domains are owned by third parties. This is consistent with findings in 2021.

OUT OF THE THIRD-PARTY OWNED DOMAINS:

82% have their WHOIS or ownership details masked in 2022, compared to **77%** in 2021, showing that more are using privacy protection. This demonstrates the attempt to mask or hide their ownership and identity, showing they may have some nefarious intentions.

48% have MX records in 2022. This compares to **43%** in 2021. MX records can be used to send phishing emails or to intercept email.

HOW ARE THIRD-PARTY DOMAINS BEING USED?

46% are pointing to advertising, pay-per-click ads, or are being used for domain parking.

41% had inactive websites.

5% were pointed toward malicious content. Undesirable content could damage a brand's reputation and customer confidence. The risk is that the user could engage with websites that contain malicious content or attempt to steal sensitive information.

8% resolve to a live website not associated with the brand holder.

DOMAIN REGISTRARS MOST ASSOCIATED WITH FAKE DOMAIN REGISTRATIONS OWNED BY THIRD PARTIES:

GoDaddy® | Namecheap™ | PDR LTD

SUSPICIOUS AND MALICIOUS DOMAINS: WHO'S BEING TARGETED?

TOP INDUSTRIES BEING TARGETED WITH FAKE DOMAIN REGISTRATIONS

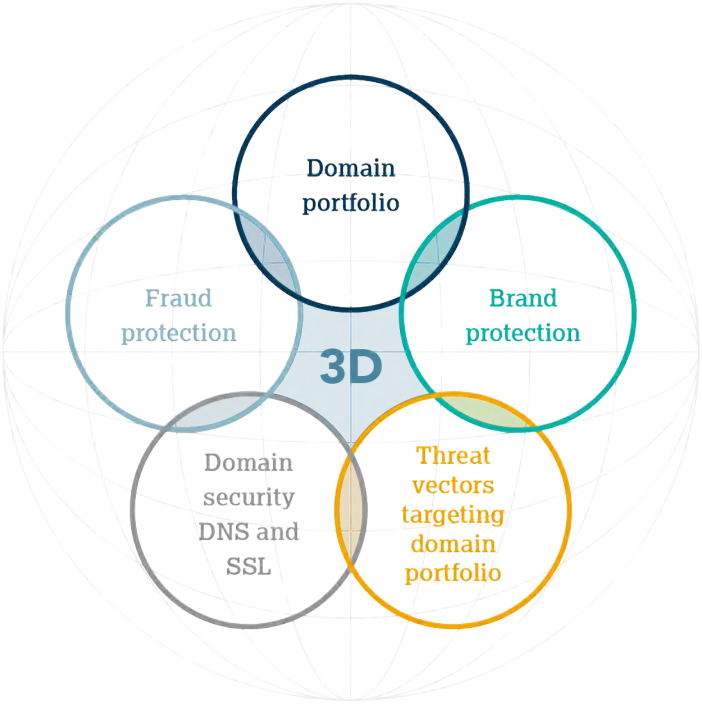
Industry	Fake domain threats % of total
Banking	10.0%
IT software and services	7.0%
Business services and supplies	5.5%
Consumer durables	5.4%
Health care equipment and services	4.6%
Diversified financials	4.6%
Drugs and biotechnology	4.6%
Telecommunications services	4.5%
Transportation	4.2%
Insurance	4.1%
Oil and gas operations	3.9%
Construction	3.7%
Materials	3.5%
Food, drink, and tobacco	3.5%
Retailing	3.2%
Chemicals	3.2%
Technology hardware and equipment	3.2%
Hotels, restaurants, and leisure	3.0%
Capital goods	2.8%
Utilities	2.7%
Aerospace and defense	2.5%
Household and personal products	2.1%
Trading companies	2.0%
Conglomerates	2.0%
Media	1.8%
Semiconductors	1.7%
Food markets	0.4%

ABOUT CSC'S DOMAINSEC℠ PLATFORM

CSC's 3D Domain Security and Enforcement solution was created by harnessing the power of CSC's DomainSec platform.

DomainSec is a software as a service (SaaS) cybersecurity platform that CSC invented, and is the industry's first holistic approach for securing and defending brands' domain ecosystems. It uses proprietary Machine Learning Deep Search (MLDS) technology and combines machine learning, artificial intelligence, and clustering technology to identify lead indicators of compromise.

DomainSec brings CSC's domain management and domain security into one platform, along with brand protection and fraud protection solutions—meaning we can offer exponentially better protection and help organizations refine their Zero Trust security model, going beyond just safeguarding perimeters.



CONCLUSION

The risk of a company not addressing their domain security can be catastrophic. Domains that are not being protected pose a significant threat to cybersecurity posture, data protection, consumer safety, intellectual property, supply chains, revenue, and reputation. We can expect awareness of the issues to grow, and that cyber insurance providers will start holding clients accountable for the quality and rigor of their domain defense strategies and approaches.

Companies need a layered security model within the Zero Trust framework to create a robust corporate security posture with the least risk to the business. As noted, components of this approach include partnership with an enterprise-class registrar, visibility into exposed surfaces (which includes domain names and DNS), and the capability to analyze threat vectors targeting a company's online presence.

Get our domain security recommendations to safeguard your domains and brands from cyber threats and fraud.

CSC is the trusted security and threat intelligence provider of choice for the Forbes Global 2000 and the 100 Best Global Brands® in enterprise domain names, domain name system (DNS), digital certificate management, as well as digital brand and fraud protection. As global companies make significant investments in their security posture, CSC can help them understand known cybersecurity oversights that exist, and help them secure their online digital assets and brands. By leveraging CSC's proprietary technology, companies can solidify their security posture to protect against cyber threat vectors targeting their online assets and brand reputation, helping them avoid devastating revenue loss, and significant financial penalties because of policies like the General Data Protection Regulation (GDPR). CSC also provides online brand protection—the combination of online brand monitoring and enforcement activities—taking a holistic approach to digital asset protection, along with fraud protection services to combat phishing. Headquartered in Wilmington, Delaware, USA, since 1899, CSC has offices throughout the United States, Canada, Europe, and the Asia-Pacific region. CSC is a global company capable of doing business wherever our clients are—and we accomplish that by employing experts in every business we serve. Visit cscdbs.com.

RESEARCH PREPARED BY CSC:

IHAB SHRAIM	Chief technology officer
VINCENT D'ANGELO	Global director, Strategic Alliances and Partnerships
ELLIOTT CHAMPION	Product director, Global Brand and Domain Security
QUINN TAGGART	Senior advisor, Global Brand Security
FERNANDO CEVALLOS	Product director, Global Anti-Fraud and Threat Intelligence

DBS11022022