Constella

Executive Blindspot: Why Monitoring The Dark Web Matters

How Executives Are Dealing With Cybercrime in The New Post-Covid-19 Digital Era

2022 | Survey Report

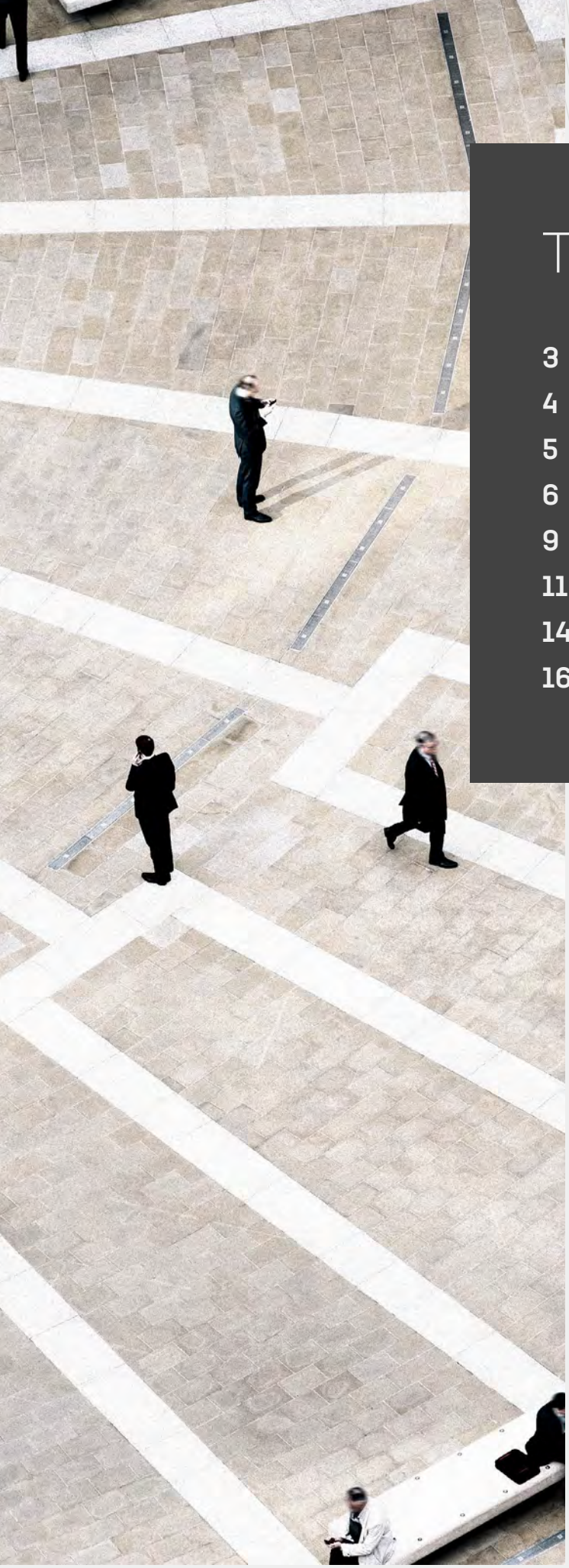


Table of Contents

About This Report

Constella Intelligence and Pulse surveyed 100 global technology executives across all major industries – including financial services, technology, healthcare, retail, and telecommunications – across North America, Europe, the Middle East, and Africa.

Survey participants serve in senior leadership roles, specifically Vice Presidents and C-Suite level executives within their respective organizations. Their answers reflect an increased awareness of the rise in cyberattacks, mainly due to the move to a remote workforce resulting from the Covid-19 pandemic and the severe risks associated with exposed personally identifiable information (PII), accounts, or financial information of organizations.

"Executive Blindspot: Why Monitoring The Dark Web Matters" survey report seeks to understand and address the significance of cyberattacks for executive leadership and other key employees, the impact of cybercrime, and what measures leaders are taking to deal with these risks.

Executive Summary

According to Atlas VPN, nearly six billion online accounts were exposed on dark web hacker marketplaces like RaidForum in 2021, and **compromised credentials were the most common initial attack vector** in data breaches. This alarming statistic underscores the prevalence of cyberattacks like ransomware on executive leadership and other key employees. While most executives surveyed are concerned with providing monitoring tools and employee training, only some are actively looking for breached credentials.

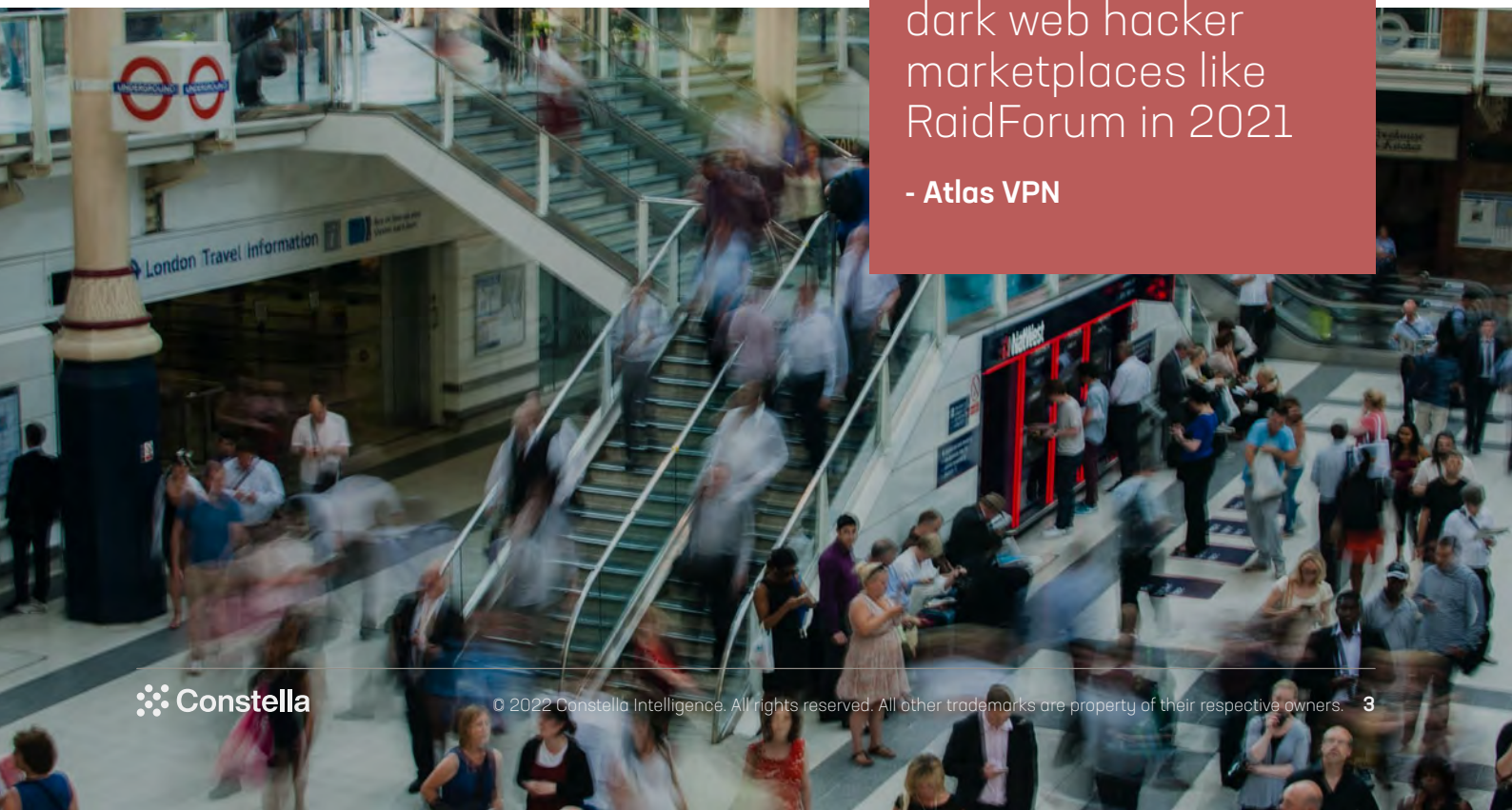
Pre-pandemic results showed an increase in cyberattacks globally. These attacks grew exponentially with the shift to remote working environments resulting from the COVID-19 pandemic. And because of their public profile and leadership roles, executives are targeted by threat actors more frequently. Cybercriminals use multiple avenues to gain access to credentials, including phishing, malware, and brute force attacks via trial-and-error attempts to 'force' their way into private account(s). They also have access to billions of email and password combinations on the dark web.

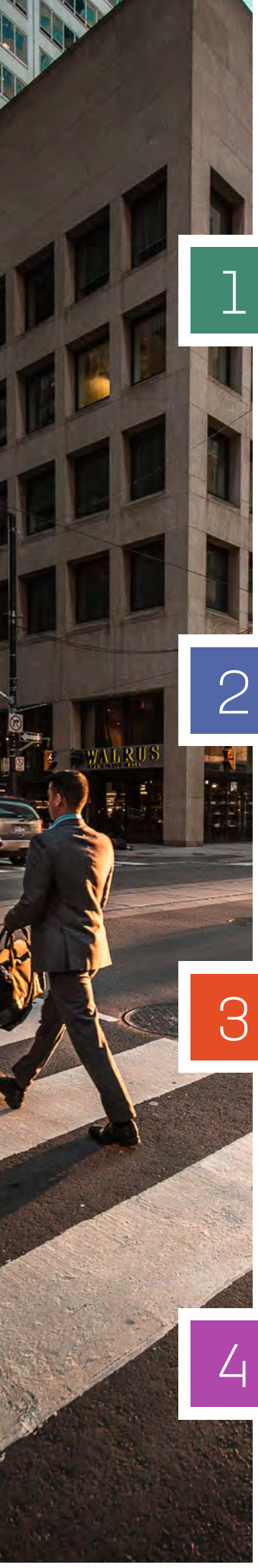
The available PII in dark marketplaces correlates to the value associated with each sector. Financial, healthcare, and retail institutions continue to be the most targeted sectors due to the personal information these institutions hold. In many cases, executive credentials get leaked, but organizations are unaware that their corporate information is being sold on the dark web until it's too late. Prevention is the best medicine, yet only some organizations actively monitor the dark web for breached credentials.

Most organizations, nonetheless, are concerned with instituting layered security protocols, including security information and event management solutions, improved processes and procedures, VPNs, and various multifactor authentication methods. Executives also continue to lead the fight by providing multiple forms of cybersecurity awareness training. But the cost of a single breach can be severe, especially for smaller organizations. With average costs reaching millions of dollars, the loss of customers and the resulting revenue drop can financially sink companies.

The following key findings and insights show that executive and employee credentials are vulnerable in a remote working environment. Concerned executives feel they have the right tools, processes, and training programs to ensure their employees are aware and prepared.

> Nearly six billion online accounts were exposed on dark web hacker marketplaces like RaidForum in 2021
>
> **- Atlas VPN**





KEY FINDINGS 2022

1

Remote work has led to increased attack surfaces and an uptick in the vulnerability of executives to cyberattacks

When the "bring your own device" (BYOD) surge began over ten years ago, most organizations struggled with the risk exposure BYOD brought to their digital ecosystems. And the increasing commonality of a remote work environment due to the pandemic has allowed for new cyber threats that target unprotected network perimeters and exposed assets. Our survey shows that executives are seriously concerned. One hundred percent (100%) of the executives in our survey, to some extent, feel that their organizations face increased cybersecurity risks due to remote work. Almost three-quarters (73%) of the respondents agree that executives and privileged IT personnel at their organizations are more vulnerable to cyberattacks when working remotely.

2

Most respondents' employees have had their credentials exposed by threat actors - yet few are actively monitoring for breached credentials

The key to the cybercriminal revenue model is quickly offloading their loot. Before organizations are even aware, they've sold their corporate credentials and other PII on the dark web multiple times, enabling bad actors to profit many times over. Our survey reveals that more than half (56%) of executives admit that, to their knowledge, the credentials of key employees have been exposed by cybercriminals at least twice in the past two years. And twice as many executives in smaller organizations have been exposed more than four times. However, almost half (46%) of executives say that their organizations don't monitor key employee exposed credentials on the dark or surface web or are unsure.

3

Most executives are concerned about employee-centric threats, while few are monitoring the dark web to mitigate risk

Staying ahead of cybercriminals means focusing on managing, securing, and monitoring credentials and ensuring access to credible and actionable intelligence. Our survey indicates that when considering threats to sensitive and confidential information, executives are most concerned with employee negligence (73%), employee-owned mobile devices or BYOD (71%), and use of public cloud services or networks (50%). Their organizations are focusing on security monitoring and authentication (82%) and cybersecurity awareness training (55%) to protect employees with access to sensitive information, like executives and privileged IT personnel, against cyberattacks.

4

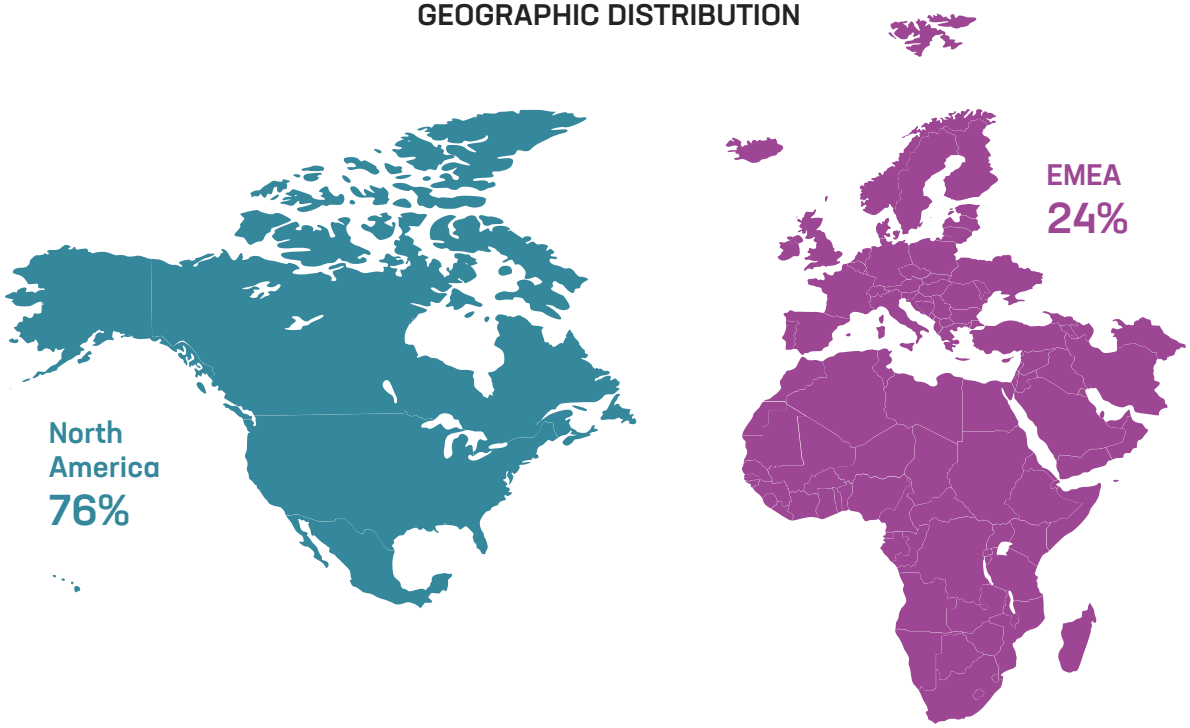
Data breaches can have a significant financial impact on enterprise organizations

If you are in any of the prominent sectors prone to cyberattacks (including but not limited to energy, financial, healthcare, telecom, retail, or transportation), a breach can inflict damage to your bottom line. Our survey results show that more than half (53%) of the executives surveyed estimate it costs their organizations between $100,000 and $1,000,0000 when a data breach occurs. The impact of cybercrime can cause severe financial damage to organizations of all sizes.

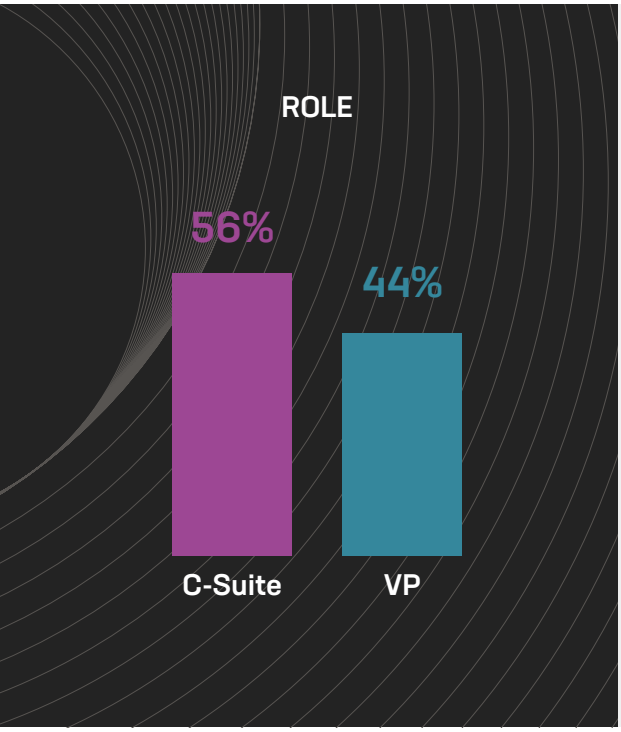
Methodology & Demographics

Constella Intelligence and Pulse conducted a joint survey of 100 global technology executives across fifteen significant industries throughout North America and Europe. Respondents are Vice Presidents and C-Suite level executives in organizations ranging from 5,000 to 10,000+ employees.

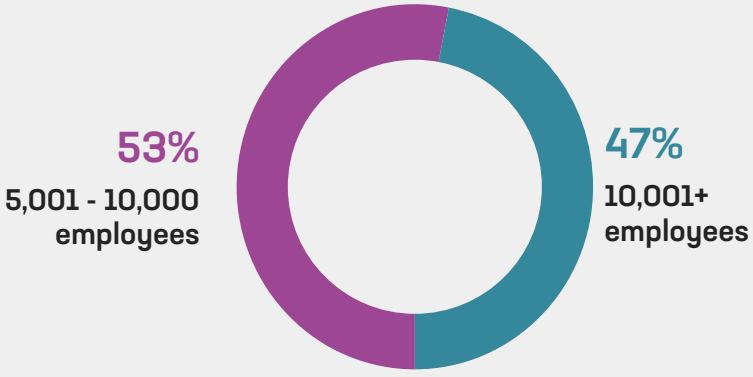
GEOGRAPHIC DISTRIBUTION



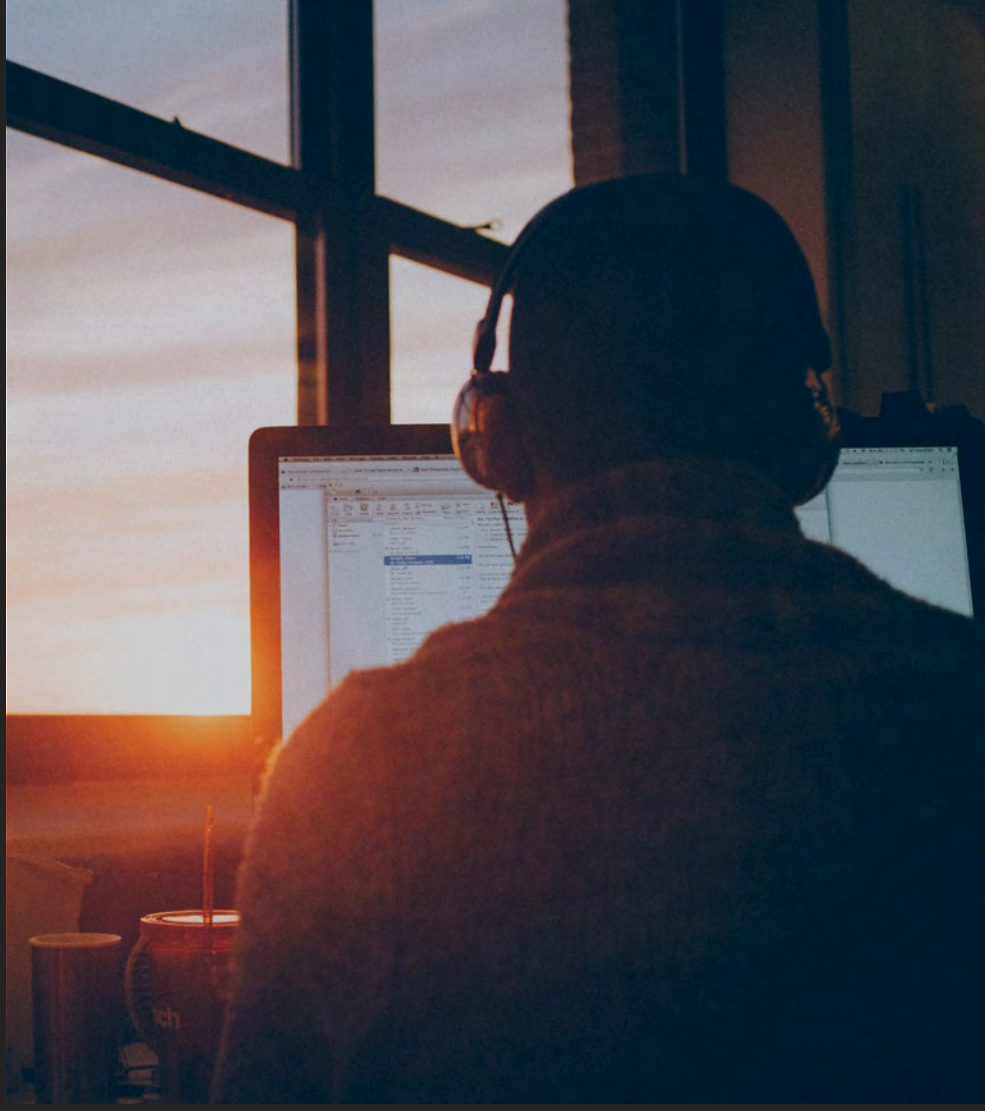
ROLE



COMPANY SIZE



Key Finding 1



Remote work has led to increased attack surfaces and an uptick in executive vulnerability

Cybercriminals exposed an estimated six billion online accounts in 2021 and credentials top the list of most compromised data. Alarming as they are, these statistics underscore the prevalence of cyberattacks like ransomware on executive leadership and other key employees.

Our survey findings confirm that almost half (49%) of respondents say their organization has been targeted in a phishing scam impersonating their CEO in the past 18 months, with more than a quarter (28%) saying they are unsure.

Healthcare executives appear to be concerned with cyber risks, especially remote working. Among healthcare executives, a majority (80.6%) were moderately concerned with these rising risks. Almost twice as many smaller organizations (5000 - 10,000 employees) in the healthcare industry were unsure about cyberattacks targeting CEOs at their organizations in the past 18 months.

ANALYST INSIGHT

In addition to credentials, cybercriminals target personally identifiable data (PII). This kind of information is then sold on the dark web or used in other types of fraud. Most North American executives (60.5%) were more likely to be moderately concerned than executives from other parts of the world.

Seventy-three percent (73%) of executives who feel their organization faces increased cybersecurity risks due to remote work also agree that executives and privileged IT personnel are more vulnerable to cyberattacks when working remotely.

Less than one-fifth (16%) of these same respondents are unsure whether executives and privileged IT personnel at their organizations are more vulnerable to cyberattacks when working remotely. PII data raises the digital risk profile of organizations, attracts threat actors, and fuels cyberattacks. These threat actors use people as their primary attack vector.

Do you feel that your organization faces increased cybersecurity risks due to remote work?

- 55% Moderately
- 41% Slightly
- 4% Significantly

100% of executives, to some extent, feel that their organization faces increased cybersecurity risks due to remote work.

Has your organization been targeted in a phishing scam impersonating your CEO in the past 18 months?

- 49% Yes
- 28% Unsure
- 23% No

Almost half (49%) of executives say that their organization has been targeted in a phishing scam impersonating their CEO in the past 18 months.

Key Finding 2

Most respondents have had their executive credentials exposed by bad actors - and only some are actively looking for breached credentials.

Executive credentials are desirable to cybercriminals. In fact, their credentials are ten times more likely to be targeted. Executives have privileged access to valuable information and computer systems that can lead to old files and records, a treasure trove for any bad actor. And because they are constantly on the move, they become easy targets for dedicated social engineering attacks such as spear-phishing, vishing, and others.

Our survey confirms that almost a third (32%) of executives say it was due to CEO impersonations for those who had exposed credentials.

But executive credentials are not the only credentials that concern executives. IBM research found that compromised credentials were the most common initial attack vector in data breaches in 2020. Compromised employee credentials have been the source of some of the highest-profile attacks in the last few years. Among these attacks were the Colonial Pipeline (US) ransomware, British Airways' (UK) £20m GDPR fine, and Swisscom (CH) exposing PII data of almost 10% of the country's population.

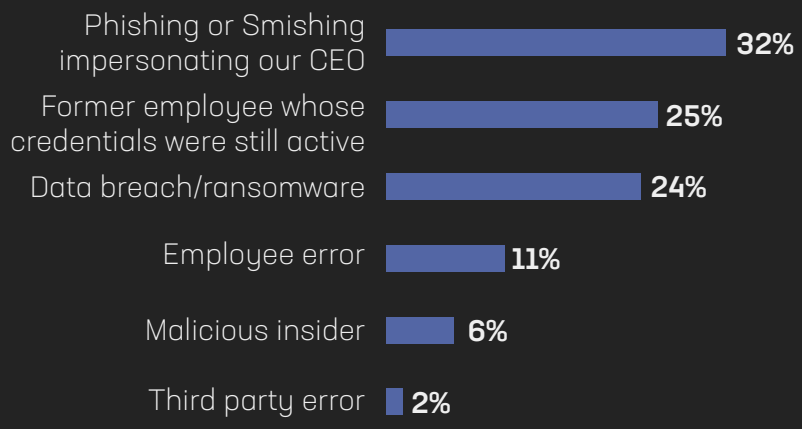
Our survey findings confirm that more than half (56%) of the executives interviewed say the credentials of key employees have been exposed by cybercriminals at least two times over the past two years. Furthermore, healthcare executives were more likely to indicate exposures from "a former employee whose credentials were still active."

ANALYST INSIGHT

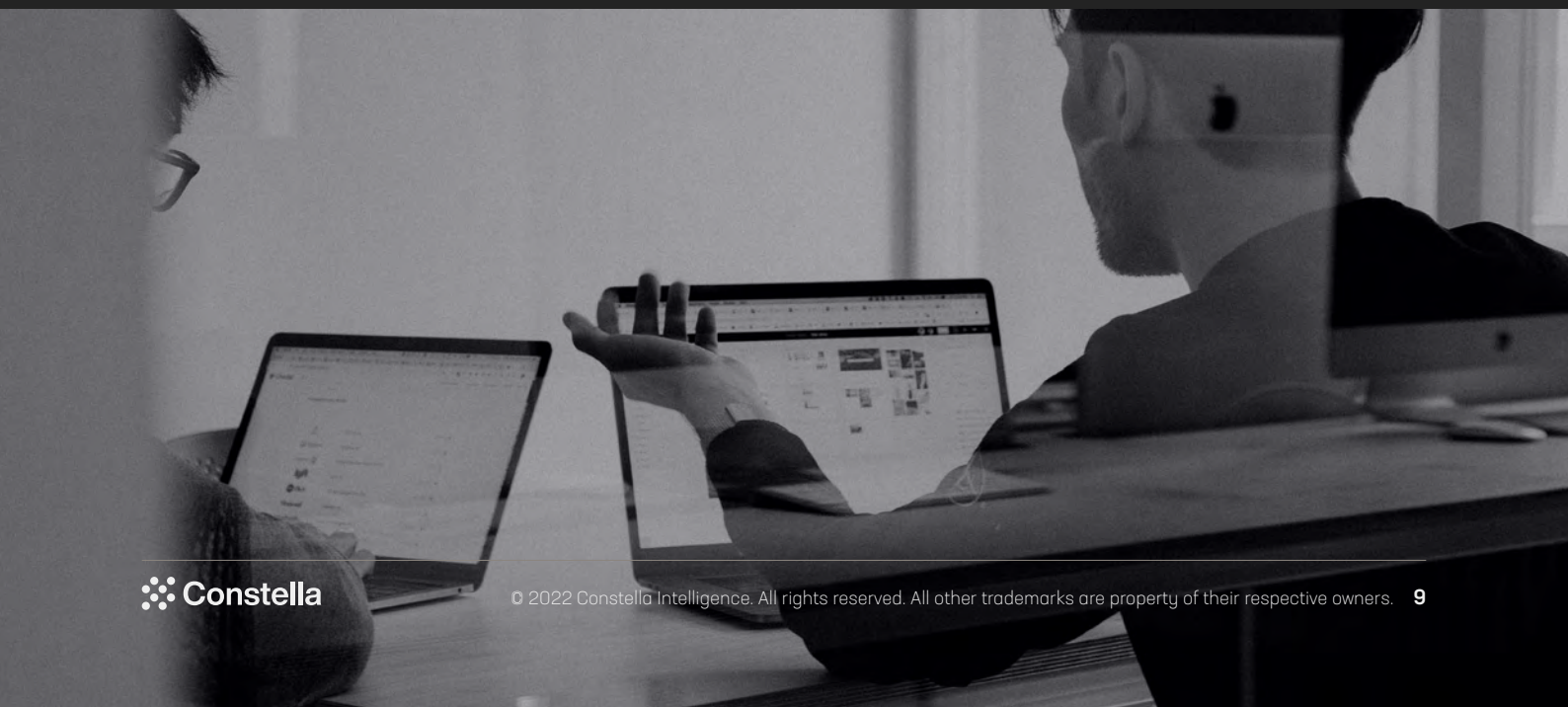
Our survey showed that more than half (54%) of executives use some combination of people, technology, and service providers to prevent breached credentials. Of those who said no (30%), nearly two-thirds (62.5%) said they had sufficient technologies. More than two-thirds (70.6%) of healthcare executives were unsure.

But no organization is immune. The dark web, a hidden network of websites requiring a particular web browser to access, is awash with exposed credentials – social security numbers, email addresses, passport numbers, and more – ready for sale many times over. In today's digital ecosystem, dark web monitoring – continuously searching for and keeping track of personal information circulating on the dark web – is a must for any organization looking to thwart criminals seeking to steal executive corporate identities.

What is the root cause of the exposed credentials in your organization?



For those who had exposed credentials, executives say it was due to CEO impersonations (32%), former employees whose credentials were still active (25%), and a data breach or ransomware (24%).



Key Finding 3

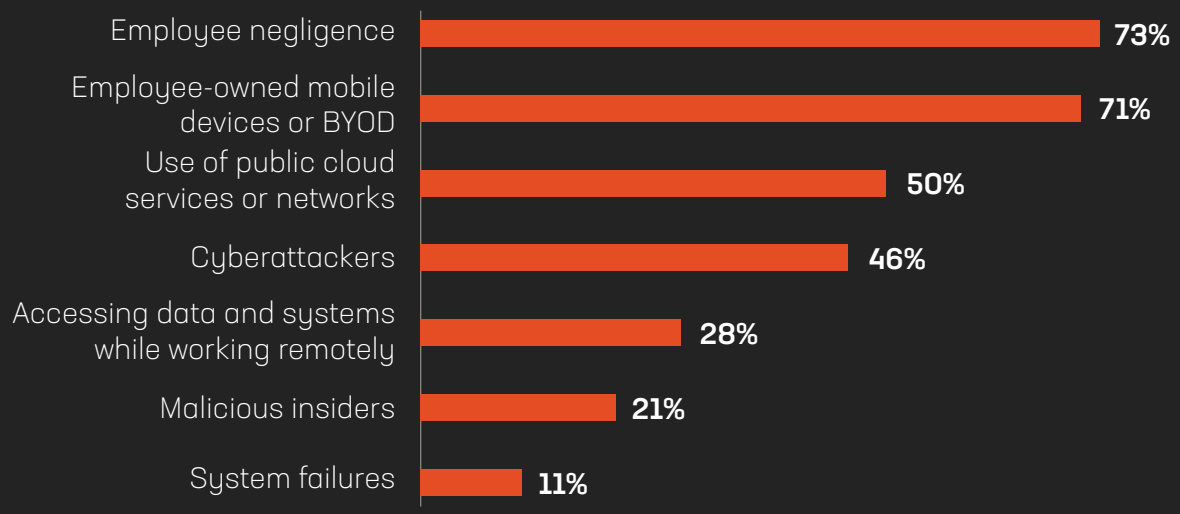
Most executives are concerned about employee-centric threats, while few are monitoring the dark web to mitigate risk

Compromised credentials can lead to significant financial loss and a tarnished brand reputation. It can bankrupt organizations, as in the case of Finland's largest psychotherapy center, Vastaamo Psychotherapy Centre.

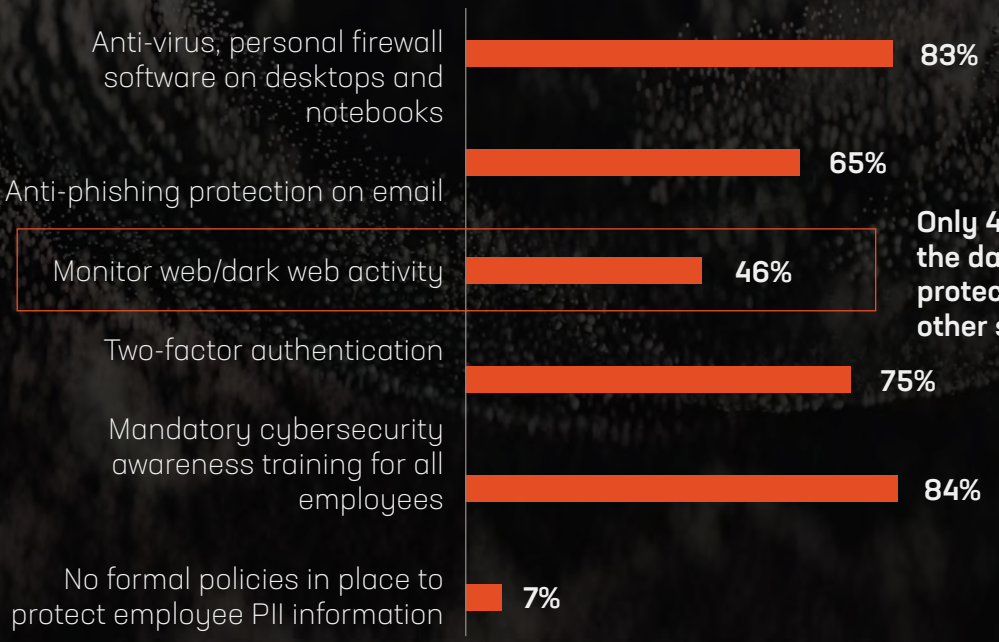
In response, executives in our survey are using several measures to combat employee-centric threats that compromise PII and other sensitive data. Their organizations employ several methods, including anti-virus and personal firewall software on desktops and notebooks (83%), two-factor authentication (75%), and anti-phishing protection on email (65%).

And the landscape has become more treacherous. As we pointed out earlier, the dark web has become the marketplace for exposed corporate credentials and other PII. But less than half (46%) of the executives in our survey monitor the dark web. And less than one-twentieth (4%) have this as a top priority. The consequences of this inattention are costly.

What threats to sensitive & confidential information within your organization are you most concerned about?

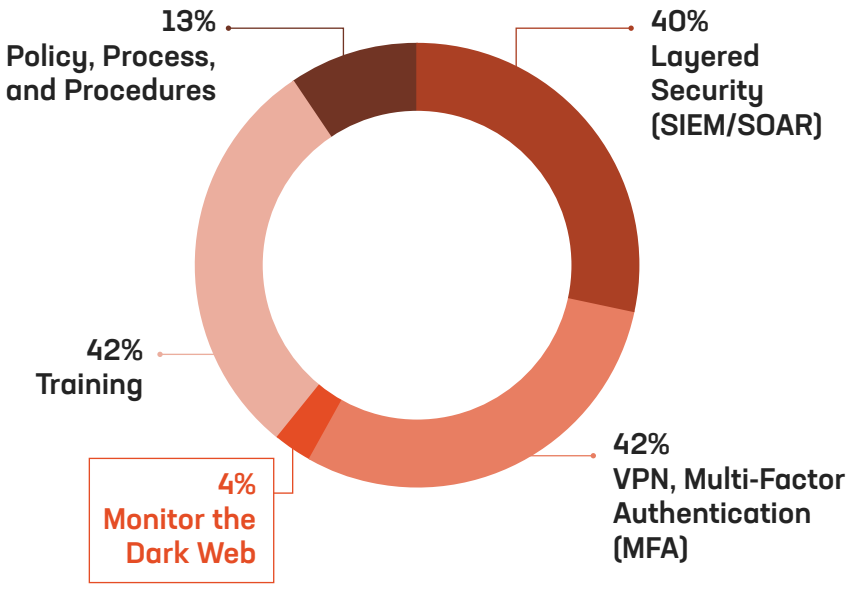


What is your organization doing to reduce the likelihood of having an employee's PII and other sensitive data compromised?



Only 46% of companies monitor the dark or surface web to protect their employee's PII and other sensitive data.

How does your organization protect employees with access to sensitive information, like executives and privileged IT personnel, against cyberattacks that target their credentials and personally identifiable information (PII)?



Only 4% of executives said their organizations leverage dark web monitoring to anticipate against threats to employees with access to privileged information. Targeted attacks towards key employees put employee credentials and PII at risk along with the security posture of the entire organization.

Key Finding 4

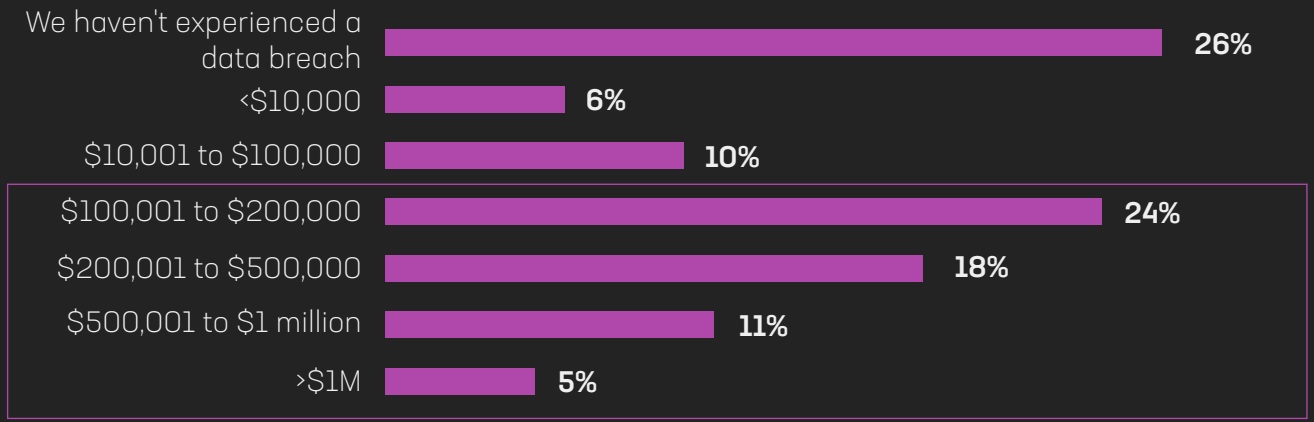
Data breaches can have a significant financial impact on enterprise organizations.

More than half (53%) of the respondents in our survey experienced a data breach of $100,000 to $1,000,000. And almost three times as many larger organizations (greater than 10,000 employees) have data breaches costing one-half million or more dollars ($500,000). Within our survey, healthcare executives appear to be the most concerned. And they should be, as most healthcare breaches (87%) are less than $500,000.

Statistically, no organization is immune to cyberattacks. The way to protect can take several forms, including:

- Investing in security orchestration, automation, and response (SOAR) to help improve detection and response times.
- Adopting a zero-trust security model to help prevent unauthorized access to sensitive data.
- Using tools that help protect and monitor endpoints and remote employees

What is the estimated financial impact on your organization when a data breach occurs?



53% of respondents estimate it costs their organization between $100K and $1 million when a data breach occurs.

Conclusion

Cyberattacks continue to rise at an alarming rate as attack surfaces have expanded during the pandemic, driven by preexisting trends of accelerating digital transformation and widespread transitions to distributed, virtual work models. Despite the benefits of efficiency and flexibility offered by hybrid-remote work, executives consider this trend to present additional vulnerabilities in their security perimeters. With more than half of executives reporting being targeted or exposed in the past 24 months, the likelihood of an attack targeting and exposing the personal credentials of executives or key employees is inevitable, even if some organizations have not yet experienced it.

The proliferation of employee-owned mobile devices or BYOD, the use of the public cloud services and networks, and employee error or negligence continue to fuel cyberattacks. As organizational perimeters expand individual and corporate attack vectors threats have become more prevalent. Therefore, organizations need to strengthen the protections around threats to sensitive information.

KEY RECOMMENDATIONS

1

Security teams must prioritize continuous actionable, contextual threat intelligence from the dark web. SOAR processes will help executives stay ahead of the constantly changing threat landscape and get in front of the ever-expanding attack surface and vanishing network perimeter. There is tremendous complexity in most organizations' security ecosystems, including the infrastructure, the massive amounts of data, and the resulting alert fatigue of many security teams. With immense volumes of corporate credentials finding their way to the dark web unbeknownst to organizations, averting catastrophe means extending SOAR to the dark web to identify and respond to digital threats targeting executives and employees.

2

Systems are only as robust as the humans who operate them, so preventing employee error or negligence is crucial in the defense against cyberattacks. While employee cybersecurity awareness training is essential, it must also be ongoing and continuously refreshed to be effective. This training must also extend to contractors, vendors, and in many instances, customers. Protecting employees and reducing the opportunity for data leaks should also include:

- Monitoring activity of domains and credentials within the corporate network, including phishing test tools to determine which individuals need additional training,
- Implementing periodic password changing policies (at least quarterly) and ensuring strong password usage through strict protocols.
- Updating workplace policies, e.g., a clean desk rule and securing physical access to information
- Performing regular in-house audits of the PII, sensitive and protected data stored and managed by your organization
- Implementing detailed privilege control and data access authorizations

Employee credentials are constantly sold on the dark web by threat actors looking to profit from compromising and breaching your organization. Constella's Dome platform enables comprehensive, real-time proactive risk intelligence by monitoring the surface, social, deep and dark web for your employees' and executives' exposed personal data, ensuring that you are one step ahead of threat actors seeking to weaponize this identity data against your organization. These capabilities for rapid action are more important than ever, empowering immediate intelligence and remediation to minimize potential financial and brand or reputational damage resulting from the diverse consequences of exposed sensitive data.

About Constella Intelligence

Constella Intelligence is a global leader in Digital Risk Protection that works in partnership with some of the world's largest organizations to safeguard what matters most and defeat digital risk. Our solutions are a unique combination of proprietary data, technology, and human expertise to anticipate, identify, and remediate targeted threats to your executives, your brand, and your assets at scale—powered by the most extensive breach and social data collection from the surface, deep and dark web on the planet, with over 100B attributes and 45 billion curated identity records spanning 125 countries and 53 languages.

To learn more about how you can proactively anticipate, identify, and remediate targeted threats to your executives, your assets and your brand visit us at **constellaintelligence.com**

Why Constella

OUR TEAM

We're a diverse multinational team committed to becoming the most trusted global partner for defeating digital risk. Constella integrates interdisciplinary intelligence community analysts, infosec pioneers, military veterans, and tech entrepreneurs with advanced analysis of surface, deep, and dark web to protect what matters most.

OUR INSIGHTS

Our diverse team of expert multidisciplinary cyber intelligence analysts delivers real-time, actionable insights to identify threats and reduce risks emerging from the surface, deep, and dark web.

OUR DIFFERENCE

Our unique technology empowers advanced analysis across the entire risk surface for superior anticipation, protecting organizations, their individuals, and their critical assets. Because, the best way to overcome future threats is by facing them today.