Recorded Future®

It’s Time to Take a New Approach to Identity Fraud Protection

As a business operating in the digital world, you have to be fast, innovative, and agile to maintain a competitive edge. Unfortunately, today's cybercriminals are demonstrating those very same strengths – constantly evolving their capabilities to breach your organization using the stolen credentials of your employees, partners and customers. With countless devices all connected to each other without clear perimeters, verifying user identities and controlling access to sensitive data are critical – but difficult to achieve.

Cybercriminals can easily purchase leaked credentials from paste sites and dark web channels to breach an organization and gain access to corporate systems and sensitive data. Unable to monitor the dark web for this information on their own, organizations can't take proactive measures, which leaves their business vulnerable to financial, legal, and reputational damage.

Businesses need to fight back and protect themselves by shining a light onto this activity to expand their visibility. Proactive, intelligence-led identity fraud detection gives businesses this power, enabling them to proactively defend against identity fraud, monitor for compromises in real time, and take action before damage to the business is done.

Strong digital identity authentication is more important than ever before

Organizations face an expanding threat landscape and unprecedented level of attacks. Today's cybercriminals don't discriminate – businesses of any size in any industry are at risk. In fact, 79% of organizations experienced an identity-related breach within the past two years alone.[1] And 85% of cybercriminals were able to access critical systems and data using stolen credentials. How and why is this happening?[2]

Security practices are outdated

Rapid adoption of cloud, Software as a Service (SasS), mobile, the internet of things (IoT), and more has fundamentally changed the way we do business. In today's on-demand, digital world, business no longer takes place within the confines of a physical office. Business is taking place whenever, wherever and however users choose. While most organizations have embraced these new ways of working, the same cannot be said for the way they manage their security practices.

Traditional security strategies focused on securing the perimeter, acting as a moat to protect a company's critical infrastructure and assets. But the attack surface of a business is no longer limited to on-premises networks or known devices. The old security model doesn't scale to support the distributed and often cloud-based applications that are used within businesses today.

---

[1] https://www.idsalliance.org/2021-trends-in-securing-digital-identities-2/

[2] https://www.prnewswire.com/news-releases/more-than-half-of-us-companies-hit-with-privileged-credential-theft-insider-threats-in-last-year-301294644.html

Ecosystems have become more dynamic and complex

Organizations are now working within a dynamic ecosystem of employees, partners, and customers. Everyone operating within this ecosystem is a target for cybercriminals looking to steal credentials so they can access privileged accounts and initiate fraudulent activities.

Today, 61% of all breaches involve credentials,[3] now the fastest kind of data to be compromised.[4] Nevertheless, customers and partners expect your organization to protect their identities and detect fraudulent activities – even if they fail to follow proper procedures and best practices.

It's reported that 52% of people still reuse passwords for multiple accounts[5], and almost half (47%) of consumers rely on a password that hasn't been changed for five years.[6] Without proper monitoring and management of these foundational security hygiene practices, and as threat actors become increasingly sophisticated, organizations face a higher level of risk for account takeovers and identity fraud activities.

Remote users are interacting across multiple channels

Over the past two years, most businesses had to accelerate their digital transformation journey to adapt to the challenges of the COVID-19 quarantines and to support a mostly-remote workforce. More users needed remote and mobile access to corporate systems, applications and platforms, which meant the creation of more credentials. 83% of system access stakeholders report that remote work due to COVID-19 increased the number of identities.[7]

Intent on adapting and keeping their business going, many organizations failed to update their security practices – some just didn't have the time or resources. Cybercriminals took full advantage of this opportunity, triggering a 300% spike in reported cybercrimes by the FBI since the onset of the COVID-19 pandemic.[8] 23% of cybersecurity professionals agree that attacks on their organization have increased since transitioning to remote work, many reporting double the number of incidents.

61%

of all breaches involve credentials

52%

of people still reuse passwords for multiple accounts

47%

of consumers rely on a password that hasn't been changed for five years

---

[3] https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

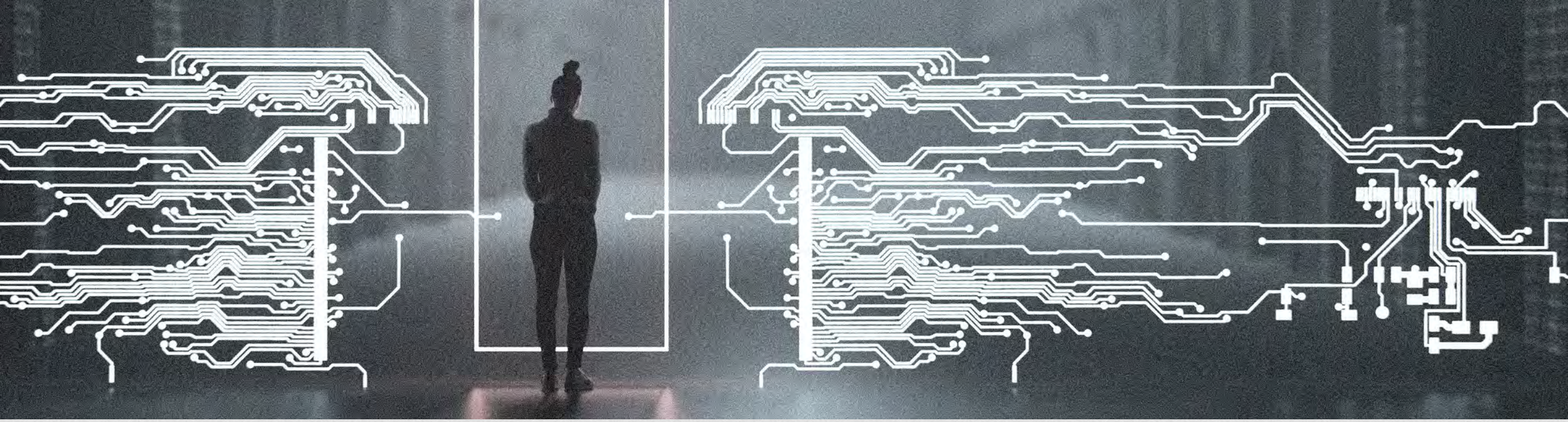
[4] https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

[5] https://datadome.co/resources/account-takeover/

[6] https://www.telesign.com/resource/telesign-consumer-account-security-report

[7] https://www.idsalliance.org/2021-trends-in-securing-digital-identities-2/

[8] https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic



Security and IT teams are overwhelmed

Securing business and employee identities is critical, yet a 2021 survey of IT security and Identity professionals found that confidence in the ability to secure employee identities dropped from 49% to 32% in the past year.[10] With the rapid growth in remote work and spike in omnichannel digital interactions, these teams are facing intense pressure to secure their business and employee identities, knowing that the fallout from a security breach can result in massive fines, a damaged reputation, customer and partner attrition, and loss of revenue. How bad is bad? The average cost of a data breach per compromised record is $148.[11] And as a result of a data breach, 46% of organizations report suffering damage to their reputations and brand value.[12]

What's the best path forward?

Organizations must expand their security practices beyond the perimeter, to secure every authentication and action request that is being made – regardless of whether the user is on the corporate network or remote. You need a solution that can scale to support today's modern and distributed workforces and provide a more secure approach for accessing business-critical applications and infrastructure. Businesses are recognizing the importance of identity protection and the critical role it plays within an overall security strategy, with 80% of organizations increasing focus on identity security over the past year.[13]

---

[9] https://www.isc2.org/News-and-Events/Press-Room/Posts/2020/04/28/ISC2-Survey-Finds-Cybersecurity-Professionals-Being-Repurposed-During-COVID-19-Pandemic

[10] https://www.idsalliance.org/2021-trends-in-securing-digital-identities-2/

[11] https://www.ibm.com/security/data-breach?_ga=2.11454388.1642912493.1579284504-1077052864.1575472342

[12] https://www.forbes.com/forbesinsights/ibm_reputational_IT_risk/index.html

[13] https://www.idsalliance.org/2021-trends-in-securing-digital-identities-2/

Proactive, intelligence-led identity fraud detection is the answer

Data is a blessing and a curse for today's organizations. It's everywhere – it's easy to find, easy to collect, and easy to aggregate. But it can also be overwhelming and difficult to leverage. The business benefit comes when you learn how to turn data into something that's useful, trusted, and actionable.

Analysts can always get their hands on more data, but they need help spending less time collecting and processing data and more time identifying and responding to threats, conducting analysis, and sharing their findings. That's where Intelligence comes in. Intelligence is the key to unlocking the potential of security programs and protecting our organizations. The right intelligence, in the hands of the right people, at the right time, stops attackers in their tracks.

When trust is data-driven, Intelligence is essential

As a business, you need to secure and have trust in the authenticity of the individuals accessing every system and application – whether the user is on the corporate network or remote. A data-driven approach is essential because as you increase your reliance on a digital identity, you also need to increase the insights that you have into that identity and its true security posture. Without that trust, backed by data, you put yourself at risk.

Whether it's an employee or customer, Identity Intelligence becomes paramount to helping you really understand which users should gain access to what information. Actionable, contextual, external insights enable organizations to reduce risk of compromised identities by knowing what users and what information are compromised and from where – so that you can create security policies to protect your organization from any damage.

Identity Intelligence is essential for a holistic, proactive security program

Strong digital identity authentication is not about layering intelligence on to existing teams and processes. It's about integrating it into existing teams and processes to build holistic, proactive security programs that can support a dynamic ecosystem of employees, customers and partners while at the same time:

- Proactively defending against identity fraud
- Automatically detecting compromises in real time
- Taking action before damage to the business is done

How intelligence-led identity fraud detection works

Account Takeover prevention

There's no business as usual when you discover account takeover fraud. Armed with real-time evidence on identity theft, security and IT teams are able to quickly detect compromises and initiate downstream response workflows — such as requiring password resets more frequently, using stronger passwords, or using MFA for every login attempt.

Employee identity monitoring

Compromised data—including leaked and stolen credentials—is often not discovered until it is actively being used to attack an organization (including its brand, customers, and employees).

With Identity Intelligence, you can automate monitoring in real time across the broadest set of sources, including the dark web for mentions of credentials.

Third-party identity monitoring

Customers and partners expect the organization to protect their identities and detect fraudulent activities. Failure to do so will result in financial, legal, and reputational damage. With Identity Intelligence, you can automate monitoring and verification of customer and supply chain partner identities, proactively shining a light on fraudulent activities before damage occurs.

How Identity Intelligence protects organizations

Capability	Benefits
Automate collection, aggregation, and analysis of data across the broadest set of sites, including dark web, producing contextual identity insights in real time.	Reduce risk of damage to the business by immediately finding and remediating compromised identities before they're used in an attack against the organization. Save significant analyst time and improve accuracy by surfacing timely, relevant Identity Intelligence.
Automate monitoring and verification of employee, customer and partner identities in real time and integrate into existing identity tools and workflows.	Proactively defend against identity fraud by deploying protective solutions against known threats targeting your specific organization, customers, and third parties.

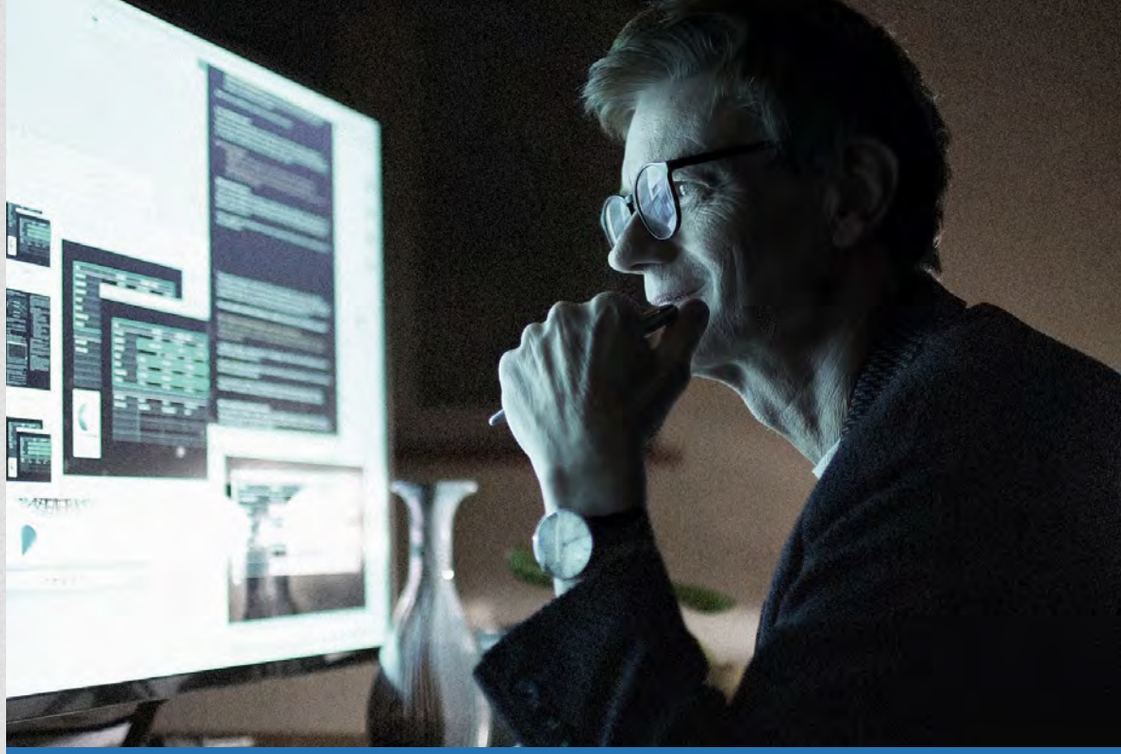
A new approach with Recorded Future

There are numerous pressures you face when managing users' identities within your organization from onboarding to protection, including provisioning of critical applications, data, and systems. Mitigating unauthorized access while managing the identities and access rights of people both inside and outside the organization is an enormous challenge in today's digital, on-demand world.

With Identity Intelligence from Recorded Future, security and IT teams can identify previously unknown credential leakages, for both employee and customer identities, and respond confidently — without any manual research. Recorded Future automates the collection, analysis, and production of intelligence from a vast range of open source, dark web, and technical sources, and then combines it with world-class research to help drive an accelerated response by your security team.

This approach produces real-time intelligence at massive scale, offering an unmatched source of truth for identity authenticity that can:

- Detect credential leaks in real time
- Respond to compromises before business impact
- Deliver unmatched visibility into closed and dark web sources
- Disrupt adversaries, while minimizing disruption to your business



"Recorded Future threat intelligence powers our Iron Core platform, providing critical awareness for us and our clients. The new Identity Module automates correlations and surfaces breach data that previously required significant processing to achieve. This real-time visibility into identity exposure enables us to better protect our clients and reduce risk."

- ERIC OOI, Director of Security and Research (Iron Vine Security, LLC)

358%

increase in malware, which is often used for identity theft, in 2020[14]

Summary

Cases of identity theft more than doubled in 2020, according to the Federal Trade Commission. And malware, which is often used for identity theft, increased 358% in 2020.[14] This is a trend that will likely persist into 2022 and beyond, as many employees are opting to continue working remotely once COVID-19 restrictions have been lifted.

While you can't prevent cybercriminals from trying to breach your organization with fraudulent credentials, you can control how you approach identity protection. With an intelligence-driven approach to identity fraud prevention, you can proactively defend your organization against identity compromises in real time and take action before damage to the business is done.

To learn more about Identity Intelligence from Recorded Future and how you can proactively defend your business against identity fraud, visit https://www.recordedfuture.com/solutions/identity-intelligence/

[14] https://www.helpnetsecurity.com/2021/02/17/malware-2020/

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.