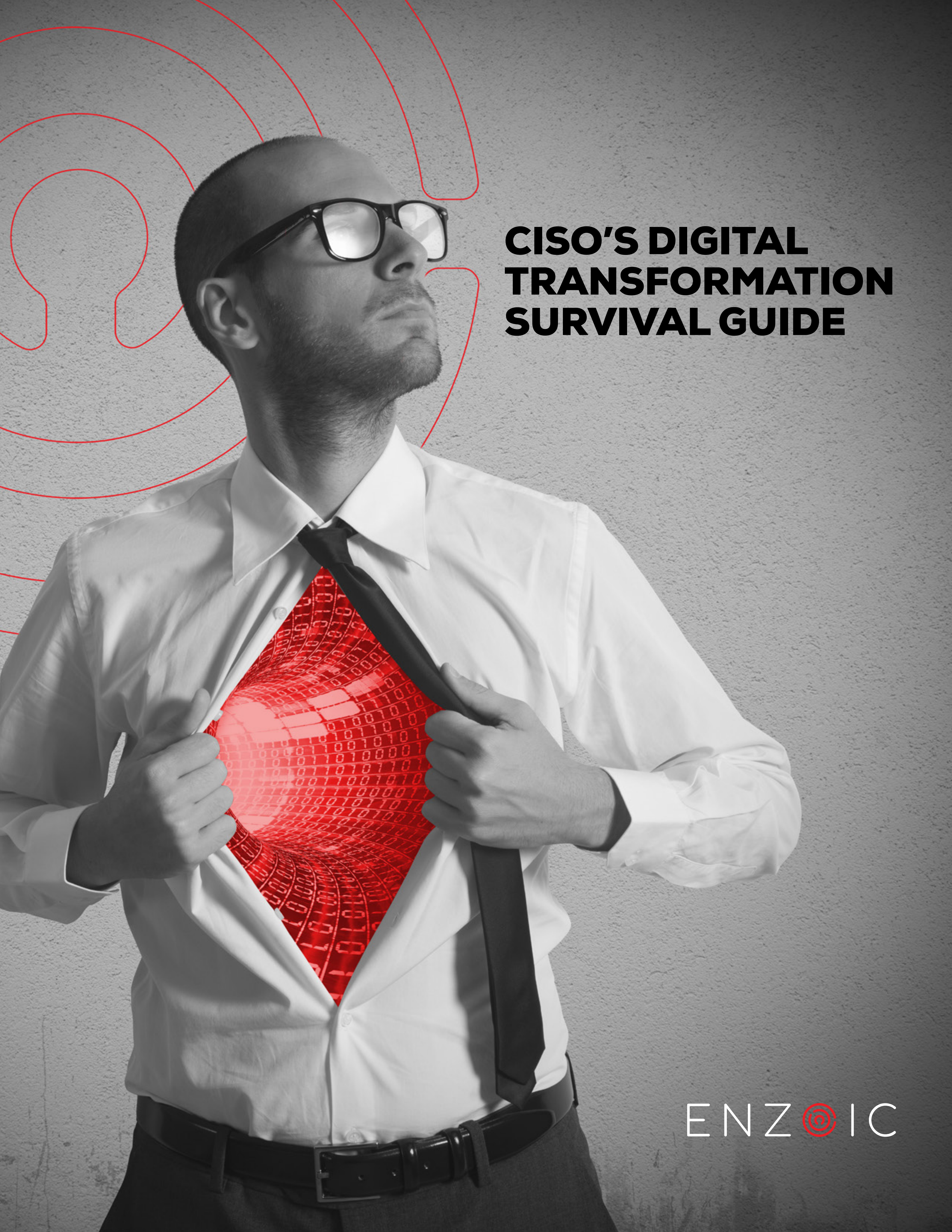


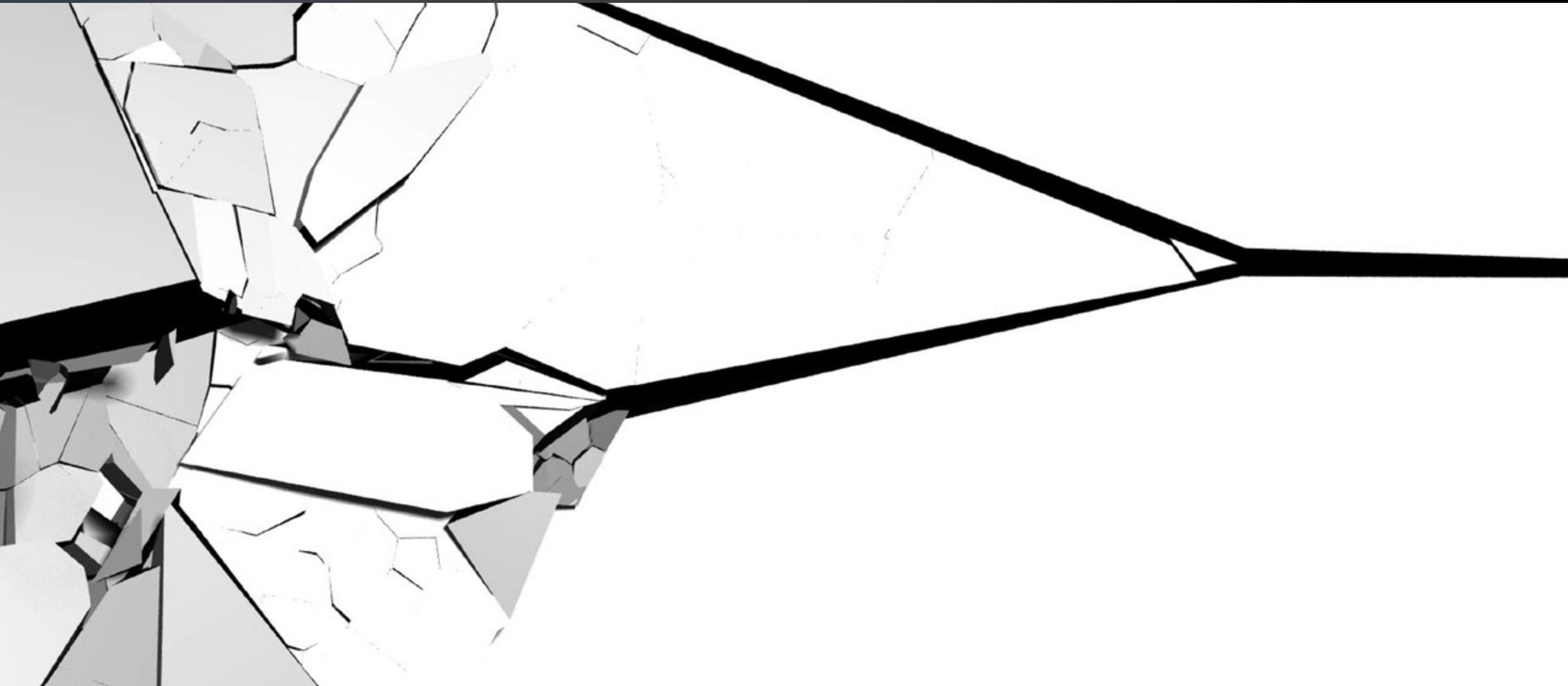
CISO'S DIGITAL TRANSFORMATION SURVIVAL GUIDE

ENZOIC

Digital transformation investments will reach

$7.4T

between 2020 and 2023.[1]



In today's digital era, business executives recognize that they must disrupt their markets or risk being disrupted themselves. Whether through development of creative new digital products, revamping of digitally enabled business models, automating back-end processes, or streamlining supply chains, forward-looking enterprises increasingly seek competitive differentiation through digital transformation.

The outcome of these initiatives will make or break the viability of future generations of businesses, even among the most traditional non-tech organizations. The trick will be maintaining a healthy balance between the upsides of digital transformation and the business and technology risks of accelerating tech-driven innovation.

Cybersecurity leaders can play a valuable role in this risk management balancing act. Security and data privacy concerns make up many of the most pressing risks associated with digital transformation. CISOs and other security executives who help their business stakeholders make better cyber risk decisions — without fighting the imperatives for digital transformation — stand to bring tremendous value to the table.

CEO Top Risks Today[2]

- Risk of Digital Disruption
- Succession and Talent Issues
- Regulatory Scrutiny
- Cyber Risks
- Organizational Resistance to Change

[1] www.businesswire.com/news/home/20191031005079/en/Direct-Digital-Transformation-Investment-Spending-Approach-7.4
[2] www.protiviti.com/sites/default/files/united_states/insights/nc-state-protiviti-survey-top-risks-2019-executive-summary.pdf

THE SECURITY TRUMP CARDS

Veteran security leaders understand implicitly that expanding one's digital footprint in the face of already intolerable cyberattack volumes poses big problems. Many organizations are already teetering on the edge with regard to cyber risks, and accelerated innovation without proper risk management could push some businesses right off a cliff. Particularly since the confluence of cyber risk and digital transformation is also overlaid by a tightening regulatory environment.

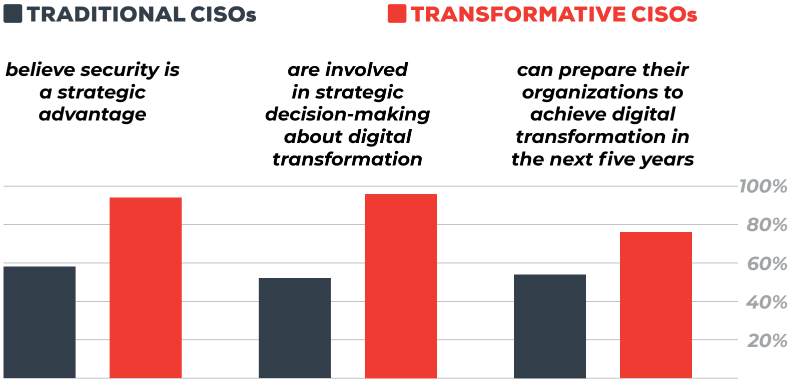
Auditors are turning the screws to organizations with regulations like CCPA and GDPR that have unprecedented enforcement 'teeth' that can take a difference-making bite out of the bottom line.

Clearly, security has to up its game. But it won't be allowed to do that simply by clamping down with draconian policies or security technologies that slow down innovation.

That's because as important as security is, there are bigger fish to fry from a business perspective. If business leaders can't keep the doors open because customers aren't happy or products aren't delivered quickly enough to beat the competition, then cyber risks are completely irrelevant.

This is why customer experience and time to market will always play the trump cards to security concerns for business stakeholders. According to recent studies, these are the biggest drivers of digital transformation today.

THE VALUE OF TRANSFORMATIVE CISOs[4]



WHAT'S MOST IMPORTANT FOR DIGITAL TRANSFORMATION[3]

#1 DRIVER (51%): Growth opportunities in new markets

#1 PRIORITY (57%): Delivering integrated, frictionless & omnichannel customer experience

8 in 10 *IT pros believe digital transformation increases cyber risk*

[3] www.briansolis.com/2019/01/the-2018-2019-state-of-digital-transformation/

[4] resources.titus.com/The_Role_of_Security_in_Digital_Transformation

ESTABLISHING A FRICTIONLESS MINDSET

Security leaders must be able to transform their security practices right in lockstep with all the other changes wrought by business-wide digital transformation.

The most significant shift for CISOs and other cyber leaders needs to occur in the security mindset they bring to their work. To survive and thrive during a digital transformation, security leaders need to act a lot less like cops and a lot more like risk concierges. The role of security professionals isn't to stop business stakeholders from incurring any cyber risks. Instead, security executives should be offering their expertise to inform and advise business counterparts about when and where the risks could manifest. This gives business leaders the knowledge they need to decide which digital risks are worth taking and which must be avoided.

Meantime, as security dispenses advice, it's also tasked with implementing technical controls and guardrails that protect digital platforms from attack and risk exposure. To add value to the digital transformation goals of the business, security's primary objective should be to minimize security friction wherever possible.

Security friction manifests itself in numerous ways.

At an **ORGANIZATIONAL PROCESS LEVEL,** security friction is introduced through impediments that slow down business growth or speed to market.

At a **USER LEVEL,** friction appears when security controls inconvenience users in minor and major ways.

At the **UNDER-THE-HOOD TECHNICAL LEVEL,** security friction shows up as slower transaction times, network speeds, or system reliability.

Whether it occurs organizationally or technologically, security friction that's introduced without enough business justification inevitably kills the credibility of the security department. Many of the cultural struggles that CISOs and security teams face tend to crop up when they roll out controls that pile friction onto processes the business depends upon to make money, to run the back office, to thrive.

That might mean controls that impede employees from getting work done most effectively, or it could be those that keep customers from spending money more prolifically. Ultimately, security friction is entirely at odds with the core drivers of digital transformation: improving customer experience and speed to market.

CLASSIC EXAMPLES OF SECURITY FRICTION IN ACTION

Key-Fob random number generators for consumer two-factor authentication

Vulnerability management tools that don't integrate into developer tools

Clunky antivirus suites that noticeably slow user endpoints

Restrictions on cloud services that prevent users from legitimately getting work done

CONSIDER 'LAUNCH-REVIEW-ADJUST'

One way for CISOs to stay flexible as things change rapidly over the course of a digital transformation could be to take what McKinsey calls a 'launch-review-adjust' mode to security strategy. Just as Agile development teams operate on sprint cycles, security can take a similar approach to modeling their threats and updating strategies:

In the spirit of agile development, cybersecurity teams may also want to take on these activities in 'launch- review-adjust' mode. They could update threat and risk profiles in one- to six-month sprints, thereby ensuring they are responsive to the latest trends and technologies.[5]

[5] *www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20 cybersecurity_March2019.ashx*

4 EXAMPLES OF REDUCING RISK WHILE MINIMIZING SECURITY FRICTION

Here are some examples of how organizations are effectively balancing

AUTHENTICATION

The most dangerous risks to consumers and businesses are triggered by credential stuffing attacks and account takeovers. Stolen usernames and passwords readily available on the black market fuel these attacks. While a lot of two-factor authentication (2FA) mechanisms effectively reduce the risk of account takeovers, the problem is that most of them add a tremendous amount of friction to very areas of online engagement that digital transformation wants to bolster.

Many organizations are recognizing that in the right situations, it makes more sense to cross-check that username credentials may have been compromised or reused on the black market than to introduce an unwieldy control to user account authentication.

PAYMENT PROCESSING

Online and mobile transactions are increasingly becoming the lifeblood of commerce for every type of organization, and digital transformation spurs this on further. While fraud protection is essential, transaction speed is tantamount.

The best security teams are managing that through behavioral indicators that bump up security measures based on risky behavior while generally keeping friction low for the average transaction.

Achieving frictionless security requires longtime security pros to bring to the table the flexibility to rethink old security paradigms without unnecessarily disrupting the flow of business. Sometimes this means making drastic changes to security models or technology to accommodate new innovations by the business. Other times it means finding creative controls that emphasize stability by making incremental changes to longstanding technological standards.

risk reduction to friction without losing their edge in innovation.

SOFTWARE SUPPLY CHAIN

Software development teams increasingly depend upon third-party code and open source libraries to quickly develop software. This practice underpins the DevOps and Agile practices that fuel the kind of swift software delivery necessary for digital transformation. But third-party code also accelerates the introduction of new vulnerabilities into enterprise software.

Rather than banning the use of the transformative practice of leaning on third-party code, successful security teams are finding ways to track and manage the use of these tools while making it easier for developers to source them. Security leaders reduce friction here by tailoring the security controls to the development process rather than making developers contort themselves to jump through security hoops.

DATA SHARING

Data sharing through cloud services, API connections between applications, and so on is crucial to digital transformation efforts. So many innovations today rest on complex digital ecosystems and integrations within and without the organization.

The most impactful frictionless security efforts are those that smooth ease of access and integration. At the business user level, that means allowing the use of common platforms such as Box, while increasingly tying data access policies and visibility into data use to identities and roles. At the application level, it means designing security mechanisms and APIs that work seamlessly in an ecosystem and help facilitate data controls. The security tools must work without breaking integrations or degrading service levels.

MAINTAINING CISO RELEVANCE THROUGHOUT DIGITAL TRANSFORMATION

In most instances, security friction increases or decreases proportionally with the severity of security restrictions put in place. Well-regarded, collaborative CISOs seek to find just the right balance of appropriate security controls so they can maximize protection and minimize security friction for any given situation. The balance depends on the business scenario at hand, with the calculus coming down to several key variables:

- **How much is at risk if no controls are in place?**
- **How could controls interrupt revenue streams?**
- **Could the aggravation of the control lose the company many customers?**
- **Must the business stop using or restrict innovative businesses processes or technology for the controls to work?**
- **Will the level of friction from controls cause a revolt among users that could scuttle implementation or induce unsafe workarounds?**
- **How much will controls slow down technology delivery or innovation?**
- **Are there any other alternative controls that could offer much less friction without compromising all the risk reduction benefits?**

In this era of digital transformation, the best CISOs are the ones who can work with the business to consider all of the variables at play. Forward-looking security leaders remain flexible to the notion that it isn't their job to eliminate risk; it's to provide the most expedient choices to reduce risk in the context of the business operating environment. They know that security exists to serve the business, and not the other way around.

Ultimately it takes a risk-based approach that consistently views security reasoning through the lens of business profitability and viability.

ABOUT ENZOIC

The Enzoic suite of solutions can help CISOs take one of many steps toward frictionless security. Enzoic provides an added level of protection to passwords by screening them for the risk of compromise without adding friction to the login experience.

Enzoic threat researchers scour the public internet and the Dark Web to find information and technical clues about all of the compromised credential details circulating online today. Our researchers correlate details about how the credentials were exposed, add additional details about unsafe passwords currently used in cybercriminal password cracking dictionaries, and turn it all into valuable threat intelligence that then feeds into our credential screening solutions. These solutions can be seamlessly integrated into an enterprise tech stack through API Services, Active Directory Plug-in, or security threat feeds. It’s an effectively elegant way to reduce risk without getting in the way of innovation.

To learn more, visit www.enzoic.com

Contact Enzoic

info@cenzoic.com
www.enzoic.com
facebook.com/enzoic/
@EnzoicSecurity