

The Data Pillar Foundation OF ZERO TRUST

anacomp[®]
we make data visible

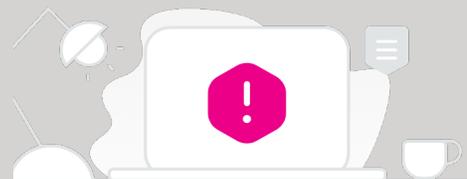


Identify and protect at-risk data that may be hidden, legacy, uncategorized, unstructured, or misfiled.

PEOPLE

HOW IS DATA AT RISK?

HUMANS + TECHNOLOGY
SUPPLY CHAIN + COMPLIANCE
INTELLECTUAL PROPERTY & PII THEFT



There were **5,200 data breaches** in 2021, an increase of **13%** according to Verizon's 2022 Data Breach Investigations Report.¹

80% of organizations experienced at least one breach during the last 12 months that they could attribute to a **lack of cybersecurity skills and/or awareness**, per Fortinet's 2022 Cybersecurity Skills Gap Global Research Report.²



64% of organizations in Fortinet's report² experienced breaches that **resulted in lost revenue and/or cost them fines**. Of those, 38% reported breaches that cost them over **\$1 million**

65%

The cybersecurity workforce needs to grow by **65%** to adequately protect enterprises' critical assets according to an analysis³ from (ISC)²

82% of breaches involved the **human element**. Whether it is the use of stolen credentials, phishing, misuse, or simply an error, the Verizon 2022 Data Breach Investigations Report found that people continue to play a very large role in incidents and breaches alike.¹



Even the C-Suite uses bad passwords. A Nordpass report found "12345" was the third most common password for CEOs and C-level executives and the fourth most common for business owners and managers.⁴

RESOURCES,
REFERENCES &
SOLUTION ON
PAGE 2

The development of quantum computing is putting the future of data encryption at risk⁵



Software supply chain cyberattacks hit three out of five companies in 2021⁶

18% of victims paid the ransom but still had their data exposed, and 35% of victims paid but were still unable to retrieve their data⁷

Chinese state actor APT 41 stole an estimated trillions in intellectual property theft from approximately 30 multinational companies⁸

insider threat

weak passwords

education

staffing shortage

legacy data

The Human Problem of Data Protection

phishing

user-friendliness

remote work

bias

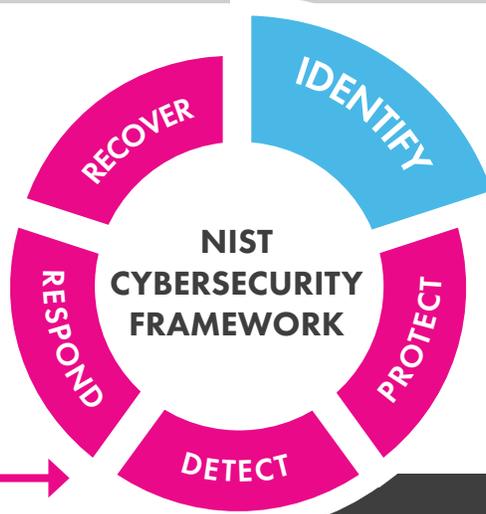
misconfiguration

It just takes one wrong click to poke a hole in the dam of security tools



“At the end of the day, our job is to get the user to the data that they deserve to have access to.”

Defense Information Systems Agency CTO discussing Zero Trust at GovCIO’s Cloud Modernization event, May 2022.⁹



The National Institute of Standards and Technology (NIST) **Cybersecurity Framework** and the Cybersecurity and Infrastructure Security Agency (CISA) **Zero Trust Maturity Model** include **identification, inventory, categorization and monitoring of critical data**

SOLUTION

IDENTIFY, INVENTORY & MONITOR ALL DATA AND INTELLECTUAL PROPERTY

Anacomp's D3 Data Discovery Solution uses AI/ML automation to crawl your entire data estate of unstructured and structured data to build an up-to-date “index of everything” with risk management filters and workflows, robust metadata, federated search, alerts, and content-level views. **Identify critical data and save IT resources and storage costs.**



Contact Anacomp
(703) 234-3910
sales@anacomp.com
www.anacomp.com

RESOURCES

- NIST Framework for Improving Critical Infrastructure Cybersecurity, April 2018
- NIST Special Publication 800-207, Zero Trust Architecture, Aug. 2020
- White House Executive Order, Improving the Nation’s Cybersecurity, May 12, 2021
- CISA Zero Trust Maturity Model, June 2021
- Office of Management & Budget, Memo on Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements, Dec. 6, 2021
- Department of Defense, Zero Trust Reference Architecture, Feb. 2022
- NIST NISTIR 8374, Ransomware Risk Management: A Cybersecurity Framework Profile, Feb. 2022
- BILL: Strengthening American Cybersecurity Act of 2022, Mar. 2022
- NIST Special Publication SP 800-161r1, Cybersecurity Supply Chain Risk, May 2022

REFERENCES

- 1 Verizon, 2022 Data Breach Investigations Report, www.verizon.com/dbir
- 2 Fortinet, 2022 Cybersecurity Skills Gap Global Research Report, www.fortinet.com/blog/industry-trends/global-cybersecurity-skills-gap-report-findings
- 3 (ISC)², 2021 Global Workforce Study, www.isc2.org/Research/Workforce-Study
- 4 Lance Whitney, “Even C-suite executives use terrible passwords like 123456,” TechRepublic, May 3, 2022, www.techrepublic.com/article/c-suite-executives-terrible-passwords
- 5 Tim Keary, “NATO and White House recognize post-quantum threats and prepare for Y2Q,” VentureBeat, Mar. 4, 2022, www.venturebeat.com/2022/03/04/nato-and-white-house-recognize-post-quantum-threats-and-prepare-for-y2q/amp/
- 6 John P. Mello, Jr., “Software supply chain attacks hit three out of five companies in 2021,” CSO, Feb. 14, 2022, www.csoonline.com/article/3650034/software-supply-chain-attacks-hit-three-out-of-five-companies-in-2021.html
- 7 Bill Toulas, “Ransomware extortion doesn’t stop after paying the ransom,” Bleeping Computer, Feb. 23, 2022, www.bleepingcomputer.com/news/security/ransomware-extortion-doesnt-stop-after-paying-the-ransom/
- 8 Nicole Sganga, “Chinese hackers took trillions in intellectual property from about 30 multinational companies,” CBS News, May 4, 2022, www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/
- 9 Katherine MacPhail, “Successful Cybersecurity Integrates Agile and Well-Trained Users,” GovernmentCIO Magazine, May 23, 2022, www.governmentciomedia.com/successful-cybersecurity-integrates-agile-and-well-trained-users