FORTRA

Why Zero Trust Needs Data Classification to Work

Zero Trust has been one of the cybersecurity industry's favorite buzzwords for a few years and for good reason; it's emerged as a legitimate strategy that—assuming the correct groundwork is laid—can help effectively guard against threats and strengthen an organization's security posture.

What is Zero Trust?

Zero Trust is rooted in the idea that everyone is a threat until proven otherwise. Only once a user's access level is verified, either via multi-factor or two factor authentication, can they be granted access. With zero trust, networks are segmented into groups that require their own access. This ensures that if an attacker were to infiltrate one network, they wouldn't be able to access them all.

Lost in the chatter around zero trust is how integral data classification is to the equation. For a zero trust framework to work correctly, it's critical that organizations know where their sensitive data is located, when it's created, how it's used, shared, and in particular, who's accessing it: that's where data classification comes into play.

Data visibility has long been a challenge for organizations.

64% of CISOs said data visibility is the biggest challenge facing organizations today.*

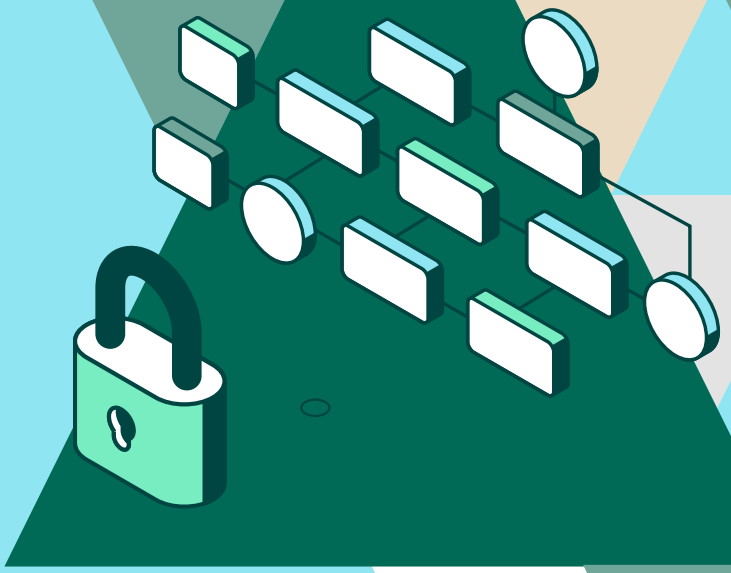
Not knowing where your data is can make it nearly impossible to protect it from loss and even harder to comply with privacy regulations such as HIPAA's Privacy Rule, PCI DSS, and the CPRA that mandate that data containing certain types of information be handled with specific safeguards.

With a data classification solution in place, organizations can determine where data resides in its ecosystem, apply sensitivity-based access control guardrails, then parcel out access determined on the data's sensitivity level.

(*https://www.fortra.com/resources/guides/data-security-survey-report)

According to Forrester, there are two foundational steps to achieving Zero Trust compliance:

1. Having a mature data identification and classification framework in place,
2. Having strong identity and access management.



Which Approach Is Right for Zero Trust?

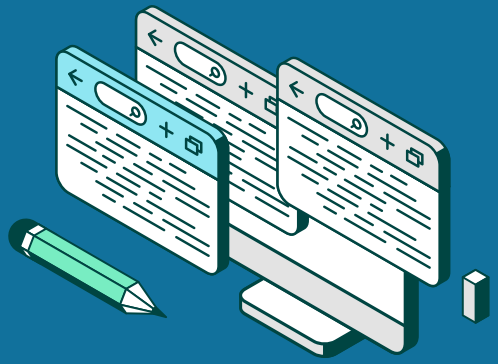
While there are three types of data classification that are viewed as industry standard, one is more helpful than the others when it comes to implementing a zero trust framework:

CONTENT-BASED CLASSIFICATION

Inspects and interprets files, looking for sensitive information.

CONTEXT-BASED CLASSIFICATION

Looks to the application, location, metadata, or creator (among other variables) as indirect indicators of sensitive information.

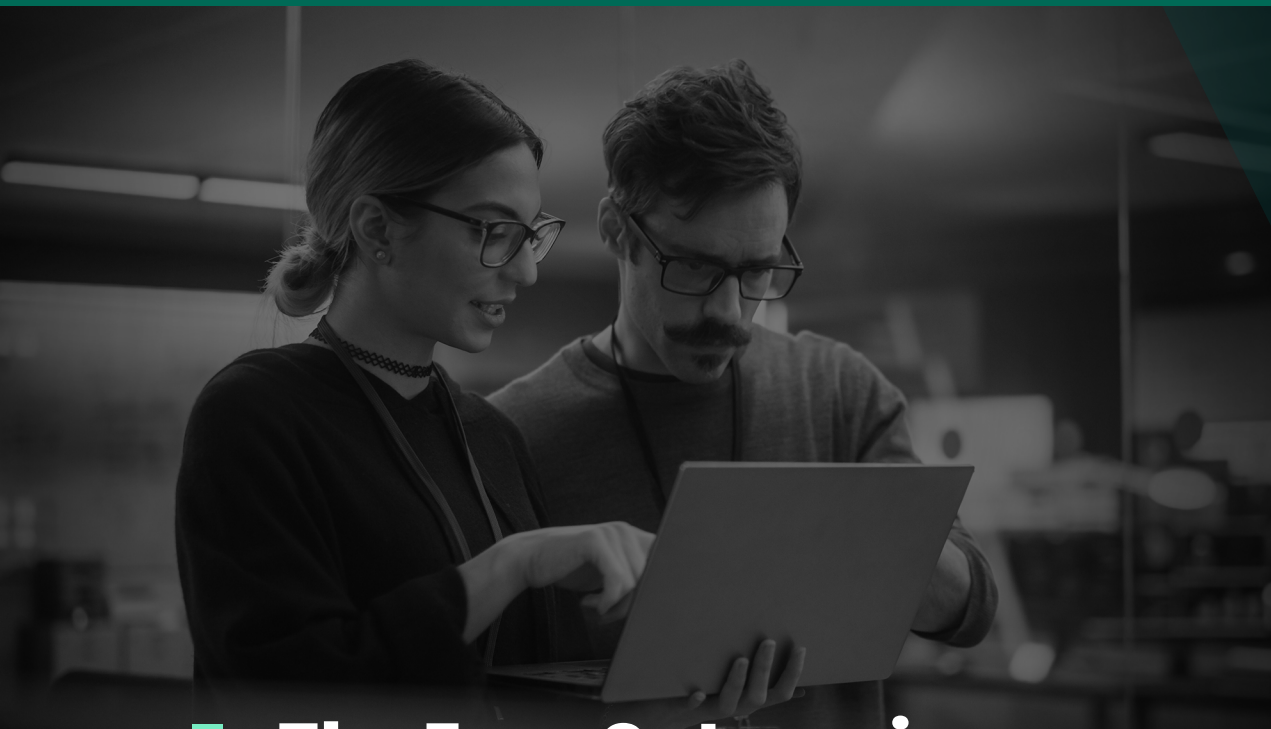


USER-BASED CLASSIFICATION

Requires a manual, end-user selection for each document. User-based classification takes advantage of the user knowledge of the sensitivity of the document, and can be applied or updated upon creation, edit, review, or dissemination indicators of sensitive information.

With context-based classification, an organization can identify, classify, and provide critical context to data, something that can be used to create visual and metadata labels to organize data by type and sensitivity.

This metadata can be leveraged across your data security ecosystem and can add accuracy to downstream data protection tools you may already use like data loss prevention (DLP), access management, and cloud access security broker (CASB) solutions.

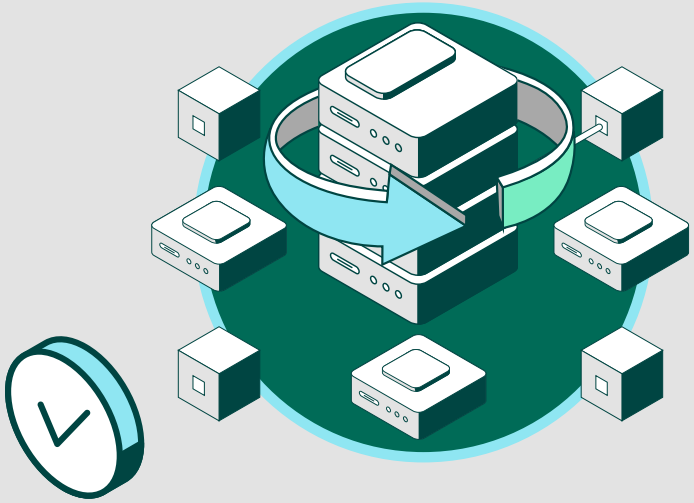


The Four Categories of Data Classification

Typically, there are four ways to categorize data.

PUBLIC

Data/information that is freely used, reused, and redistributed with no restrictions on access or usage.
Examples: press releases, brochures, and published research.



INTERNAL

Data that is strictly accessible to internal employees/personnel who are granted access.
Examples: company memos, internal communications, and marketing research.

CONFIDENTIAL

Data that requires granted access and/or authorization and should be contained within the business or specifically permissible third-parties.
Examples: Personally identifiable information, intellectual property.

RESTRICTED

Data that is highly sensitive with use limited on a need-to-know basis. If compromised or accessed without clearance, this could result in criminal charges, heavy legal fines, and irreparable company damage.
Examples: trade secrets, PII, health information, and data protected by federal regulations.

Fortra and Cybersecurity Insiders collaborated on a Zero Trust security report, asking 400 cybersecurity professionals what the most compelling tenet of implementing Zero Trust is. 64% of respondents said data protection.

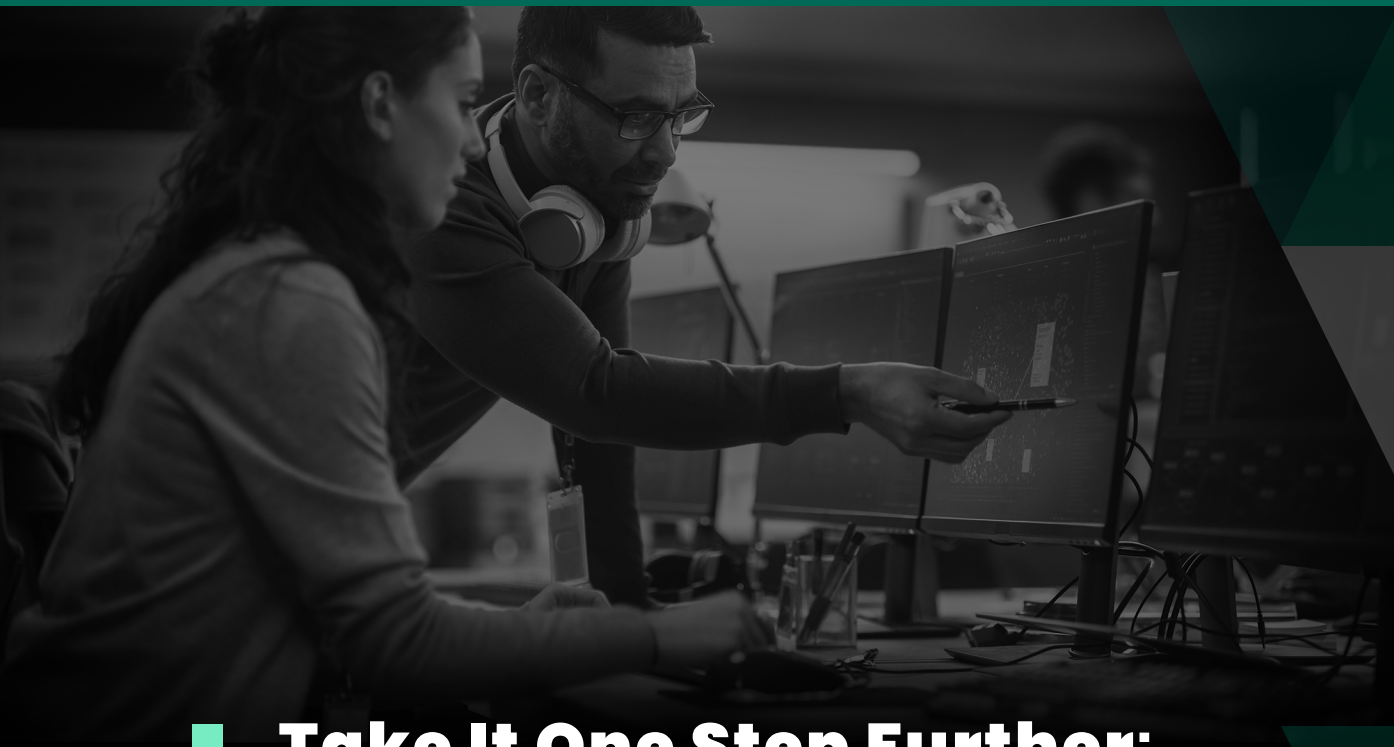
64%
Data Protection
(e.g. secure connection)

65%
Trust Earned Through Entity Verification
(e.g. user, device, infrastructure)

61%
End-To-End Access Visibility and auditability

66%
Continuous Authentication, Authorization

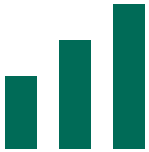
60%
Least Privilege Access



Take It One Step Further: Sensitivity Tags

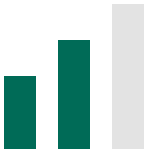
Further context can also help organizations segment data based on its risk sensitivity.

If your data was compromised, what would the damage be?



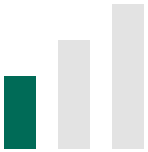
HIGH

Confidential; data that's remotely sensitive, crucial to operational security, or extremely difficult to replace if lost.



MODERATE

Restricted; data that isn't public or is used internally (by your organization and/or partners).



LOW

Public; data is usually public and not easy to permanently lose.

Data Classification and Zero Trust Go Hand in Hand

Without data classification labels and context, zero trust models wouldn't know how to check permissions around who can and can't access certain data and in turn, provision access.

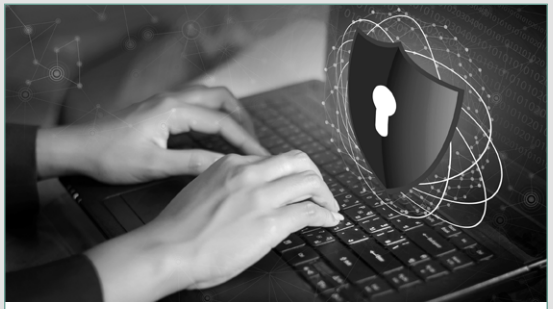
For some organizations, it's not just who can access what. It's *who* accessed what. By being able to trace back what's been accessed, organizations can get a clearer picture as to how data is being handled behind the scenes, another benefit of data classification.

79% of respondents of a recent survey said that data protection was a key driver for implementing a Zero Trust program at their organization.*

(*2023 Zero Trust Security Report: https://www.fortra.com/resources/guides/2023-zero-trust-security-report).

Zero trust requires a robust portfolio of security solutions to work—access control only solves part of the problem—thankfully the context around data provided by classification can also help inform:

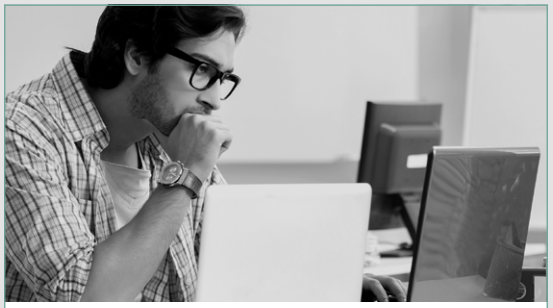
IDENTITY MANAGEMENT



FIREWALLS

AUTOMATION & ORCHESTRATION

DEVICE SECURITY



WORKLOAD SECURITY

THREAT ANALYSIS

If you're in charge of securing data at your organization, you already know that classifying it is foundational for data security. It's especially the case for organizations looking to take a zero trust approach to data protection.

Organizations serious about getting started on their zero trust journey should prioritize creating a data classification framework to determine what sensitive data they have, then classify it by sensitivity level.

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

 | fta-corp-ebook-01024-r2-as