

 BRIEF

U.S. MIDTERM ELECTIONS SERIES: ZERO TRUST AND ELECTION SECURITY

ZEROFOX INTELLIGENCE

B-2022-09-06a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Internet Infrastructure

September 6, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 5:00 PM (EDT) on August 30, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Zero Trust and Election Security

Executive Summary

Elements of network security architecture can be incorporated into the U.S. elections process to help in securing the integrity of election assets. Zero Trust architecture, which eschews implicit trust even of personnel approved for access to resources, is fully applicable to the oversight of voter registration databases. The principle of least privilege, which limits access according to minimum need, is more applicable to the non-networked processes of counting in-person votes and mailed ballots.

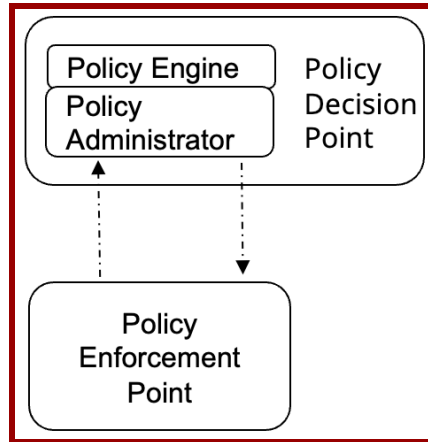
Details

Zero Trust is an approach to a security architecture that expands on the concept of least privilege. Under a least privilege architecture, access to resources is provided on a rigorously contingent basis. The minimum access needed for a user to carry out enterprise functions is allowed, with the goal of preventing an intruder from moving laterally within a system after gaining entry.¹

Under a Zero Trust architecture, no user is accorded implicit trust. In addition to a user's approved status, access is based on variable environmental conditions. A user approved for access to a resource, for example, may be denied a session or subjected to additional verification procedures if a request is made from an unusual location, the user's device shows a change in its security profile or other deviations from behavioral patterns are observed.

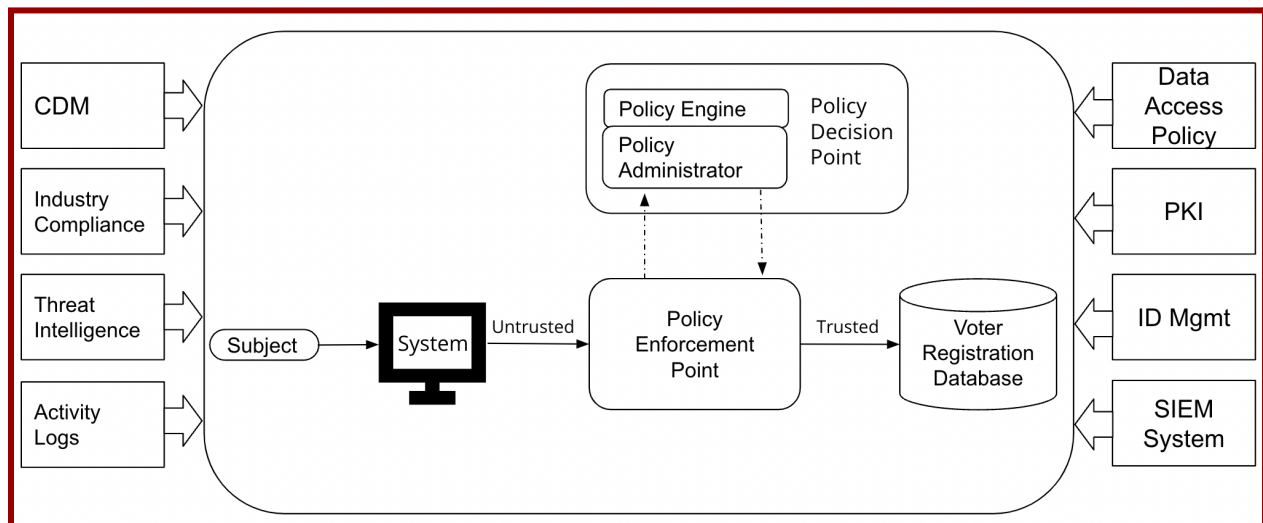
A Zero Trust deployment is comprised of two basic components: 1) a Policy Decision Point (PDP) that reviews information provided by multiple sources against a request for access and then determines whether to grant the request; and 2) a Policy Enforcement Point (PEP) that enables, monitors, and terminates connections to a resource based on forwarded requests or policy updates received from the PDP.

¹ [hXXps://www.cisa\[.\]gov/uscert/bsi/articles/knowledge/principles/least-privilege](https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege)



Source: NIST, ZeroFox Intelligence

In the context of U.S. elections, the dynamic control environment of a Zero Trust implementation lends itself most readily to securing voter registration databases for which access decisions can be informed by the resources of a mature network. Activity logs and information provided by SIEM systems can alert a PDP of anomalous behavior associated with a user, threat intelligence feeds from reliable sources can flag high-severity vulnerabilities within a user's environment, and an Identity and Access Management system can provide notifications of user attributes that fall short of compliance with access policy.²



Source: NIST, ZeroFox Intelligence

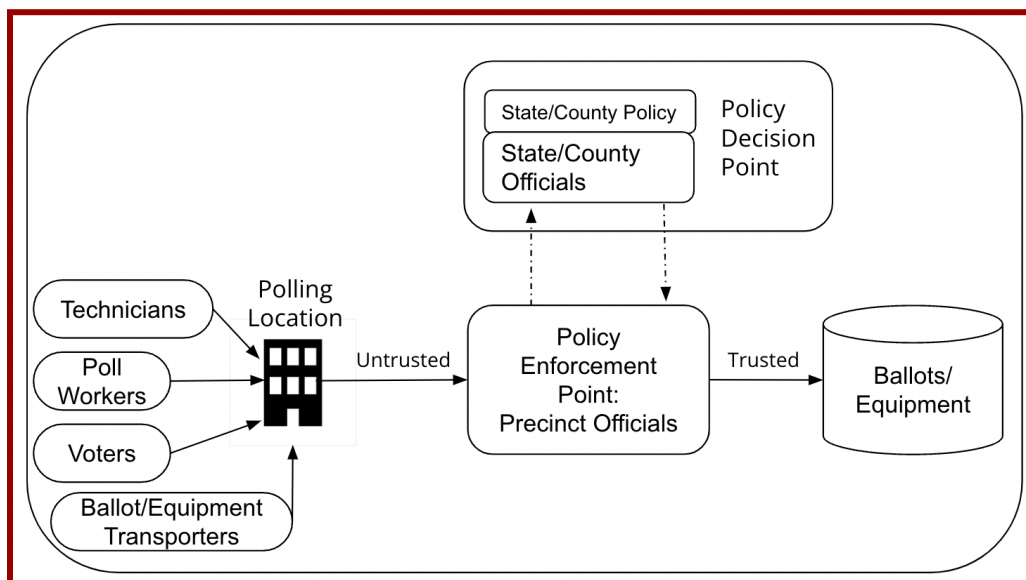
²

<https://www.ncsl.org/research/elections-and-campaigns/access-to-and-use-of-voter-registration-lists.aspx>



The voting phase of elections concerns manual and automated functions that only minimally involve network connections. That being the case, least privilege is a more applicable architecture for securing the voting process than Zero Trust. The integrity of ballots and voting equipment can be protected to a significant degree by allowing employees, officials, volunteers, and voters only the minimum access required to perform critical activities. For the most part, determinations of appropriate access will depend on predetermined needs rather than the fluid circumstances monitored in a Zero Trust environment.

Guidelines provided by the U.S. Election Assistance Commission (EAC) for staffing at polling locations delineate roles and responsibilities for handling ballots and equipment at this stage. When fully implemented, these guidelines provide the equivalent of a least privilege control environment by granting each participant no more than the minimum access needed to fulfill predetermined roles. Transporters of provisional ballots and voting equipment to polling locations are not permitted contact with these assets during the actual voting process. Voting machine technicians are allowed access to equipment solely for the purpose of conducting logic and accuracy tests prior to voting. Poll workers supervising voters are permitted contact with equipment and ballots only to the extent that voters require assistance. The voters are permitted contact with equipment and ballots only during the time required to cast individual votes. Elements of Zero Trust can be incorporated into such a scheme by codifying EAC guidelines through state and county policies, which would then serve the function of a PDP. Empowering precinct officials to enforce these policies at voting sites would provide a mechanism analogous to that of a PEP.³

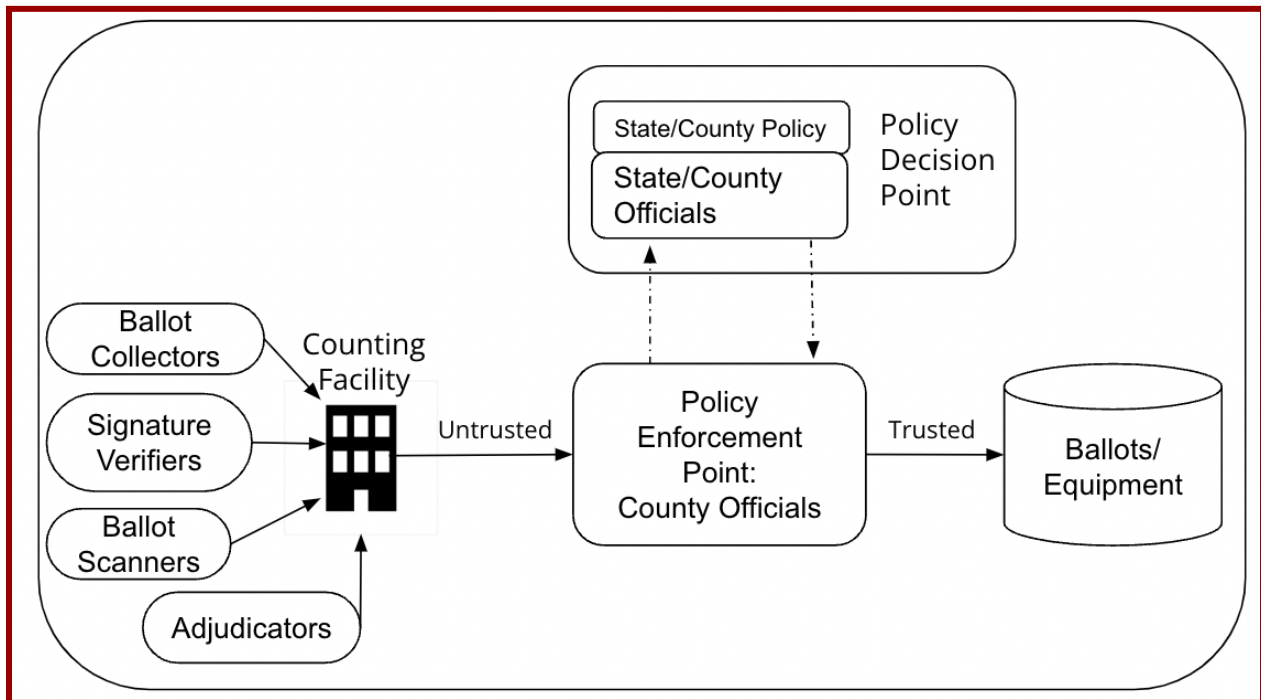


Source: ZeroFox Intelligence

³ [hXXps://www.eac.gov/voters/election-security](https://www.eac.gov/voters/election-security)



EAC guidelines concerning the “inbound ballot process”—the counting of ballots submitted by mail—would also provide what amounts to a least privilege implementation. In accordance with these guidelines, teams of personnel are allowed access to mailed ballots only for the fulfillment of distinct functions that collectively enable the ballots to be counted. Ballot collectors transport mailed votes from drop boxes and USPS centers to a counting facility in sealed containers but are not permitted to break the seals. A separate team at the counting facility would then unseal the votes and run them through a sorting machine to register their receipt, automatically verify signatures, and sort them. Another team of adjudicators would verify signatures not automatically accepted by sorting machines against voter databases to determine their validity. Yet another team would then scan all accepted ballots for a final tabulation, which would be conducted by other personnel on a non-networked device and reported. County officials present at a counting facility can provide the Zero Trust function of a PEP by enforcing limitations on the various teams’ access.⁴



Source: ZeroFox Intelligence

4

[hXXps://www.eac.gov/sites/default/files/electionofficials/vbm/Inbound_Ballot_Process.pdf](https://www.eac.gov/sites/default/files/electionofficials/vbm/Inbound_Ballot_Process.pdf)



Analyst Commentary

Implementation of Zero Trust and least privilege architectures in the networked environments for which they are intended comes at a financial cost to organizations. States and counties considering their partial or full deployment for election processes likewise face decisions about whether the benefits realized through enhanced security outweigh related costs. In issuing its recommendations for counting in-person votes and mailed ballots, the EAC suggests that cost constraints may make it desirable to cross-train teams to fill multiple functions.⁵ The resulting increased contact cross-trained participants in the vote-counting process would have with ballots and equipment would necessarily come at the cost of diminished security. Determining whether this cost is acceptable in the context of elections involves different considerations than those faced by private companies, for whom cost is generally measured in financial terms. State and county officials must account for intangibles, such as diminished voter confidence in the integrity of the elections process.

Recommendations

State and county officials can optimize decisions about incorporating Zero Trust or least privilege controls into voting processes by weighing the likelihood and impact of actions that compromise voter rolls or ballot integrity. An official may, for example, determine from a risk assessment that the likelihood of a malicious attempt to delete names from a voter registration database is low. That official may also determine that the potential impact of such an action—rejection of an electoral outcome’s legitimacy by a significant swathe of the public—is unacceptably high, leading to a decision to implement Zero Trust architecture in providing access to the database.

⁵ *Ibid.*



Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.