Implementing Zero Trust Security

A Leader's Model for Collaboration

BACKGROUND

In May 2021, the Executive Order on Improving the Nation's Cybersecurity[1] mandated advancement toward Zero Trust Architecture (ZTA) for federal departments. The Memorandum for the Heads of Executive Departments and Agencies[2] set forth a Federal ZTA strategy, requiring agencies to meet specific cybersecurity objectives by the end of FY 2024. Following U.S. Cybersecurity and Infrastructure Security Agency (CISA) guidance[3], the Centers for Medicare and Medicaid (CMS) batCAVE Zero Trust team mobilizes to meet these requirements.

CHALLENGE

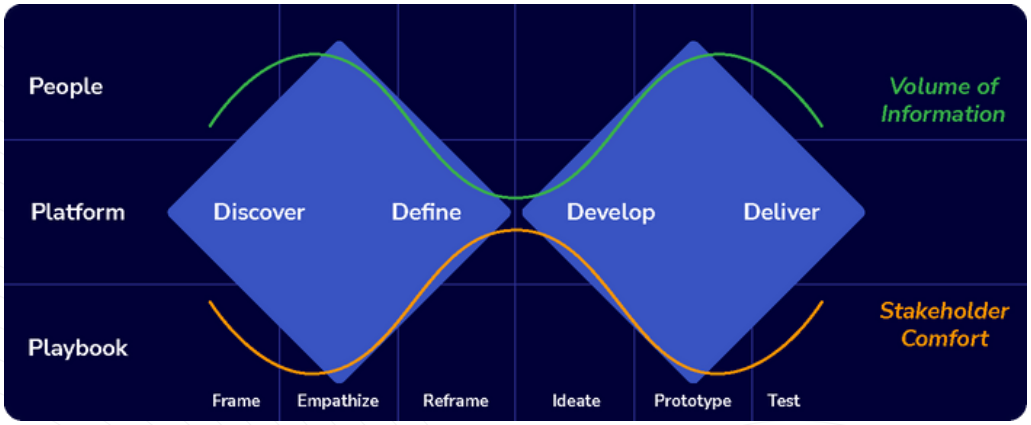
Zero Trust is a countercurrent to traditional perimeter-based security practices. Published CISA guidance helps us get better at employing accurate, least privileged, per-request access in information systems and services facing a network assumed to be compromised. This guidance means that every resource should be untrusted until proven otherwise. Most of what's published on ZTA dives into the technical requirements and engineering processes that flow toward a given Zero Trust Maturity (ZTM) level while offering instruction on what it may take to reach the successive maturity level.

However, challenges arise when organizations open the console or the conference room to start making changes to existing security workflows, governance documentation, or working processes. All guidelines acknowledge that every organization has a different starting block depending on its existing configurations. Implementing Zero Trust principles with existing SecOps is not a monolithic operation but an ongoing and, often zigzag process involving identity, infrastructure, networking, applications, and more. It quickly becomes evident that moving toward a Zero Trust Architecture (ZTA) requires cross-functional, interdisciplinary collaborations between DevSecOps experts, governance specialists, and business process influencers. How might we approach the challenge?

APPROACH

Tripod strategy to support ZT. People, Platform, Playbook

The batCAVE Zero Trust strategy builds on existing security practices but evolves them through an agile collaboration between leadership, DevSecOps, governance, and human-centered service design. We begin with the end in mind and view security from the inside out (starting from data, network, and resources) rather than the outside in (starting from the perimeter). We separate our efforts into three swim lanes, People, Platform, and Playbook, navigating change management and software implementation in four design phases: Discover, Define, Develop, and Deliver.



PEOPLE

A Zero Trust Strategy is everyone's responsibility. People often work in silos or are segmented by function. Additionally, a history of management and technology choices may lead to change-resistant organizational configurations. Our approach aims to discover and grow a customer-focused, cross-functional collaboration and break down barriers. Ironically a zero trust strategy requires an abundance of "people trust" to accomplish. While organizations may have unique titles and reporting structures, we represent Zero Trust stakeholders using a handful of Archetypes who work together to bring about a ZTA.

- The **CIO** is someone who understands ZTA's business value and the risk to the brand if there's a security breach. They champion and invest, propelling the project over time while buoying executive leadership's expectations and motivating the team.
- An **Architect** brings a systems-level view and synthesizes and prioritizes competing project needs across identity, devices, networks, apps, and data.
- The **Engineers** collaborate across Identity, Network, Security, Infrastructure, and Applications to implement detailed, often interdependent development and documentation requirements.
- The **Governors** ensure that the project direction exceeds existing organizational governance and enforcement policies and work with the team to document and canonize Zero Trust changes.
- The **Stewards** manage the project and service design process, customer user experience, and components that require evangelism and socialization. They keep it real. They are disciplined in honoring human-centered exchanges essential to successful change management.

There is no one channel toward maturing a zero-trust stance! These Personas work together across their expertise and influence to invite and promote positive velocity toward ZTA through small, quick wins followed by socialization and coalition-building. The aim is to deliver working solutions in an agile, iterative process, first understanding and mapping the Platform and its People through the Discover & Define processes, then constructing a Playbook to help Develop and deliver on Zero Trust guidelines.

PLATFORM

With batCAVE Zero Trust, our Architects, Engineers, Governors, and Stewards collectively map the configuration of the current platform and the people who operate it. With collaboration from our CIO and the Customer, we form a series of instruments to help us understand what and who we're working with and where we are starting from. Our instruments include network diagrams, customer personas and archetypes, workflow diagrams, system maps, and many references–all of which may be used to project future state advances. We capture the technological and business processes at play, as both influence how improvements can happen. As we Discover and Define, we uncover the platform's risk appetite and learn about existing security practices that may already implement Zero Trust principles or be able to with minor adjustments (quick wins).

One obvious next step has been to approach Network Policies head-on. Micro-segmentation is critical to a zero-trust-enhanced networking environment. Network Policies divide a network into increasingly smaller zones and enforce access control policies between those zones. These policies move an environment away from a traditional 'perimeter-based' security schema to one that is more resilient to lateral movement. Implementing Network Policies within the batCAVE brings us closer to a higher level of maturity in the Networks Pillar (see below).

PLAYBOOK

Simultaneous with platform discovery, batCAVE Zero Trust works with our stakeholders to agree on a maturity model to follow. We refine the CISA model to meet the specific needs of the batCAVE and CMS customers. The CISA model separates Zero Trust into a "gradient of implementation across five pillars" of activity. The pillars include Identity, Devices, Networks, Applications and workloads, and Data. These five pillars are supported by cross-cutting security functions: Visibility and Analytics, Automation and Orchestration, and Governance. Through our customizations, we can more accurately focus on specific improvements. For example, our CMS stakeholders customize the Identity pillar to include both user identities and developer and non-person entity identities, further describing the model and opening opportunities for incremental changes for each identity type.

Our playbook brings us in contact with an abundance of solutions. Continual friction within a zero-trust journey can be the constant pull of promising technology solution products in the marketplace. The batCAVE Zero Trust team continually evaluates new and existing products but aspires to let people and their requirements inform solutions before deciding on products.

In the case of Network Policies above there are several open source and proprietary solutions that could serve the problem statement we defined. As part of our batCAVE journey we thoroughly vet and test competing products through rigorous proof of value assessments, issuing recommendations on which solution offers the best value for investment.

Our playbook helps us socialize and educate, bringing stakeholders along on the vetting and testing journey and building relationships to Develop and Deliver. Through demo days, working groups, and office hours, the batCAVE Zero Trust team continually monitors and collaborates with the people who will help make platform, infrastructure, and application changes happen.

Ultimately, to develop and deliver, we embed the Zero Trust Architect and Engineers within the customer teams. This may mean we have our own dev and test clusters where we attempt changes and test results before calling the whole team to test and deploy.

SOLUTION

The batCAVE Zero Trust initiative is a solution in progress. There is not a monolithic outcome but instead a series of small integrated and ongoing changes that bring the batCAVE toward ever-higher levels of Zero Trust Maturity across the five pillars of functional activity. We work collectively with stakeholders across infrastructure, governance, and zero-trust subject matter experts to first discover, prioritize, define, and develop prototypes and beta tests, and deliver them to production.

REFERENCES

[1] Executive Order on Improving the Nation's Cybersecurity

[2] Memorandum for the Heads of Executive Departments and Agencies

[3] CISA Zero Trust Maturity Model

batCAVE

rvcm.com/batcave-zero-trust