Invicti

WHITE PAPER

Modern application security in a Zero Trust approach

Highlights from the May 11, 2022 Roundtable

2021 was a banner year for cyberattacks, with reported breaches increasing by 68 percent. The record-breaking number of 1,862 data breaches had most organizations in the public and private sectors scrambling to secure their supply chains. Attacks are not slowing down, and the road to an improved security posture in the public sector is steep, especially for agencies still relying on legacy systems.

In a recent roundtable discussion hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with **Invicti**, IT leaders from various Federal agencies discussed the challenges that come with updating legacy systems and some of the factors holding their teams back from modernizing web application security.

Challenges to updating legacy tools

One of the primary challenges agencies face when updating legacy tools is in minimizing the risk of breaches to systems when transitioning from one system to another. During the migration process, systems are particularly vulnerable to attacks, and security measures must be robust enough to bridge the gap from legacy systems to new ones.

Additional challenges involve siloed teams and competing security priorities within agencies. For many agencies, operations and security teams continue to function independently and are not quite operating in a DevSecOps fashion. Each team has its own priorities, which makes implementing new security applications across systems more challenging.

Roundtable participants agree that changing the culture of an organization is the first step in formulating an agency's identity to prioritize modern security applications. For agencies to successfully transition from legacy systems, they need leaders and teams that are adaptable and willing to change.

Existing processes blocking innovation

When thinking of the modernization journey of an agency, often it is the hierarchy of an organization that slows down innovation. Agencies with multiple divisions have different priorities and goals, leaders, and teams. Typically, security applications require the work of multiple teams to move forward for successful implementation. If one team does not view a new technology or application as a priority, there will be problems successfully implementing new technology.

Silos also impede workflow pipelines and even require manual interception of workflows in order to communicate with systems in the same organization. Moreover, many new projects require the expertise of contractors who work in different locations and in different pipelines.

With so many stakeholders, progress can slow down or stop, usually because there is a lack of leadership and direction in how progress should continue. While culture is a critical component to the successful implementation of new technology, there are tools agencies can deploy, like APIs, to tie together disparate processes in certain instances.

Overcoming challenges to updating legacy tools:

- *Minimize risk of breach in migration stage*
- *Harmonize security priorities between teams*
- *Promote culture of change and adaptation*
- *Eliminate innovation blocks caused by hierarchy*

The most urgent element of Zero Trust

Panelists agree that while tools and automation are important to meet Zero Trust mandates, agencies must first determine what Zero Trust means for their organization. This involves defining what Zero Trust is in context to the needs of an organization, as they will differ from one organization to the next. Agencies should first approach Zero Trust by determining what the end goal is rather than implementing tools for the sake of meeting a mandate.

From an application security perspective, the most urgent element of Zero Trust is the overall principle of **trust nothing and test everything**. When building a DevSecOps pipeline, there is nothing that is insignificant in the Zero Trust framework and every aspect requires testing. However, to do this successfully at the enterprise scale requires the use of automation tools.

The importance of modern, updated tooling in Zero Trust

When thinking about CISA's Zero Trust Maturity Model and its emphasis on automation and integration, modern tooling is a critical component to meet these standards. The ability to scale without sacrificing accuracy requires automation, especially when teams are composed of a few people or less. Modern tooling, particularly the multitenancy ability to coordinate implementation across teams, is critical for agencies to meet mandates of Zero Trust security.

Elements in Implementing Zero Trust:

- *Implement tools towards a defined end goal versus meeting mandates*
- *Scale without sacrificing accuracy*
- *Be proactive by keeping up with technology trends*
- *Allow additional attention to API integration points*

When an agency goes through the process of modernizing tools, they are faced with two definitions of Zero Trust. They must define what Zero Trust means in their current environment as well as the modern environment they aspire to. The more advanced agencies are in their current environment, the more agencies can adhere to the Zero Trust methodology.

A challenge smaller agencies encounter is the lack of budget to put towards Zero Trust. Costs go up every year from a vendor standpoint, so it is important for agencies to structure contracts to save on costs. Smaller agencies are also disadvantaged because their needs are typically not reflected in many of the security tools available on the market.

Some agencies have complex budgets where funding comes from and is tied to multiple places, such as trusts, donations and traditional operating funds. This makes modernizing tooling and meeting Zero Trust mandates more challenging. Other larger agencies that utilize capital funding are not met with funding constraints and can more easily update tools.

The key drivers to adopt Zero Trust

While the private sector is continually identifying trends to remain competitive in an ever-changing market, the government is much more reactive in its approach to implementing technology. Unfortunately, breaches are often the key drivers for change in the government. These security events initiate change and prompt executive orders. Another driver that leads agencies to Zero Trust is the promise of efficiency gains and saving taxpayer dollars.

In order to be more proactive, top leaders must be knowledgeable on key trends and give technology practitioners more leeway to implement new technology more quickly. The reality is that Federal IT leadership tends to be risk averse, which puts them at odds with any modernization efforts or the desire to make application and infrastructure changes to truly embrace Zero Trust.

Current gaps in web application security

The applications that are the safest do not allow anyone into the network or have role-based identity protections to limit or prevent access to internal networks. Gaps in security can exist when APIs touching servers introduce integration points that are not as secure as possible. While not an ideal form of security, security wrappers may exist for APIs to secure legacy systems during transitions. It is important for agencies to take steps, even though they may not be ideal, towards Zero Trust.

Conclusion

Agencies will need to continually move towards attaining Zero Trust, because there is no end to advancements in technology. Zero Trust concepts may transform or adjust, but there will not be an end to Zero Trust. Perhaps when security is no longer necessary and attack vectors are completely hardened will Zero Trust be achieved.

Zero Trust is important to move towards, even for small agencies with few resources. However, all agencies, regardless of size, must be able to articulate their security problems and understand where they fit into Zero Trust in order to procure the correct tools from vendors. Panelists encouraged all those who are pushing for change to continue to be proactive.

Invicti is a scalable, multi-user web application security solution with built-in workflow and reporting tools ideal for security teams of all sizes. It's available as a hosted and self-hosted solution and can be fully integrated in any development or testing environment.

Contact us for more information here.