Zero Trust Report

Lessons Learned from Vendor and Partner Research

Cybersecurity Community of Interest

Date Released: May 5, 2021

Synopsis

As government agencies try to cut through the jargon of "Zero Trust", IT security officials are looking to implement Zero Trust principles. However, a lack of understanding and confidence with Zero Trust architectures may be slowing adoption. ACT-IAC launched projects to support agencies in their Zero Trust journey, specifically to enhance understanding of and more confidence with Zero Trust.

The project team developed this whitepaper in alignment with the National Institute of Standards and Technology (NIST) standards and Cybersecurity and Infrastructure Security Agency (CISA) guidance. This report synthesizes the work of the industry-government partnership to gather and organize industry reported solutions that will assist professionals in conceptualizing the next step in their unique Zero Trust journey.

This page is intentionally blank

American Council for Technology-Industry Advisory Council (ACT-IAC)

The American Council for Technology-Industry Advisory Council (ACT-IAC) is a non-profit educational organization established to accelerate government mission outcomes through collaboration, leadership and education. ACT-IAC provides a unique, objective, and trusted forum where government and industry executives are working together to improve public services and agency operations through the use of technology. ACT-IAC contributes to better communication between government and industry, collaborative and innovative problem solving, and a more professional and qualified workforce.

The information, conclusions, and recommendations contained in this publication were produced by volunteers from government and industry who share the ACT-IAC vision of a more effective and innovative government. ACT-IAC volunteers represent a wide diversity of organizations (public and private) and functions. These volunteers use the ACT-IAC collaborative process, refined over forty years of experience, to produce outcomes that are consensus-based.

To maintain the objectivity and integrity of its collaborative process, ACT-IAC welcomes the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of technology. For additional information, visit the ACT-IAC website at www.actiac.org.

Cybersecurity Community of Interest

The ACT-IAC Cybersecurity Community of Interest mission is to facilitate collaborative development and implementation of solutions and best practices related to cybersecurity challenges. The COI provides opportunities for industry and federal government to identify, raise awareness, and provide solutions to cybersecurity challenges critical to protecting our national interests.

Disclaimer

This document has been prepared to contribute to a more effective, efficient, and innovative government. The information contained in this report is the result of a collaborative process in which several individuals participated. This document does not – nor is it intended to – endorse or recommend any specific technology, product, or vendor. Moreover, the views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development. Every effort has been made to present accurate and reliable information in this report. However, neither ACT-IAC nor its contributors assume any responsibility for consequences resulting from the use of the information herein.

Copyright

Table of Contents

Table of Figures

Executive Summary

As government agencies try to cut through the jargon of "Zero Trust", IT security officials are looking to implement Zero Trust principles. ACT-IAC launched projects to support agencies in their Zero Trust journey. In 2019, ACT-IAC published a report on the current Zero Trust trends[1] including market research, presentations and demonstrations, and evaluation of the underlying trust algorithms.

The concepts and components of Zero Trust have caught the eye of federal agencies seeking to implement least privileged access principles. However, a lack of understanding and confidence with Zero Trust architectures (ZTA) may be slowing progress. ACT-IAC embarked on phase 2 of the Zero Trust project to enhance understanding of and more confidence with Zero Trust.

The project team developed this whitepaper in alignment with the National Institute of Standards and Technology (NIST) standards and Cybersecurity and Infrastructure Security Agency (CISA) guidance. This report synthesizes the work of an industry-government partnership to gather and organize industry reported solutions into categories that will assist professionals in conceptualizing the next step in their unique Zero Trust journey.

The ACT-IAC Phase 2 project team was organized into three teams. The team authoring this report (referred to as "Vendor Outreach Team") was assigned to conduct research and determine what the original equipment manufacturer (OEM) vendors and managed services partner community could offer in terms of products and capabilities as aligned to various Zero Trust models in the market (ACT-IAC Cloud Pillars, NIST Publication 800-207[2], Department of Homeland Security Continuous Diagnostics and Mitigation (CDM) program[3], and NIST SP 800-53 controls[4]). The project team sent Request for Information (RFI) to over 150 companies directly operating on Zero Trust initiatives, with well over half responding. The results and findings from the information collected were informative and, in some cases, surprising.

Research Methodology

Background

Zero Trust concepts have been around for several years now. However, federal government demand for information and the potential to implement Zero Trust's principles is currently high. In seeking support from industry, the General Services Administration (GSA) and ACT-IAC partnered to bring structure to the Zero Trust narrative. Is there something fundamentally new about Zero Trust in the modern, cloud-first world? Is Zero Trust marketing fluff to get agencies to open their wallets? Likely a bit of both. The stated goals of seeking this information are:

[1] Zero Trust Cybersecurity Current Trends, April 18, 2019 https://www.actiac.org/zero-trust-cybersecurity-current-trends

[2] Zero Trust Architecture https://csrc.nist.gov/publications/detail/sp/800-207/final

[3] https://www.cisa.gov/cdm

[4] Security and Privacy Controls for Information Systems and Organizations https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

1. Educate the Federal Government on the vendor products and solutions available to them to assist in implementing Zero Trust designs,
2. Organize and correlate the information received into a reference matrix to be used by Federal Government entities to assist them with selecting products and solutions targeted at specific focus areas within their network, and
3. Improve the overall posture of cybersecurity within the Federal Government with more modernization based on the principles of Zero Trust.

The project team developed a request for information (RFI) to collect current information about Zero Trust from industry. A fundamental assumption underlying the RFI was that Zero Trust is at its core, a concept that requires a complex set of mature capabilities to implement at scale. Underlying this assumption is that no single company can provide an end-to-end Zero Trust solution; multiple components must converge for successful implementation and service delivery. The intent is to educate and clarify how Zero Trust concepts are implemented in real-world situations and to identify any trends in capabilities and use cases currently in the market.

Approach

The RFI was developed to provide a balance of open response and structure so that vendors would tell their story and force a modicum of standardization to the replies. The open-ended questions helped to define the boundaries of Zero Trust. Additionally, the questions sought to understand how Zero Trust solutions are designed and implemented and where they have been creatively applied to mission problems. The structured questions focused on facilitating comparison across solutions and capabilities, providing a framework for strengths and weaknesses in Industry, and highlighting where interoperation and integration were critical to a real-world implementation.

Figure 1: Vendor Responses

The team compiled a list of 165 companies, both large and small, to solicit responses and information. These were various OEM and Managed Services vendors from a wide range of solution categories: software-defined networking, identity management, authentication, cloud security, data analytics, and endpoint security. The hope is that the wide net would pull in a variety of viewpoints and use cases. Sixty separate vendors replied to the request for information, including a number that had not been a part of initial brainstorming efforts as likely prospects. The additional 20% of the respondents not in the prospect list were primarily from service providers and integrators. These responses provided a unique perspective on the ways to integrate solutions in a multi-vendor environment.

Here is a summary of the respondents:

- The research identified potential OEMs and Managed Security Service Providers (System Integrators, Carriers, etc.) who have marketed that they offer Zero Trust solution components.
- 165 targeted companies were directly invited to respond to the RFI.
- The RFI process was released in partnership with GSA.

- The 165 companies invited to respond to the RFI represented a diverse group. Examples of this diversity included domestic and global companies, large/mid-sized/small companies (in terms of revenues), new (< 5 years) and old (>100 years), public and private companies, OEMs, Service Providers, and value-added resellers.
- 60 companies ultimately responded. 46 of the companies who responded were OEMs. 14 of the companies who responded were service providers, integrators, or value-added resellers

RFI Questionnaire

The questionnaire was structured to address a range of topics from conceptual to actual and focused on a balance of ACT-IAC's previous work and the (at the time) draft NIST 800-207 publication. Questions were grouped and vendors were asked to answer as many as they desired but guided to ensure at least one question from each group was answered and all responses included use cases.

The first two questions were considered **Architectural:**

1. *How do your company's products/solutions align with the "pillars" of Zero Trust as described in the ACT-IAC Zero Trust white paper dated April 18, 2019?*
2. *How are the Zero Trust tenets (cited inside of "Draft" NIST Special Publication 800-207 "Zero Trust Architecture") realized through the use of your products?*

The next two questions were considered **Operational:**

3. *Where do your products fit into the logical design of a Zero Trust Architecture as documented in the latest draft of NIST SP 800-207 "Zero Trust Architecture"?*
4. *How do your products implement and operationalize Zero Trust (refer to sections 3.1 and 3.2 of draft NIST SP 800-207 "Zero Trust Architecture")?*

The final question pair mapped capabilities into existing federal **Frameworks:**

5. *How do your products/solutions align with the Zero Trust Pillars when mapped with the DHS Continuous Diagnostics and Mitigation (CDM) capabilities?*
6. *Identify how agencies can utilize your Zero Trust products and solutions to implement NIST SP 800-53 security controls.*

The final question asked for documented **Use Cases:**

7. *Provide descriptions and references for no more than three currently implemented use cases (preferably of environments of 10,000+ end users) that leverage your products and services in a Zero Trust architecture. If any of your use cases require integration with other 3rd party products to demonstrate its Zero Trust capabilities, please provide details.*

Response Overview

There were not significant differences in how organizations chose to engage the questions, but there were general themes. 40% of respondents took the recommended path and answered one of each question pair, and 25% chose to answer every question. Overall, the nature of the responses was indicative of a greater familiarity with the ACT-IAC document than the recently released NIST SP 800-207. However, the team expected this since the NIST SP 800-207 was still in draft when the RFI was released. Most

companies found the DHS CDM framework preferable to answer than the NIST SP 800-53 framework. Given the flexibilities afforded in the CDM framework, and fewer components of the CDM framework in comparison, this is an expected outcome. The majority of NIST SP 800-53 respondents provided previously developed content.

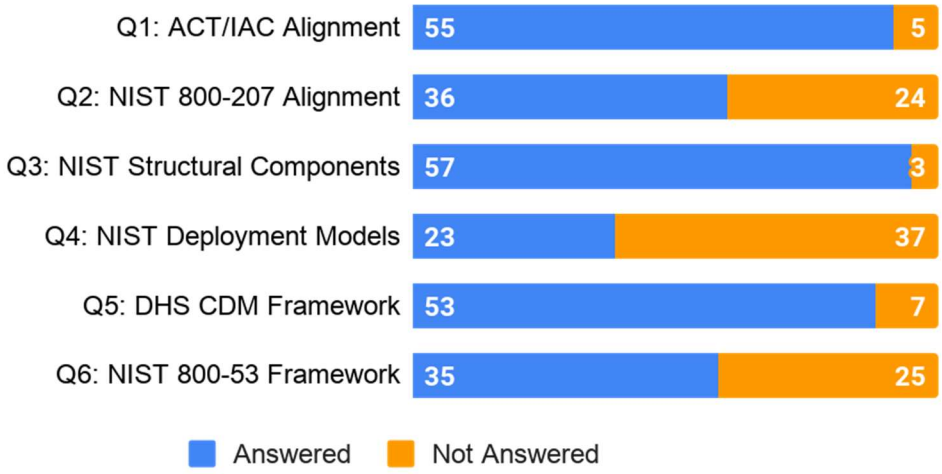

Figure 2: Overview of Response Rate per Question

Observations of the Architectural Concepts Responses

The responses to the RFI's first two **Architectural** questions showed a distinct difference in how responses from OEM vendors and service providers (carriers and system integrators) were given. OEM vendors provided a pillar centric view of how their product or products fit into a Zero Trust Architecture. Service providers typically provided a more comprehensive view of a complete Zero Trust architecture through additional details related to integrating products from an agency's existing environment with new Zero Trust components that could be added.

As an example, one OEM vendor response spoke to the specific capabilities of a device identity tool in terms of clarifying the device type, operating system version, and determining Government Furnished Equipment (GFE) versus other ownership, but did not speak to how this information would be integrated with the Zero Trust policy engine to "take action" depending on the findings. A typical service provider response would speak to satisfying a complete component of Zero Trust through the integration of multiple named vendor products, often followed by a wrapping of the individual products together into a unique system or process name of their own ("Secure Verify", "Security Verify Suite", "Infinity", "Stealth", etc.).

Observations of the Operational Concepts Responses

Questions 3 and 4 of the RFI focused on Zero Trust's **operational** components and referred the respondents to sections of the NIST SP 800-207 publication for guidance. The project team fielded questions from vendors seeking clarification on some of the reference material in NIST Publication 800-207. Respondents at the time did appear to struggle with correlating their solutions to the "new" guidance provided in NIST SP 800-207 (which was in draft form when the working group's RFI was released).

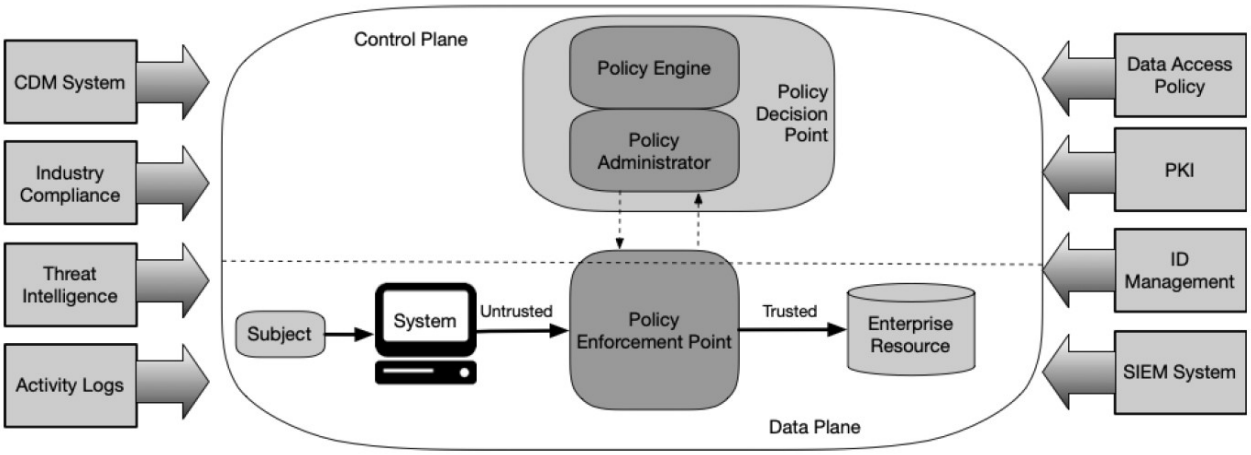

Figure 3: Core Zero Trust Logical Components (source: NIST Publication 800-53[5])

Policy Administration and Policy Enforcement Points were the most mentioned areas where both OEM vendors and service providers believed they were best aligned. Responses were scored against how many of the NIST 800-53 components were addressed. The top three responses came from a service provider (highest) followed by two OEMs. Operationalizing Public Key Infrastructure (PKI) requirements and operationalized security information and event management (SIEM) systems were the two lowest responded areas. There are possible reasons for industry having "low" capabilities in these areas. The PKI market seems to be serviced by only a handful of companies (low competition), whereas one or two large leaders dominate the SIEM market. Additional information is available in Appendix 1, where all scoring models are presented in more detail.

One additional observation is that larger companies did not necessarily show more capabilities than mid-size or small firms when directly addressing Zero Trust. This would suggest that some of the mid-sized and smaller firms that are more focused on capturing the Zero Trust market have equal or better (perceived) offerings and capabilities than some of the larger OEMs and service providers who may have divided focus on other technologies.

Observations of the Framework Concepts Responses

Questions 5 and 6 regarding **framework** concepts and capabilities around protecting data were some of the weakest represented in the RFI responses. Specific weak areas included protecting against data spillage, data discovery/classification, and data rights management. The table below shows the percentage of respondents who stated that they had capabilities in the various components of a Zero Trust framework.

[5] Security and Privacy Controls for Information Systems and Organizations
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

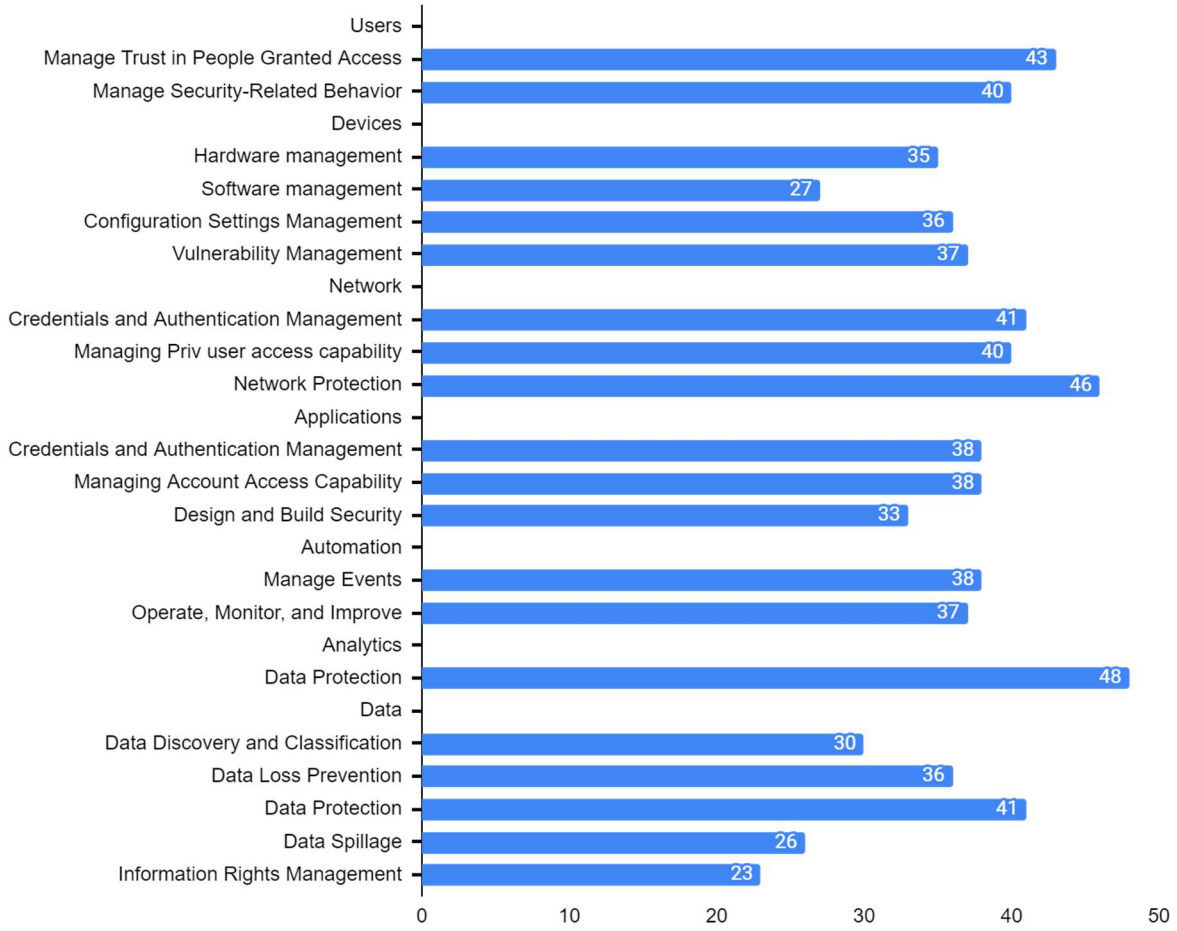

Figure 4. Percentage of Respondents Who Had Capabilities in Zero Trust Framework Components

Regarding support for the NIST SP 800-53 controls, the feedback is summarized in the Treemap shown in Figure 5. The Treemap suggests more robust industry capabilities in the Access Control and Identification & Authentication control families, while fewer options and capabilities are found in Media Protection and Contingency Planning. Concerning the RFI, this makes sense to an extent as these control families are less related to Zero Trust. Additional details of the framework responses can be found in Appendix 1.

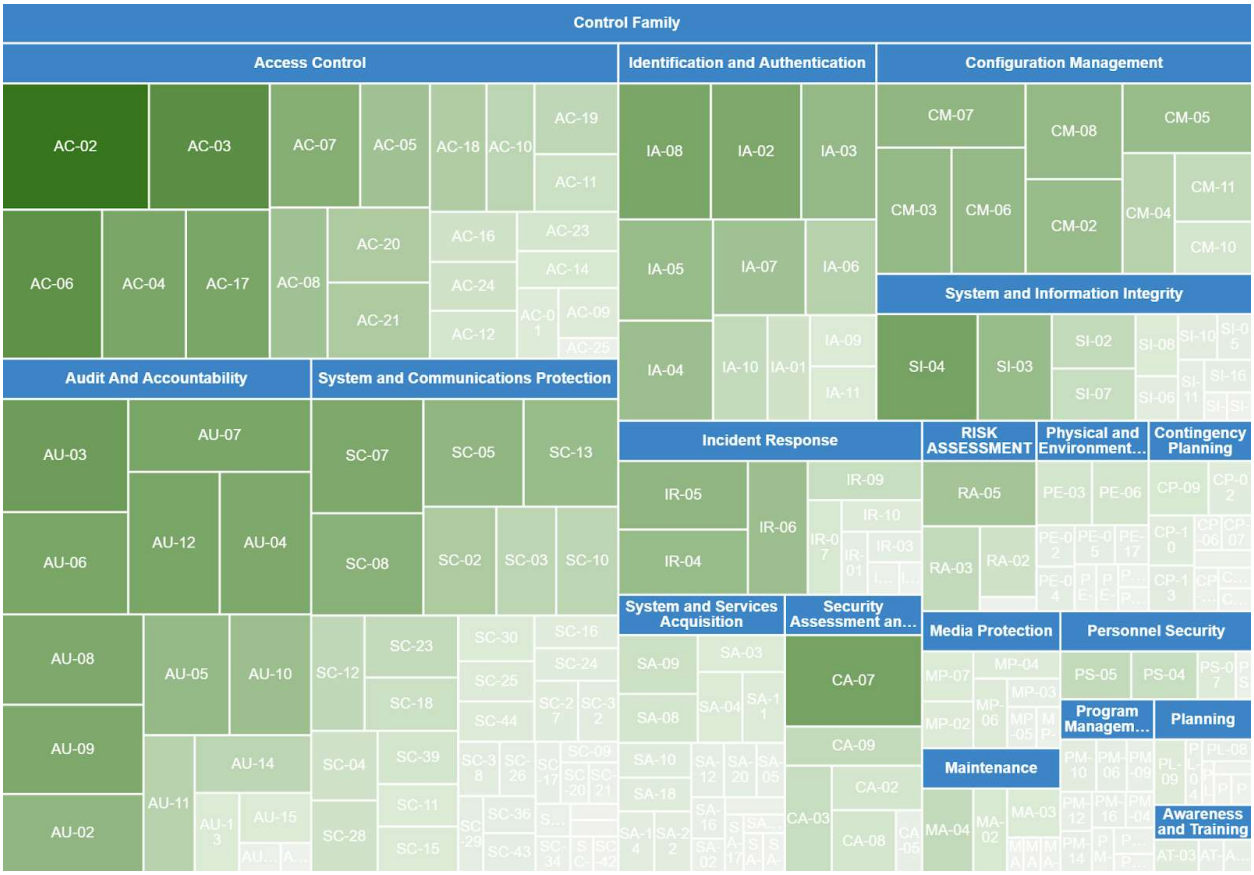

Figure 4. Treemap of Vendor Response Capabilities to Z.T. Aspects of NIST SP 800-53 Controls

Themes Discovered

Areas of Strength

One significant observation resulting from the 60+ vendor responses and 125 products "pitched" is that agencies should be able to construct a complete Zero Trust architecture today as the products are available now. In some cases, the products and solutions were manufactured uniquely for a Zero Trust architecture, whereas in other cases, existing products have been "repurposed" or "bent" for an application in a flexible Zero Trust architecture. The result of this observation is that agencies can build a first-generation Zero Trust network today, and they should expect to see significant innovation (i.e., more features, more automation, etc.) as more Zero Trust focused architectures are implemented and mature. Agencies should expect to see near-term innovation with Z.T.'s architectural components, followed later by the operation and framework components, as more experience with Zero Trust architectures will drive additional best practices and produce lessons learned.

The vendor responses also illustrated that "maturity depth" varied depending on the tenet, pillar, or Zero Trust architectural component that an agency would want to construct. For example, user and device identity offerings were numerous and represented one of the mature areas of the Zero Trust architecture with the most significant number of product responses. Additionally, policy engine and policy enforcement were additional areas that received a high volume of vendor responses, also suggesting

maturity with this component. On the other hand, data spillage and data information rights were areas within the NIST SP 800-207 document that received minimal vendor response. Vendors seemed at times to be "guessing" their product and solution applicability to these newer components of Zero Trust, and as time goes on, we would expect to see growing maturity in these areas.

Although a Zero Trust architecture's core components are available now and can enable a Zero Trust structure, the business systems to efficiently run a Zero Trust network may be lagging. Once constructed, a Zero Trust network is very dynamic and requires nimble and flexible tools and processes to run it. While reviewing the vendor responses, there was not enough confidence provided to the review team to attain a high level of comfort that currently available tools are enough to run a Zero Trust architecture efficiently. The team anticipated that more integration, automation, high performance, and artificial intelligence/ machine learning capabilities would be required to optimize a Zero Trust model's operations and thus lead agencies to the greater security return on investment that they seek with implementing Zero Trust.

Finally, the project team noted that Zero Trust definition is narrowing and becoming more standardized. Historically, the definition has had many interpretations based on the early understanding of Zero Trust concepts as it came from some of the early adopters and leading voices in the space. As time has gone on, widespread vendor messaging and a large number of public webinars available on the topic have contributed to more common themes and a more unified understanding of Zero Trust.

While there are still some differences in defining the topics and core ideas around Zero Trust, NIST, who should be the authority for the federal government's understanding, defines Zero Trust as:

> *Zero trust (Z.T.) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (Z.T.A) is an enterprise's cybersecurity plan that utilizes Zero Trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a Zero Trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a Zero Trust architecture plan. (Source: NIST SP 800-207)*

Agencies can expect the definition and related terms of Zero Trust to continue to narrow as more experience is gained through common architectures, lessons learned, and best practices.

As mentioned, three areas received the lowest response rates to the RFI: data, automation, and analytics. One possibility for reduced responses could be perceived overlap with the CDM program, where Data Protection Management Pilots (How is data protected?) have been taking place with data loss prevention (DLP) solutions since approximately June 2020.

Data Attributes: A Zero Trust architecture (and its management) is concerned with the pillars as having been defined. CDM is concerned with those same concepts, although perhaps organized differently.

As pointed out in a recent Federal News Network article[6], "By the end of fiscal 2021, agencies must certify to OMB and the Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security that they have implemented the CDM Program Data Quality Management Plan (DQMP) and can be "fully able to exchange timely data to the federal dashboard." An August 2020 GAO report points out

[6] OMB sets new CDM data standards deadline for agencies https://federalnewsnetwork.com/reporters-notebook-jason-miller/2020/11/omb-sets-new-cdm-data-standards-deadline-for-agencies/

some of the difficulties associated with data quality when tools for hardware asset management, software asset management, or configuration management are not fully configured or deployed in such a way to ensure data quality[7]. A well-implemented and documented Hardware Asset Management (HWAM) and Software Asset Management (SWAM) inventory is the starting point for data quality.

Data Security: While agencies and vendors alike would like to automate data classification and policy building tasks, one of the challenges that remain is that data classification and meta-data tagging remain largely a manual burden.

Another area of weakness relating to the themes that the working group received is that there **does not appear to be a "handbook" or a "how-to" user manual** for Zero Trust. Agencies will ultimately find themselves working through the best methods to interconnect the various components of a Zero Trust architecture without an authority present who could confirm that the design and implementation were done "the right way." Much like guidance for building a doghouse might suggest you have a roof and an opening for the dog to come in and out, the actual design and look of the doghouse could vary widely yet achieve the same result. The same is true with building an agency specific Zero Trust architecture.

Although the respondents' use cases are reviewed further in this report, there was indeed a weakness in the fragmented nature of the use case examples. A couple of responses that claimed an entire Zero Trust platform could be built from products available from a single vendor, but the use cases provided to support these claims did not provide confidence that any current vendors could accomplish this effectively or at scale.

Another area where the working group saw weakness was a general understanding of how to reply to an RFI. While outside the scope of this effort, we would like to provide some general feedback to vendors. When responding to any RFI, start and be clear on all the assumptions being made about the target environment and/or use cases around deploying a product or solution. Many vendors assume a set of circumstances (and perhaps think the customer is making the same assumptions). They should clearly state what assumptions they are making to help the customer better evaluate their product's suitability in the environment or overall mission.

Vendors should also ensure they describe their products in terms of how it overlays on top of the complete holistic Zero Trust solution and then identify all the gaps that remain after overlaying their solutions/products. This will give the reader a sense of the coverage gap and where they need to supplement to attain the complete holistic Zero Trust solution.

Lessons Learned from Use Cases

The last RFI question requested the respondents to provide use case examples where they have implemented Zero Trust components. Responses varied from "no response" suggesting that respondents had no production experiences with Zero Trust to an "end to end" response stating that one entity is fully on a ZTA already (although did not protect data at rest). In between those two extremes were use cases for both commercial and federal entities with write-ups of varying partial applications of technology in a ZTA. The majority of the use cases cited were for the commercial sector (57%) and were limited in terms

[7] Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program https://www.gao.gov/products/gao-20-598

of extensive implementations. The use cases read as if the market is new and emerging with Zero Trust and further suggested that there are only a few complete implementations especially in the Federal sector.

For federal agencies that have not started their journey to Zero Trust and that represent a "green field" opportunity, a wholesale transition may be an option. For example, an agency may have never placed any systems into the Cloud and is looking to modernize via digital transformation. That may be a situation that could warrant a large Zero Trust investment (Identity, Credential, and Access Management [ICAM], Cloud, etc.). As movement toward the Cloud increased, the redesign effort could be infused with Zero Trust capabilities and technologies. Merging two separate efforts, in this case a modernization along with an implementation of Zero Trust principles, can potentially add complexity to the effort but also adds to the possibility of achieving an end state more quickly.

Also based on the use cases, vendors seem to be pro-actively thinking about integration as it appears that no single vendor can implement the entire ZTA on their own. However, several vendors have "fabrics" and/or "platforms" into which they plug/integrate other vendor's offerings which is key when working with ZTA that have such dynamic decision making requirements. Performance will be a factor in a successful Zero Trust deployment. Agencies should be aware that integrating two best of breed products together does not necessarily produce a best of breed outcome. In one example, a vendor responded with a Zero Trust design involving 19 separate products that while it achieved a Zero Trust approach appeared to be difficult to scale and operationally cumbersome.

Several cloud-specific Zero Trust use cases were mentioned suggesting that Zero Trust outcomes can be obtained inside or outside of the traditional network. Zero Trust appears to be applicable to both traditional and emerging network architectures.

Overall, across all of the use cases, there were wide examples and sampling of use case applications provided. Examples include applications for remote workers, data center cloud shifts, securing cloud workloads, user/device identification, segmenting the network, insider threat protection, virtual private network (VPN) replacement, improvements on network visibility, utilizing hardware tokens, and password-less authentications. This suggests there are lots of design options applicable to Zero Trust and because the parts of Zero Trust are indeed interrelated, planning is key. Do not get two-thirds of the way down the road and then have to retreat and rework previous components of the solution.

Associated inventories are critical to Zero Trust implementations and as such, the use cases generally showed organizations selecting technologies tightly aligned to the use case and implementation model, and a narrowly focused or green-field deployment. For example, the brokerage model is popular for protecting specific cloud applications and for VPN replacement. The narrow focus or green-field approach can simplify the associated data management and leads to more successful outcomes.

Further Innovation and Upcoming Trends

More Features and Capabilities

With the building blocks of Zero Trust already available and in place today, agencies can expect to see vendors develop more in-depth features and capabilities for the existing Zero Trust architectures. Examples might include additional criteria to authenticate users and devices (e.g., time, geo, biometrics,

password-less, predictive identity, etc.), improved integration and sharing across vendor products with additional common formats and standard graphical user interface (GUIs), and improvements in data housing such as separation, encryption, and archiving. Expect to see an increased reliance on behavior analytics and machine learning as the cloud-native vendors continue to increase the capability to expand the definition of multi-factor authentication. There continues to be significant interest in Zero Trust, and with that interest, anticipate and expect innovation and improvement.

Expect to see more "Security as Code" as it is required to handle the granular nature of Zero Trust at scale. Additionally, expect to see increased support for seamless integration in SecDevOps, DevSecOps, and GitOps environments and other tools like IT service management (ITSM)\SIEM platforms to meet sustainment challenges. These technologies should have robust API support and work with and not against the continuous integration/ continuous deployment (CI/CD) pipeline.

Additionally, more ZTAs will take a Data-Centric Approach. Understanding access beyond IP Addresses and URLs will be critical to lay the foundations moving to Zero Trust designs. For example, security policies and controls that can use Meta-data (Tags/Labels) applied to cloud workloads/services, or data objects, are pivotal for granular control inside those use cases. These concepts allow network-based access controls and data-at-rest object controls to be well integrated to achieve a Zero Trust data-centric approach and allowing for conditional controls while detaching from the legacy "*ball-and-chain"* location requirements.

More Automation

With AI and ML capabilities expanding, agencies can expect to see more applications of these technologies in ZTAs. AI/ML capabilities are expanding at the same time ZTAs are growing, so agencies should proceed with caution to manage the risk associated with new technologies. Effective ZTAs require constant analysis of who is on the network and what they are trying to access, all while making dynamic decisions to allow, deny, or challenge access. Automating the sharing of information across the Zero Trust components will help enforce automated decision-making regarding granting access, narrowing the span of control, constant monitoring and challenging behaviors, and processing data.

More Adoption, Use Cases, Lessons Learned, and Experience

The use cases and references provided by the vendor respondents to the RFI were limited and shallow regarding a complete Zero Trust architecture. As new ZTAs launch and as more agencies drive maturity into their current Zero Trust deployments, expect improvements in the architecture, operations, and frameworks of Zero Trust. Additional best practices and lessons learned should come from new and deeper Zero Trust deployments. It will be necessary for agencies to share their experiences to foster continued adoption and more mature use cases.

More Competition and Product Offerings

As the marketing hype and agency Zero Trust deployments continue to grow, more vendor competitors will enter the space and more product offerings will be available. There are benefits and challenges associated with more competition. These benefits will include more customer choices, the pressure to innovate, and often higher quality options at lower prices. Be aware that the challenges will consist of

market confusion in the options to choose from, continuously evolving (and conflicting) standards, and feelings that your organization's installed solution is already obsolete. Competition could get fierce, and competitors may need to innovate, or they could get pushed out. Always keep a measured approach while moving forward.

Conclusion

The ACT-IAC project team has been working through the response data for the RFI for more than six months before completing this report. Along the way, some of the group's observations have changed and are reflected in the information above. Zero Trust remains a dynamic topic even as it settles in as a key potential architecture for government agencies moving forward. Here are five key takeaways from the Phase 2 research:

1. The definition of a Zero Trust architecture is narrowing thanks to additional Federal and industry guidance, additional deployments, growing experience, and increased collaboration and awareness in the community.
2. The components necessary to start or complete your agency's Zero Trust journey are available now.
3. No one company can do it all (nor would an agency necessarily construct such an implementation)
4. There is room for additional innovation, especially in the operational aspects of running a Zero Trust architecture.
5. Although early in its implementation stage, Zero Trust has shown great promise and appears to be a viable architecture moving forward. We can all expect more use case data and best practice recommendations in the months ahead.

Authors

This paper was written by a consortium of government and industry representatives. The organizational affiliations of these contributors are included for information purposes only. The views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development.

Indrajit Atluri	Ernst & Young
Julia Benson	CGI Federal
Tom Conway	Palo Alto Networks
Darren Death	ASRC
Lauren Fishburn	Cisco
Dan Flynn	Verizon
Theodore Gates	Cisco Systems, Zero Trust Project Lead
Greg Gutman	ArdentMC
David Harris	Department of the Interior, Zero Trust Project Lead
James Harrison	Fortinet
JD Henley	Verizon
Steven Hernandez	Department of Education
Dan Jacobs	General Services Administration, Project Government Sponsor
Jodi Kohut	Broadcom
Stephen Kovac	Zscaler
Dave McClure	Accenture Federal Services
Emell McKelvey	Mackkell Technologies, LLC
Kenneth Myers	General Services Administration
Adewale Omoniyi	IBM
Jonathan Roy	Appgate
Rachel Schultz	Appgate
Matthew Shallbetter	Department of Health and Human Services
Sudhindra Shetty	CC Pace Systems
David Stepp	Environmental Protection Agency
Gary Wang	SAIC

Appendix: Additional Analysis of RFI Response Data

This Appendix provides additional analysis of the responses to the RFI questions. Review this entire report as some of the findings, conclusions, and opinions related to the responses are in earlier sections. Questions 3 through 7 provided the opportunity for more in-depth quantitative analysis so graphs and charts have been provided.

Question 1 Response Analysis

How do your company's products/solutions align with the "pillars" of Zero Trust as described in the ACT-IAC Zero Trust white paper dated April 18, 2019?

Given the history of the ACT-IAC engagement with the vendor community and the draft status of NIST SP 800-207, it is not surprising that most vendors answered question 1. Even though it was not requested, many vendors provided an overview of their company and a broad description of their overall approach to Zero Trust and how their products fit into this more extensive architecture. This story-telling was extremely useful, as it helped to ground their specific responses and instill more confidence in what was intended with what was presented.

Because the Zero Trust arena is still new and the various deployment methods, supporting services, and technologies vary widely, this open-ended storytelling is critical to ensuring proper communication. Future RFI's and procurements will be well served in soliciting solutions rather than prescribing requirements in the Zero Trust space.

Question 2 Response Analysis

How are the Zero Trust Tenets (cited inside of "Draft" NIST Special Publication 800-207 "Zero Trust Architecture") realized through the use of your products?

While not as many vendors responded to the NIST SP 800-207 architecture question, the NIST tenets' broad wording seemed to invoke a more technical response from vendors. This was particularly the case for vendors who answered both Architectural questions. Where a vendor only responded to question 2, it was more commonly treated as an opportunity to describe their solutions at a high level. This was helpful to gain an understanding of the scope of a solution suite, and when combined with the more defined structure of later questions, provided a method to uncover areas of follow-up where weaknesses seemed to arise. The combination of open storytelling and structured responses was effective for companies engaged in the response process more deeply.

Question 3 Response Analysis

Where do your products fit into the logical design of a Zero Trust Architecture as documented in the latest draft of NIST SP 800-207 "Zero Trust Architecture"?

Vendors were asked to rate their capabilities against NIST SP 800-207 Zero Trust ecosystem. It was left up to the respondents to read the publication and interpret the definitions. While the items active in a Zero Trust conversation (i.e., the subject using a system to access an enterprise resource) may not be defined explicitly in NIST SP 800-207, these components were included as part of the request. Quantitative analysis showed a significant preference for managing, administering, and implementing Zero Trust policies and integration with SIEM solutions. The weakest response areas show up in the System, PKI, and identity management areas. For PKI and Identity Management, respondents

leverage point solutions rather than implementing their capabilities. Within NIST SP 800-207, the System is the PC, mobile device, or other clients the subject uses to access an enterprise resource. Lacking a specific definition, the responses exposed those vendors who understand the solution and those who simply checked all the boxes. Example responses here can quickly reveal effort and understanding:

Clear understanding

[The product] ensures that only corporate devices meeting a specific security posture can access private applications.

System as illustrated above is the platform (including devices, applications, or services) by which a subject requests access to the PDP/PEP

[The product] attests to the risk level of a mobile device. This information would be provided to make dynamic risk-based decisions on access.

Missing the mark

The System … is the cybersecurity paradigm . . . there are various components which work together as a system.

NIST SP 800-207 Capability	Responses			
	Implements	Enhances	Integrates	No Part
Policy Engine	33	16	8	3
Policy Administrator	34	17	9	5
Subject*	27	16	10	9
System*	22	17	20	13
Policy Enforcement Point	34	17	9	2
Enterprise Resource*	23	18	18	7
CDM System	25	17	16	5
Industry Compliance	27	15	15	1
Threat Intelligence	26	20	14	2
Activity Logs	26	21	12	2
Data Access Policy	28	12	9	7
PKI	22	14	12	11
ID Management	20	23	13	8
SIEM System	17	32	16	1

Figure 6: Question 3 Response Table

Question 4 Response Analysis

How do your products implement and operationalize Zero Trust (refer to sections 3.1 and 3.2 of draft NIST SP 800-207 "Zero Trust Architecture"?

This question saw the least response and the most variation in alignment between expectations and results. The core of this question was a matrix between NIST SP 800-207 Sections 3.1 and 3.2 which addresses architectural and deployment variations respectively. This question asked vendors to understand these two sections and place their tools in the nexus of the architectural approach to enforcement and the underlying methodology for managing policy. For example, Google's well publicized BeyondCorp model could be characterized as a Resource Portal.

	Deployment/Enforcement Mechanism				
Policy Creation Mechanism	Device Agent/Gateway-Based	Enclave-Based	Resource Portal-Based	Device Application Sandboxing	{OTHER}
Identity Governance	GOV-A	GOV-B	GOV-C	GOV-D	GOV-O
Micro-Segmentation	SEG-A	SEG-B	SEG-C	SEG-D	SEG-O
Network Infrastructure and Software Defined Perimeters	PER-A	PER-B	PER-C	PER-D	PER-O
{Other Mechanism}	OTH-A	OTH-B	OTH-C	OTH-D	OTH-O

Figure 7: Deployment/Enforcement Mechanism (source: NIST Publication 800-207)

The expectation was that this would provide a direct comparison of how solutions are used in the real world and validate the data required for the trust decision. Unfortunately, either the request was not clearly articulated or the option to avoid was too enticing. Vendors who have been active in ACT-IAC and Zero Trust discussion did a good job of interpreting and sharing their methodology.

Question 5 Response Analysis

How do your products/solutions align with the Zero Trust Pillars when mapped with the DHS Continuous Diagnostics and Mitigation (CDM) capabilities?

The CDM pillars were the favored framework. The flexibility and scale of the CDM areas was easier for vendors to slot in their products while still allowing thoughtful responses.

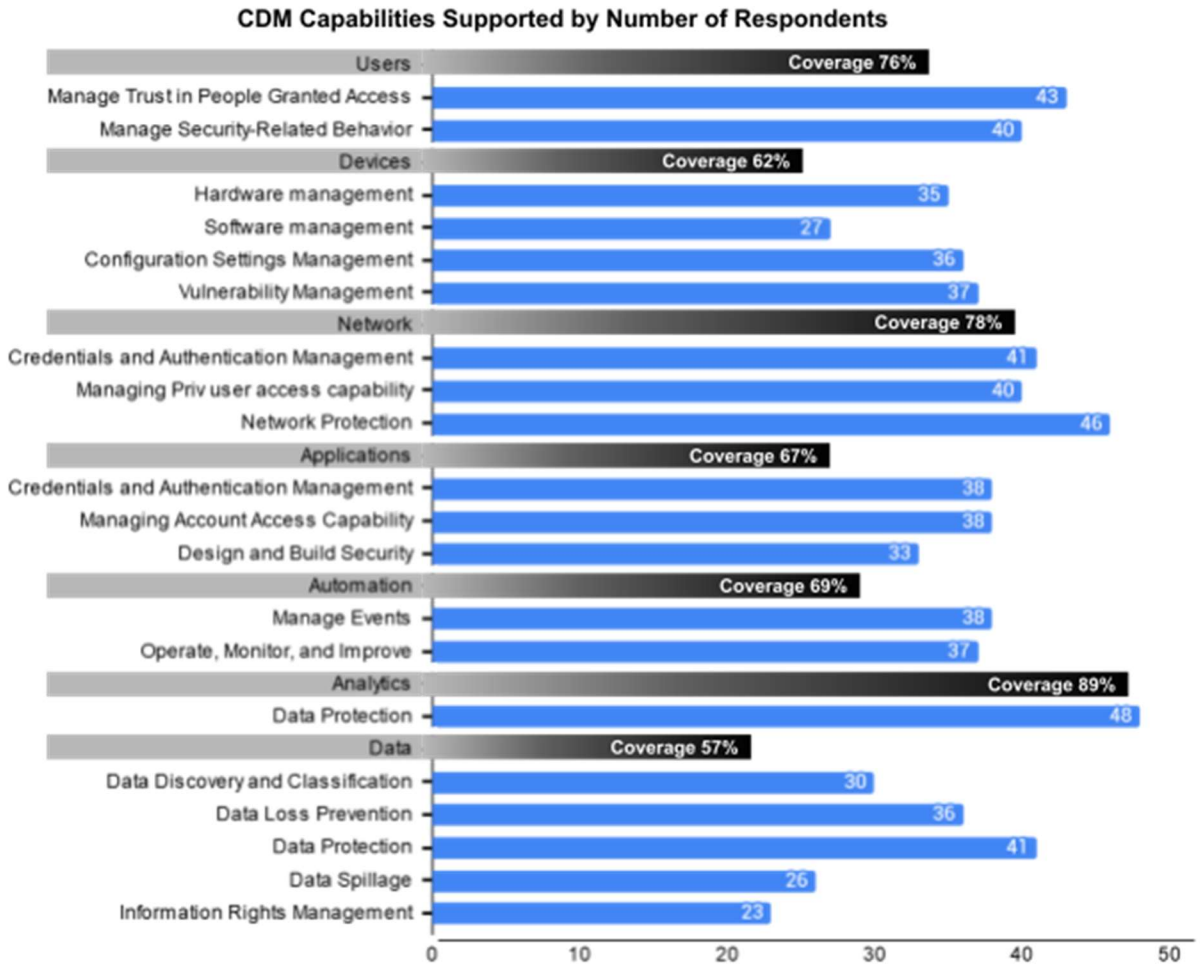

Figure 8: CDM Capabilities Supported by Number of Respondents

Zero Trust Pillars	CDM Capabilities	Description	Functional Area
Users	**Manage Trust in People Granted Access**	Assesses the inherent risk to an Agency from insider attacks for the purposes of granting trust to users and authorizing each user for certain attributes.	**TFA6**
	Manage Security-Related Behavior	Ensures that authorized users with or without special security responsibilities exhibit the appropriate behavior for their role.	**TFA7**
Devices	**Hardware management**	Discover unauthorized or unmanaged hardware on a network.	**TFA1**
	Software Management	Discover unauthorized or unmanaged software on a network.	**TFA2**
	Configuration Settings Management	Ensures that authorized security configuration benchmarks exist and contain acceptable value(s) for each relevant configurable setting for each IT asset type.	**TFA3**

Zero Trust Pillars	CDM Capabilities	Description	Functional Area
	Vulnerability Management	Discover and support remediation of vulnerabilities in IT assets on a network as defined in NIST SP 800-53 controls.	**TFA4**
Network	**Credentials and Authentication Management**	Ensures that only proper credentials are authenticated to systems, services, and facilities.	**TFA8**
	Managing Privileged User Access Capability	Provides an agency the assurance that users and systems have access to, and control of, only the appropriate resources. The capability identifies access beyond what is needed to meet business requirements.	**TFA9**
	Network Protection	Limits, prevents, and/or allows the removal of unauthorized network connections/access via devices such as firewalls that sit at a boundary and regulate the flow of network traffic. It also includes the use of encryption to protect traffic that must cross logical boundaries and addresses physical access systems that limit unauthorized user physical access to Federal Government facilities.	**TFA5**
Applications	**Credentials and Authentication Management**	Ensures that only proper credentials are authenticated to systems, services, and facilities.	**TFA8**
	Managing Account Access Capability	Provide an agency the assurance that users and systems have access to, and control of, only the appropriate resources. The capability identifies access beyond what is needed to meet business requirements.	**TFA9**
	Design and Build in Security	Describes preventing exploitable vulnerabilities from being effective in the software/system while in development or deployment.	**TFA13**
Automation	**Manage Events**	Describes preparing for events/incidents, gathering appropriate data from appropriate sources, and identifying incidents through analysis of data.	**TFA11**
	Operate, Monitor and Improve	Describes audit data collection and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing).	**OMI**
Analytics	**Data Protection**	Provides data protection functions through cryptography, masking/obfuscation, or access control. This CDM Capability includes user and entity behavioral analytics that support detection of suspected compromised accounts (people or application), endpoint devices, data exfiltration, and insider access abuse (including excessive or unauthorized access to data, functions, and privilege abuse) and provide context for security investigations.	**TFA14**
Data	**Data Discovery and Classification**	Supports data protection functions through data identification, data classification, and data tagging.	
	Data Loss Prevention	Provides data protection functions through data loss prevention capabilities, to include data protection policy management and data protection security orchestration.	

Zero Trust Pillars	CDM Capabilities	Description	Functional Area
	Data Protection	Provides data protection functions through cryptography, masking/obfuscation, or access control. This CDM Capability includes user and entity behavioral analytics that support detection of suspected compromised accounts (people or application), endpoint devices, data exfiltration, and insider access abuse (including excessive or unauthorized access to data, functions, and privilege abuse) and provide context for security investigations.	
	Data Spillage	Provides data breach/spillage response actions.	
	Information Rights Management	Provides data protection functions through information rights management capabilities using fine-grained access control to encrypted data.	

Question 6 Response Analysis

Identify how your Zero Trust products and solutions can be utilized to implement NIST SP 800-53 security controls.

Qualitative analysis process: Responses were accepted when they asserted whether the solution implements, supports, integrates, or plays no role. Lacking an obvious assertion, the team looked at the response language for guidance. For example, an active verb used in description was interpreted as Implements, while the use of "help" or "supports" indicated a supporting role. The ratings are given a numeric value from three (3) for implements to zero (0) for plays no role.

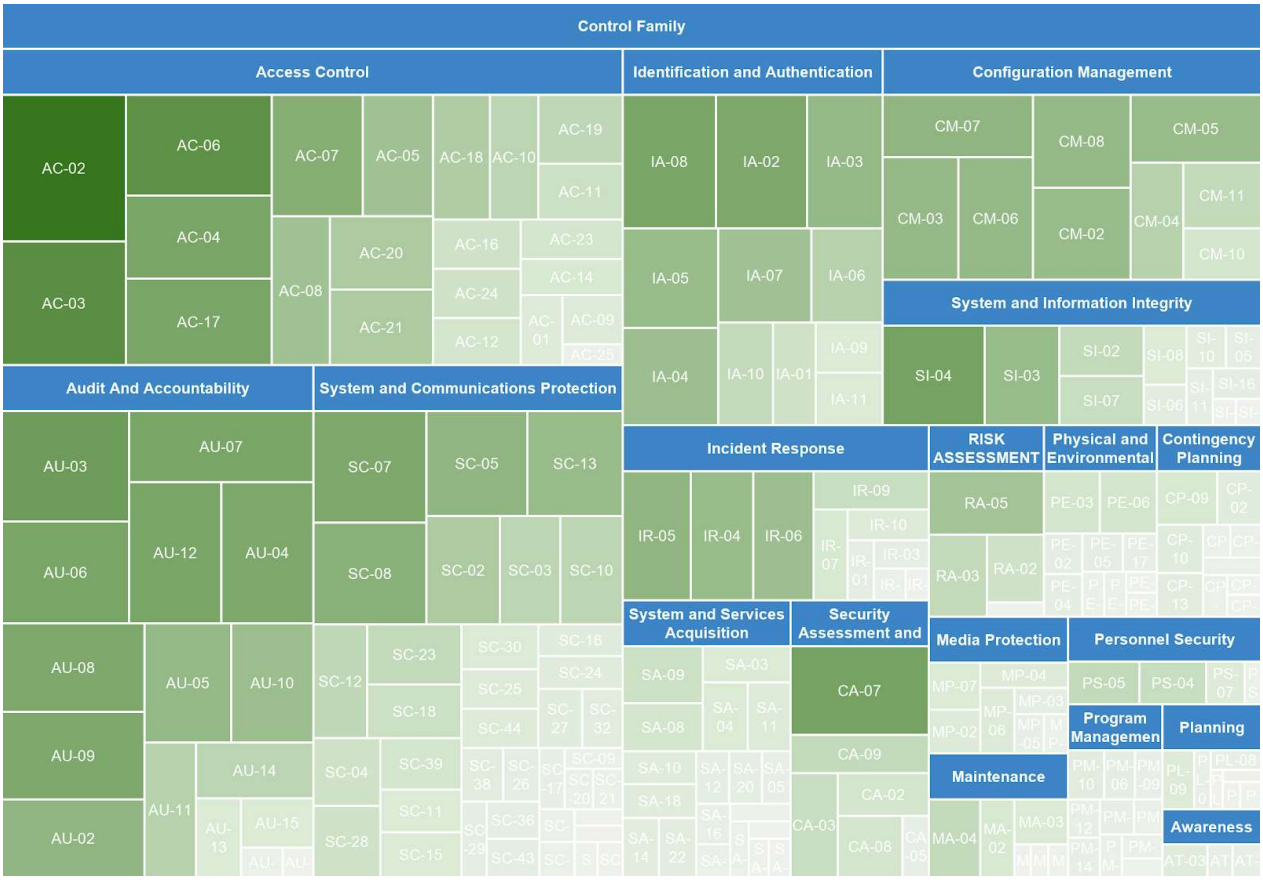

Figure 9: Treemap of Control Families

The treemap above shows which control families and controls are most commonly supported by the Zero Trust vendors. The relative size and darker color represent a higher score.

The chart below shows the Access Control, Audit and Accountability, and Systems Communication Protection families as most supported. Training and Awareness, Contingency Planning, and Maintenance are examples of control families that are not handled well within the Zero Trust space.

Most Supported NIST SP 800-53 Controls

Control	Control Name	Score
AC-02	ACCOUNT MANAGEMENT	51
AC-03	ACCESS ENFORCEMENT	42
AC-04	INFORMATION FLOW ENFORCEMENT	34
AC-06	LEAST PRIVILEGE	41
AC-17	REMOTE ACCESS	34
AU-03	CONTENT OF AUDIT RECORDS	37
AU-06	AUDIT REVIEW, ANALYSIS, AND REPORTING	34
AU-07	AUDIT REDUCTION AND REPORT GENERATION	34
AU-12	AUDIT GENERATION	34
CA-07	CONTINUOUS MONITORING	35
IA-08	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	34

Control	Control Name	Score
SI-04	INFORMATION SYSTEM MONITORING	35

Question 7 Response Analysis

Provide descriptions and references for no more than three currently implemented use cases (preferably of environments of 10,000+ end users) that leverage your products and services in a Zero Trust architecture.

The use case question was surprisingly poorly handled across respondents. Many vendors seemed to feel that "available on request" to be appropriate to the research efforts as if the intent was to validate the response's authenticity rather than elicit a specific example of their products supporting Zero Trust implementations. Generally, the most effective responses followed any standard CV structure: problem statement, solution, outcomes, and impacts.

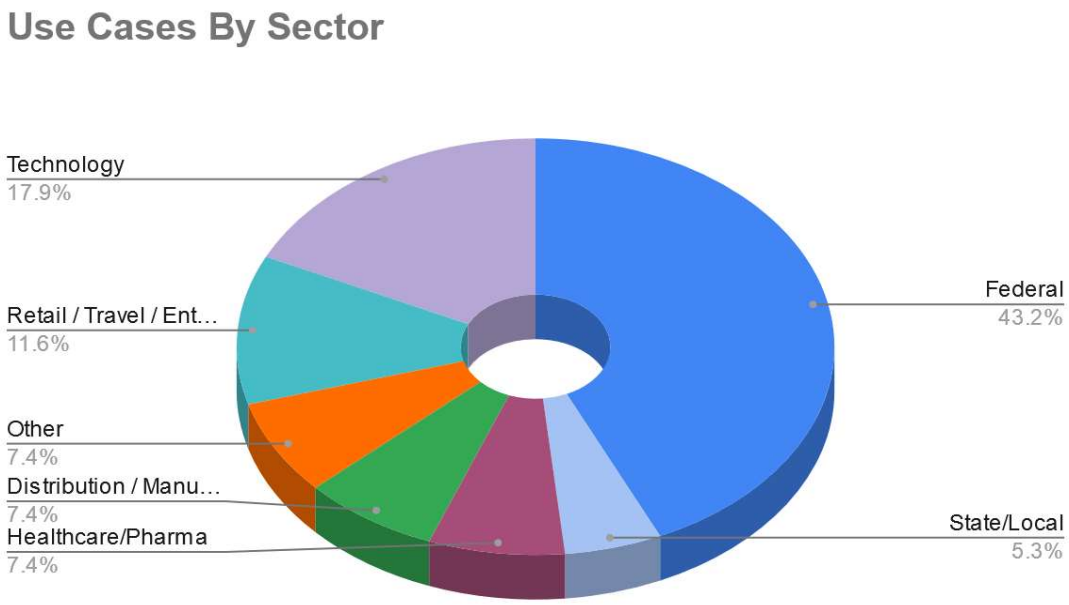

Figure 10: Use Cases by Sector

As seen on the above pie chart, the use cases were ~43% Federal (largest) and ~5% State/Local deployments. The Technology, Retail/Travel/Entertainment, Distribution/Manufacturing, and Healthcare/Pharm responses represented a wide variety of business sizes ranging from large, multi-billion dollar firms to smaller ($25M) firms. The Banking/Finance use cases had several large Global 50 firms with use cases focusing on protections for customer-facing services, data loss prevention, and implementing Zero Trust inside of shared data centers.

One use case from the “Other” slice was from the Education sector and involved moving a distance learning application into a Zero Trust design.

Overall, the use cases typically represented partial components of a ZTA with a wide range of write-ups on user and device identification, protecting data exfiltration, network segmentation via the policy engine/enforcement points. Use case impacts also identified inter-Cloud trust, security orchestration and automation, and visibility.