CROWDSTRIKE

REQUEST FOR COMMENT RESPONSE
Zero Trust Maturity Model

1 October, 2021

I. INTRODUCTION

In response to CISA's request for comment on its Zero Trust Maturity Model, CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

In recognition that the primary audience for this document is Departments and Agencies rather than a broader group of stakeholders, we will focus on feedback that reflects our experience working with such organizations and aligns best to their needs.

II. COMMENTS

We emphatically agree that it is necessary for federal agencies to adopt a zero trust model, as described in E.O. 14028, "Improving the Nation's Cybersecurity." We have previously offered specific feedback on NIST's *Planning for a Zero Trust Architecture: A Starting Guide for Administrators* (3 September 2021) and OMB's *Federal Zero Trust Strategy* (21 September 2021), and encourage readers to consult those documents directly, though certain elements are cited here. In general, we view this Maturity Model (hereafter, "the Model") as a well-conceived, thoughtful approach to a difficult and complex problem and think it will serve as a helpful companion to those documents and NIST Special Publication (SP) 800-207. We offer specific feedback on the Model below on a section-by-section-basis.

Front Matter

Section 4 states that "Zero trust presents a shift from a location-centric model to a more data-centric approach for fine-grained security controls between users, systems, data and assets that change over time." And indeed, several of the existing ZTA resources cited in Section 5 utilize this framing. We caution that, rather than data-centricity, ZTA should attempt to emphasize resource-centricity and/or identity-centricity. Thinking about data itself--disconnected from the question of who can establish permissioned access to it, and how they are challenged to do that--risks leading planners astray.

Additionally, not all data should be viewed as equal. The confidence of that data, and where it exists within the architecture, are important elements when later utilizing it as a signal into ZTA policy enforcement points (PEP).

Section 7 provides an overview of existing federal cybersecurity programs, and notes that on account of new ZTA guidance within E.O. 14028, "CISA programs will evolve and new CISA programs may emerge to align with this EO." We note that Section 7 of the E.O. requires the establishment of an Endpoint Detection and Response (EDR) program across the '.gov,' which both may be a reasonable candidate for a new program and could drive ZTA principles during design and implementation. Many large enterprises in the commercial/private sector space, as well as several in the State, Local, Tribal, and Territorial (SLTT) space have used migration to a cloud-based endpoint protection platform as the basis for such transformations/initiatives.

Identity

In our view and as noted above, this section is one of the most central elements of the ZTA journey. The Model's stated intent is to enable minor advancements such that they "can be made over time toward optimization," and it appears to avoid prioritizing or sequencing steps. That said, arriving at the "optimal" state for authentication ("Agency continuously validates identity, not just when access is initially granted") would clearly have a substantial impact on the journey. We would add that authentication challenges premised on risk-based conditional access can have the desired impact while minimizing friction for permissioned users.

In addition, ZTA is meant to drive and increase resiliency, especially against a capable cyber adversary. We encourage redundancy in the Identity Provider (IdP)-layer, to ensure resilience and ability to operate if a given service is disabled or temporarily terminated. Solutions which can support multiple Identity providers, measure risk across the multiple IdP layers, can enable a true, end-to-end

risk-based and quantifiable outcome regarding the confidence and trustworthiness of a credential--regardless of whether it is for a user, service, or application.

Device

This section represents the other most essential set of criteria to strengthen ZTA, from our perspective. In general, we recommend that the "optimal" state of each element specifically guide Departments and Agencies toward "real-time" capabilities. At present, some categories do not specify frequency, and others use softer requirements ("constantly," or "continuously").

This section is practical and forward-looking in its treatment of devices. The inclusion here of Bring Your Own Device (BYOD) and Internet of Things (IoT) concepts is a practical way to ensure this guidance stays relevant as large enterprises adapt to these conditions. We believe that, from a maturity perspective, at least some attention should also be paid toward the elimination of legacy, on-premise type of systems and devices, including security devices, that introduce additional attack surface and frequently lack the capability to operate with other controls specified in this document. (We did note and agree with the statement: "[l]egacy infrastructure and systems may not support a zero trust implementation," in the 'assumptions and constraints' disclaimer. However, this is why we believe it's appropriate to emphasize the importance of depreciating such assets in this section.)

While EDR tools are referenced in the 'Visibility and Analytics Capability' category, we note that best-in-class EDR tools can enable or promote the optimal case in several other categories, as well as each of the elements in this section of CISA's tentative, forthcoming offerings.

Modern EDR tools also have unparalleled visibility of credential use and credential exposure on a resource. Almost all recent cyber attacks include the compromise of a credential on an already compromised resource. It is important to link and fuse signals from device security to that of the identity plane for comprehensive visibility of the full lifecycle of a credential. If an EDR tool can detect the compromise of a device, all credentials in-memory at that time should be deemed compromised, or at least assigned a lower trust-score unless or until the integrity of that credential can be verified.

Networks/Environment

The elements specified in this section can also contribute to Departments and Agencies ZTA journey. From our perspective, threat protection plays an essential role. We would caution however that this capability is not confined or constrained in any way to network-centric depictions. Some of the richest and most granular views of threat activity are only available on devices or endpoints (discussed above) and cloud workloads (described below). This distinction becomes clearer over time, as networks further "dissolve" into cloud, mobile, and BYOD environments, and HTTPS is deployed ever more broadly.

Application Workload

We strongly endorse the concept of threat protection within workloads, and support the guidance provided in this section. In the spirit of Zero Trust, before a user authenticates and potentially exposes their own credential to an application, the application's trustworthiness should be measured. An important use-case for ZTA is to prevent the exposure of a trusted identity from a trusted device being exposed to a compromised or untrusted application. This use-case should be considered for applications both in the cloud as well as on-premises.

Data

Subject to the points we raised in the *Front Matter* section above regarding the role of data security within ZTA, we agree with the objectives articulated here.

III. CONCLUSION

We commend the Model's authors and contributors for developing a thoughtful approach to gauging Department and Agency maturity in their ZTA journey. This, in combination with the Federal Strategy and Cloud Security Reference Architecture, will also serve as a helpful reference to large enterprises seeking to implement or adopt Zero Trust principles.

IV. ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®,

CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Robert Sheldon
Director, Public Policy & Strategy

Email: policy@crowdstrike.com

***