REQUEST FOR COMMENT RESPONSE

Federal Zero Trust Strategy

21 September, 2021

I. INTRODUCTION

In response to OMB's request for comment on its Federal Zero Trust Strategy, 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.

II. COMMENTS

We agree strongly with the need for the Federal Government to adopt Zero Trust principles as described in E.O. 14028, "Improving the Nation's Cybersecurity" and as outlined in this Federal Zero Trust Strategy. In general, we view the Strategy as a well-conceived, thoughtful approach to a difficult and complex problem. Accordingly, our feedback is narrow in scope. We offer it below on a section-by-section-basis.

Purpose

While the portion of the document that follows "*This strategy envisions a Federal zero trust architecture that…*" captures several of the Strategy's primary themes, it leaves others out. The section could be strengthened by:

- Adding a bullet that focuses on a need for a more robust approach to identity and authentication.
- Modifying the bullet that reads "*Relies on encryption and application testing instead of perimeter security*," to say "*Relies on the defense of applications,*

> *endpoints, workloads, and identity, as well as the broader use of encryption instead of perimeter security.*"

Goals

We agree with the goals outlined in this Strategy. E.O. 14028 rightfully grouped Zero Trust, universal logging, stronger asset inventories, and enhanced detection and response as a basket of complementary reforms, and we agree with the extension of that paradigm here. We share perspectives on each of these individual topics below.

Of note, this section guides Federal IT leaders to "*assume networks and other components will be compromised.*" We agree with this sentiment but encourage readers to further operate from an assumption of breach. That is, assuming that an enterprise is *actively* breached, not that it will be breached at some future point. This assumption clarifies the need for an active adversary hunting program, as well as the value of the "1-10-60 Rule."[1]

The Strategy notes that "*agencies are broadly expected to continue increasing their use of cloud infrastructure and associated security services,*" and indeed E.O. 14028 emphasizes the need for Departments and Agencies to favor SaaS, PaaS, and IaaS systems. However, we view the Strategy as a good opportunity for OMB to position a cloud-first approach as a more formal requirement across the ".gov."

Identity

This section of the Strategy is critical, and we believe it can be strengthened by integrating three emerging and related concepts. These include the need to:

- **Use risk-based conditional access to trigger MFA only when required to achieve the true "never trust" ethos of Zero Trust.**[2] On the one hand, this

[1] For more detail on the need to hunt and the evolution of the 1-10-60 Rule, *See* Mike Sentonas, "Vendor Hype Gives New Meaning to the Term 'Zero Trust Security' (And Not in a Good Way)," CrowdStrike Blog, August 31, 2021. https://www.crowdstrike.com/blog/vendor-hype-gives-new-meaning-to-zero-trust-security/.

[2] As we suggested to NIST earlier this year, "One aspect of ZTA that bears consideration is emerging tools that can dynamically identify anomalous behavior within a permitted session, and respond by policy. This is an important capability in light of identity-based attacks that, for example, abuse legitimate credentials. The policy may default to blocking or another action, such as imposing a multifactor authentication (MFA) challenge to the user. Flexibility is important here to adjust for different use cases and threat models. Notably, one particularly promising use case is the ability to set policies on the basis of a dynamically generated score, which may incorporate aspects like resource sensitivity, user behavioral cues, or aggregate threat activity across an enterprise." *See* Section 1.1.3. III. CrowdStrike RFC Response, NIST: *Planning for a Zero Trust Architecture*: A *Starting Guide for Administrators*. September, 3, 2021.

can reduce friction for low risk, permitted use. On the other hand, this can radically increase barriers against unpermitted use, to include dynamically presenting suspicious users/uses with a new MFA challenge within a permitted session.

- **Extend identity requirements even to unmanaged systems or legacy systems that cannot typically use MFA.** By monitoring and using credentials (including SSO) tied to users and applications of those systems that can directly force an MFA, a risk based conditional access model can be setup to examine behavioral signals of identities (in real-time) at the identity store and determine anomalous activity that may require an MFA to be triggered by the monitoring system.
- **Enforce the principle of least privilege at the identity-level**. Least privilege seeks to limit the scope of any system, effectively limiting the impact (or "blast radius") of a breach. Identity based segmentation monitors a user or application by the use of its credential, which is not based on the physical location or deployment model.[3] This can include where and how the credential is used, behavioral usage analysis, and other factors.

With respect to coverage, the Strategy clarifies that certain MFA requirements extend to staff, contractors, partners, and public users. We believe the Strategy should further or more explicitly mandate such coverage for privileged users and service accounts (e.g., non-human accounts), which in practice frequently fall outside of such controls and are increasingly abused by threat actors. This is especially important when factoring in legacy devices that remain in use despite IT modernization initiatives.

While these points apply across the "Identity" section of the Strategy, they apply directly to the accurate characterization of current Department and Agency challenges within the "1. *Enterprise-wide identity*" subsection. ("As *agencies adopt cloud-based infrastructure and applications, they must ensure the same level of strong authentication across various platforms. The more separate account systems an agency operates, the more challenging it is to implement strong authentication across the enterprise, and the higher the burden on agency staff to manage credentials across the various applications they need to use for their jobs. The simplest way for a Federal agency to address these challenges is to support a single well-designed authentication system, and to integrate it into as many applications as possible throughout the agency.*")

[3] Traditional models of enforcing least privilege utilize network based segmentation, which relies upon limiting the application or user by IP address, domains, router rules (eg. ACLs), port communication, and other methods. Since most modern IT environments are hybrid and dynamic (and are not trivial to modify), these policy rules must be updated often and eventually fail to restrict the scope as a result.

The Strategy notes that "*[a]gencies should aim ultimately to use a single identity system that serves all internal users.*" Such a system could have certain positive attributes, notably simplicity of administration. However, persistent issues with architectures used today by some primary identity providers raise questions about whether a more federated, community-driven approach to identity would offer more robust security.[4] From our perspective, universal security management of identity is the real priority--not a singular identity platform per se. The essential requirement for robust identity is visibility across:

- All credentials (users, privileged users, service accounts, etc.);
- Credential attack path/scope across all infrastructure (cloud, on-premise, etc.);
- Credential usage scenarios (including for example, Active Directory or SSO providers).

We agree with the need to strengthen identity hygiene. The Strategy directs CISA to "*make available to agencies one or more services to privately compare user passwords against known-weak and known-breached data, to help agencies protect against reused stolen credentials.*" To that, we would add the need for systems that identify not only weak or compromised passwords, but also stale accounts (i.e., those not used for a set period of time) which introduce unnecessary risks. Privileged accounts require special attention due to their scope and potential impact, as evidenced by several notable breaches over the past year.[5]

Devices

We agree strongly with the approach of utilizing Endpoint Detection and Response (EDR) capabilities as the backbone for device security--and by extension enterprise security--across the ".gov." We further agree that CISA must have access to this data to fulfill its federal cybersecurity mandate, and we note that this includes in particular its recently codified authorities to hunt across the extended Federal enterprise, as recommended by the U.S. Cyberspace Solarium Commission.

1. *Inventorying Assets*

[4] George Kurtz, Testimony on Cybersecurity and Supply Chain Threats, Senate Select Committee on Intelligence (Feb. 23, 2021), https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary.

[5] *See generally*, Andrew Harris, What SUNBURST Can Teach Government About Zero Trust (2021), https://www.crowdstrike.com/wp-content/uploads/2021/08/crowdstrike-gt21-qa-cyber-resilience-datasheet.pdf.

Accurate asset inventory is an important element of enterprise security. Notably, this is just one element of a broader model for IT hygiene, which can be enriched by additional information about the Operating System, users/accounts, usage, and applications (and by extension, vulnerabilities) associated with each particular asset. A best-in-class Endpoint Protection Platform solution should deliver these capabilities in tandem with EDR, enabling security operators to pivot between depictions of the defended IT environment.

Further, for any degree of precision, an asset inventory must be based on dynamic/real-time data about device status. Periodic "scans" that provide point-in-time snapshots may be useful for certain use cases (e.g., software usage/licensing matters), but they are insufficient for hunting operations and incident responses. While we acknowledge the importance the Strategy attaches to the CDM program, we note that these attributes are uneven across current CDM portfolio solutions and may yield dated or inaccurate results at the CDM dashboard-level.

2. *Government-wide endpoint detection and response*

We appreciate the concept of the operations[6] that this Strategy provides for operationalizing the EDR requirement articulated within E.O. 14028. We believe that the most straightforward way to achieve an operating picture for CISA is to ensure that to the extent possible, EDR solutions are cloud-native, rather than merely cloud hosted,[7] in order to:

- Achieve the scale required by the formidable size of the ".gov.";
- Enable CISA to evolve machine event data and log collection retention expectations either dynamically (e.g., in response to an incident or event) or by policy over time in response to new requirements, using cloud-based storage;
- Leverage native APIs to:

[6] *"To ensure government-wide EDR coverage, agencies must ensure strong EDR tools are deployed across their agency. Agencies with robust EDR tools in place will continue to operate those tools, while agencies that lack them will work with CISA to procure them. To enable government-wide incident response, agencies must establish information sharing capabilities with CISA, implemented in accordance with upcoming OMB guidance."*

"Agencies should anticipate establishing procedures and technical facilities to make information reported from their EDR tools available to CISA. This approach is intended to maintain a diversity of different EDR tools throughout the government that can support agencies in differing technological environments, while ensuring a baseline of insight into activity across the Federal civilian government."

[7] The fact that a solution is hosted in the cloud does not in and of itself mean that it incorporates or confers the benefits of cloud-native technologies.

  - integrate EDR data from multiple tenants within the same Department/Agency, across multiple Department/Agency-level users from the same vendor, and across different vendors; and
  - enable at-scale, API-based response and remediation actions.
- Train AI/ML models for more precise detection/prevention actions on devices and beyond;
- Store machine event data and logs off-host and off-premise to prevent adversary manipulation or deletion.

These are fundamental requirements to achieve the vision for EDR described in both E.O. 14028 and the Strategy. Beyond these core issues, cloud-based solutions also comport with the importance attached to *as-a-Service* solutions in the E.O., and better comport with the shared services acquisition models favored by recent plans for modernizing government technology broadly. Further, they are most straightforward to update, operate, and maintain, and they reduce on-premise attack surface,[8] which adversaries exploit frequently, and in several recent, high-profile campaigns targeting the ".gov." effectively.

Networks

We agree with the vision and action items described in this section.

Applications

We agree with the vision and action items described in this section.

Data

We agree with the approach on strengthening cloud security generally, and leveraging cloud security specifically to assist in protecting sensitive data. As noted, the role of enterprise-wide logging capabilities is crucial here, and underscores industry's acceleration of the Extended Detection and Response (XDR), Security Orchestration, Automation, and Response (SOAR), and Observability spaces. Capabilities in these areas have developed considerably in recent years and we anticipate that this evolution will continue. The most important requirement therefore is for Departments and Agencies to acquire solutions and design architectures that can adapt to new conditions or meet emerging requirements.

[8] *See* Software Bill of Materials Elements and Considerations, NTIA, (June 6, 2021), https://www.federalregister.gov/documents/2021/06/02/2021-11592/software-bill-of-materials-elements-and-considerations. We note that the NTIA Software *Bill of Materials Elements and Considerations* document identifies on-premise software as the first and highest priority area for SBOM development. We agree with this approach; CrowdStrike's RFC response to NTIA (June 17, 2021).

From our point of view, the current, fundamental cybersecurity requirements include: maintaining visibility across the entire enterprise (including for identity) and at an exceptionally granular level at the individual endpoint level; the ability to secure workloads across the federated enterprise, both on endpoints and within the cloud; and the ability to monitor, log, and maintain an adversary hunting regime across these spaces. This informs the increasing importance we attach to robust and flexible XDR-type solutions in particular. Components of this strategy support a future that evolves into more formal requirements for these sorts of solutions across the ".gov."

III. CONCLUSION

We believe the Strategy represents a critical step forward for the ".gov's" Zero Trust journey, and we appreciate the opportunity to review the document. Several of the suggestions and amplifications we've offered above, if adopted, may strengthen it further. We would welcome the opportunity to expand on these matters, provide additional references/examples, or, to the extent that it is helpful, discuss them further with OMB or relevant Departments and Agencies. Recognizing the alignment between these initiatives, we will submit additional comments and feedback on CISA's Zero Trust Maturity Model and Cloud Security Reference Architecture.

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

©2021 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are trademarks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.

***