CROWDSTRIKE

REQUEST FOR COMMENT RESPONSE

Cloud Security Technical Reference Architecture

1 October, 2021

I. INTRODUCTION

In response to CISA, USDS, and FedRAMP's request for comment on their Cloud Security Technical Reference Architecture, 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 hunting, 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 find this document (hereafter "the Architecture") to be a thoughtful approach to the urgent requirement of strengthening federal cybersecurity. We share CISA's view that increasing the usage of a cloud-based shared services approach to IT is the best way to do this effectively. The transformation from legacy to more modern approaches should be managed carefully, while decreasing total cost of ownership while raising the security posture of the government. We offer several discrete pieces of feedback below on a section-by-section basis.

1. & 2. Front Matter

We strongly support the emphasis within Executive Order (E.O.) 14028 on the extension of cloud services across the ".gov," and the specific orientation toward "as-a-Service" consumption models. We believe that the deprecation of legacy technologies and systems provides a security end in its own right, and that the process presents opportunities to further strengthen Department and Agency security posture during and throughout the transition. This reference architecture provides helpful guidance toward these outcomes.

3. Shared Services Layer

The Architecture notes that "*[a]gencies are likely to operate in a multi-cloud environment where they consume one or more SaaS offerings and one or more PaaS or IaaS offerings. Agencies operating in a multi-cloud environment need to plan for how they can optimize their use of multi-cloud environments while maintaining situational awareness and proper security practices in each CSP they operate within. Agencies can choose to protect each of these services as an entity on its own or they may decide to maintain a holistic view of their security posture for all the services they consume*." We would strongly encourage Departments and Agencies to maintain a holistic and real-time view of their security posture across their digital estates, from legacy systems and on-premises endpoints to their multi-cloud environments. This is by far the best way to fully understand the threat environment and manage it effectively. It also promotes holistic and comprehensive threat hunting and incident response activities, as necessary.

4. Cloud Migration

With respect to the principle of least privilege (as discussed in section 4.4.4), we advocate for enforcement at the identity-level.[1] 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, service or application ("non-human") by the use of its credential, which is not based on the physical location or deployment model. This can include where the credential is used, behavioral usage analysis, and other factors.

Traditional models of enforcing least privilege utilize network based segmentation, which relies upon limiting the application or user by IP address, domains, router rules (e.g., 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.

We strongly agree with the need to further centralize security services within the ".gov" space, as described in Section 4.5.3. We note that a centralized approach is the best way to achieve scale and enables the shared services approach to acquisition and delivery, as described elsewhere in this document. Beyond the identity use case referenced in this section (and Cloud Security Posture Management, referenced below), we note that this approach is appropriate for threat intelligence, threat hunting, Endpoint Detection and Response, and hygiene,

[1] This section draws on CrowdStrike's RFC response to OMB's Federal Zero Trust Strategy (21 September 2021).

among other areas. In addition, this centralization prevents "data silos," enabling multiple teams to operate with the same data and tools, which in turn significantly reduces the total cost of ownership.

5. Cloud Security Posture Management

We agree with this description in general and this assertion in particular: "CSPM *supports continuous improvement of an agency's cybersecurity posture, and capabilities to enable agencies to keep up with emerging threats, protect against misconfigurations, and reduce the risk of a security incident or data breach.*" A key point we would highlight (from Section 5.1.2) is that Departments and Agencies should "consider cloud-native products for application delivery." We think this is a key criteria, particularly in the security space where some legacy, on-premise applications are shifted to cloud for delivery, but because of their architecture never truly attain cloudscale visibility and performance.

III. CONCLUSION

CrowdStrike agrees with the approach advanced by the Cloud Security Technical Reference Architecture. Cloud-based technologies help increase innovation in our nation's toughest cybersecurity problems, applying cutting-edge machine learning, applied both on-device and in the cloud. The model outlined here will strengthen security outcomes in hybrid multi-cloud environments, across federated teams and organizations, increasing security, increasing situational awareness and operational capability, while reducing cost and time to operate and defend assets.

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

***