Broadcom and Symantec (A Division of Broadcom) Position Paper on Standards and Guidelines to Enhance Software Supply Chain Security

Issue # 3: *Guidelines outlining security measures that shall be applied to the federal government's use of critical software*

Author: Timothy Balog
Title: Regional Technology Officer, Federal Sales
Email: timothy.balog@broadcom.com

Many of the policies, processes and technologies that Broadcom recommends be used for critical software are already documented in existing NIST, OMB, DHS, and DOD standards, guidelines, procedures, etc. Thus, our primary recommendation is to ensure that adherence to existing requirements is inspected, and where an organization is not in compliance, measures are taken and resources are applied to bring the organization into compliance. Broadcom recommends further emphasis be placed in the following key areas regarding the use of critical software within the federal government:

Ensure that systems used to **identify, authenticate, and authorize users (FICAM systems)** are themselves secured as they are key to all other effective policy management. Strict control over administrative access and privileged user controls must be in place.

Ensure that **any system level account** associated with tools that are **granted privileges to update infrastructure** are reviewed and their scope confirmed regularly just as individual users are. Wherever possible these tasks should make use of a credential vault, not static credentials to run.

Ensure **privileged users** who interact with any infrastructure software **are challenged out of band**, even where a smartcard was the primary factor. With the proliferation of smartphones, and the ability to issue push notifications to users, this can be implemented with minimal impact on the user experience.

Ensure that the handling of **session data is limited to trusted devices** and that zoning is applied to limit the use of a session across boundaries, especially for users with privileged access. This is especially critical anywhere existing sessions are allowed access without being subject to a unique authentication step (SSO tools, Apps that are "integrated with AD", etc.).

Record and store the actions of privileged users within the enterprise to assist in determining the extent of breaches involving privileged access. Record privileged access sessions for enhanced visibility and post-breach response. Recorded sessions help determine the extent of a compromise.

Employ **user behavior monitoring** and **multi-factor authentication** for all access to critical software.

Employ **API management tools** to secure applications as microservices and APIs become more prevalent due to the increasing adoption of DevSecOps.

Employ **API gateway technology** to connect systems and apply consistent security and governance to agency APIs across any combination of cloud, container or on-premises environments.

Employ only endpoint security tools that include **tamper protection** that prohibits users or scripts from maliciously or inadvertently modifying, disabling, or removing security settings.

Employ **Active Directory defense** tools on endpoints that disrupt domain reconnaissance activity, detect an attacker that attempts lateral movement or credential theft, and mitigate intrusion by operations, users or endpoints by reducing the exploitation of Active Directory.

Ensure endpoint protection tools provide **proactive defense mechanisms** that include real-time application isolation and control capabilities that allow only known good applications to run, shield known-good applications to prevent attackers from exploiting application vulnerabilities, and isolate unknown and untrusted applications.

Employ endpoint protection tools with **behavioral application isolation** capabilities that reduce the attack surface by specifying how to handle suspicious behaviors performed by trusted applications.

Employ **web isolation technologies** to prevent websites from delivering zero-day malware and phishing threats to users' devices by executing web sessions in a remote virtual isolation environment that sends only safe rendering information to web browsers.

Employ **software defined perimeter** technology based on zero trust principles that cloaks all corporate resources on the network and fully isolates datacenters from the end-users and the internet to prevent lateral movement and network-based threats.

Employ **reverse proxy technologies** to protect critical web applications by providing a termination point where deep inspection for malware and mission-critical policy is applied to inbound traffic. Ensure the reverse web proxy can govern traffic and payloads on a wide variety of parameters, including location, devices, clients, software, protocols, and more.

Employ **mirror gateway** technology to enforce controls over the use of sanctioned cloud apps on unmanaged endpoint devices. Use mirror gateway technology to eliminate the risk of users uploading sensitive information to websites or downloading malicious code to unmanaged endpoints.

Employ **secure web gateway** and **cloud access security broker** technologies to control and audit user access to web sites and IaaS, PaaS and SaaS platforms.

Employ **data loss prevention** tools to prevent malicious, accidental, intentional and unintentional exfiltration of data and source code. Use data loss prevention tools to locate where critical software and source code is located (on endpoints, physical storage devices, cloud storage repositories) and control exfiltration to unauthorized individuals or locations.

Segregate the network and do not have a flat infrastructure.

Do not dual home servers from one segment to another.

Monitor the flow of server-server and human-server interactions, looking for new patterns.