Quokka

Whitepaper

Zero Trust Architecture:

Mobile Application and Device Security for Federal Agencies

Zero Trust is a security paradigm many organizations have adopted to enhance their mobile security. It is an approach to network and information security that assumes that any connected system cannot be trusted.

In Zero Trust, every endpoint on the network is considered untrusted, and all users are treated as adversaries who might try to exploit the organization's resources. This means that all users must prove their identity before accessing protected resources, and once they have done so, they are only given the rights they need to do their job. This is known as a problem-solving approach, which reduces the number of false positives. Zero Trust examines users' motives and intentions rather than their actions.

This enables organizations to be more proactive with security while reducing the need for manpower. The Zero Trust model allows organizations to provide consistent protection for their resources; this includes everything from corporate-owned personnel-enabled mobile devices to laptops, tablets, and any other device that may connect to the network.

Federal Agencies' Adoption of Zero Trust Architecture

In alignment with Executive Order 14028, "Improving the Nation's Cybersecurity," the recently released Federal Zero Trust Strategy from the Office of Management and Budget provides agencies with a strategy for moving to a Zero Trust architecture and adjusting to new technologies and practices.

This hyper-focused solution to cybersecurity also requires a detailed look into how mobile devices and their applications can be used as exploitable touchpoints in the network and the security assurances needed to mitigate these risks in the rush to add new features that attract users and enhance the user experience.

If these apps are attacked, sensitive personally identifiable information (PII) and digital identity data are at risk.

Three Characteristics of a Zero Trust Architecture:

Microsegmentation: As defined by TechTarget, microsegmentation breaks down the network into definable zones with specific access policies and barriers to entry. Microsegementation is defined at the software level, unlike standard network segmentation, which focuses on hardware segmenting. Microsegmentation allows network administrators to silo and create subnetworks based on application, tier, environmental, or user policies.

Zero Trust Network Access: According to Gartner, Zero Trust Network Access (ZTNA) creates identity and context-based access controls around an application or set of applications. Access to these applications, even seeing them in an available application list, is hidden via a trust broker. Trust brokers validate user identity against established policy and access settings and, when confirmed, allow users to access this application while prohibiting lateral movement throughout the network.

Security Configuration and Posture: An essential component of Zero Trust is confirming not only the identity of the user and/or the device but also the security configuration and posture of each device used to access the services. Different devices have various requirements and definitions of security—a personal computer's security requirements are very different from a mobile phone, which is also very different from a smartwatch—although all three can be used to access the same service, such as email.

Redefining the Conventional Security Perimeter to Include Mobile Applications

Mobile device usage is not going to slow down anytime soon. The use of mobile devices—tablets, phones, and wearables—has increased the ability of employees to connect to work-related applications from anywhere at any time. What does this mean for federal agencies with personnel who need to access data-sensitive information while working from home or quickly respond to an email on the go?

Many network security professionals agree that mobile device manufacturers have implemented security measures that align with the principles of a Zero Trust architecture. Features such as sandboxing, segmentation, or secure memory management provide a solid foundation for device security. However, as noted in a recent Cybersecurity and Infrastructure Security Agency (CISA) document, "Applying Zero Trust to Enterprise Mobility," there is a critical need to review mobile application security and exploitable vulnerabilities lurking in commonly used or essential mobile apps.

Deploying a Mobile Application Vetting (MAV) security testing process will allow security professionals to scan publicly available applications before deployment on approved Corporate Owned Personnel Enabled (COPE) devices. This application security testing will give network administrators and security teams insights into exploitable risks lurking undetected in an application. These tests can also help developers and those responsible for the apps address these risks promptly and ensure that when any federal agency uses them, they meet the most stringent security requirements.

Best Practices for Integrating Mobile Application Security into a Zero Trust Architecture

As network administrators and IT teams set the parameters for a Zero Trust architecture within their agency and organization, there are some best practices they should follow:

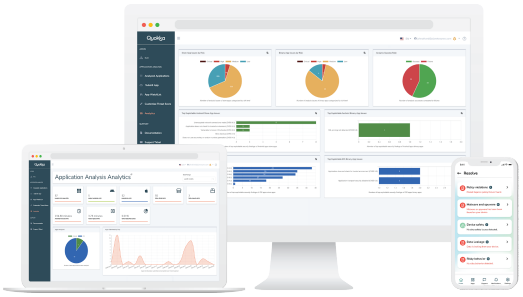
- Validate that mobile apps used in your environment meet your policies for risk acceptance before deploying or allowing use. There should be a high security emphasis on apps installed on personnel devices that have access to potentially sensitive organization data or that may handle sensitive information. The risk acceptance for these applications may differ from other apps, such as a calendar or daily planner, if it is not connected to an internal system.

- Validate that mobile devices used by personnel may be trusted and meet policies for risk acceptance continuously and on every login to access business resources. Validation should include the following:
  - Risk analysis of third-party (app store) applications installed by the device owner.
  - System applications (firmware).
  - Analysis of apps colluding on the device.

- Automatically enforce and remediate violations of policies on mobile devices. Don't rely on IT/security staff action to initiate enforcement or communicate with the affected party. Violations should revoke access to business data from that device until they are corrected.

Quokka Solutions for Mobile Application Security in a Zero Trust Architecture

Addressing public sector mobile security needs across federal, state, and local governments is what we built Quokka (formerly Kryptowire) was built on. Our company mission was kicked off and funded by the Defense Advanced Research Projects Agency (DARPA) to identify, reduce, and eliminate security vulnerabilities associated with mobile apps. With the intelligence Quokka provides, government agencies and civilians can better understand the mobile threat and risk associated with their third-party apps.



Q-Vet: Mobile Application Vetting

Continuously ranking #1 in government and lab evaluations, Quokka's Mobile Application vetting solution, Q-Vet, evaluates security and privacy risks associated with mobile apps, uncovering more vulnerabilities and ensuring compliance across all branches of government.

Agencies and Organizations leverage Q-Vet to continuously assess the security and privacy of mobile apps against the highest internationally recognized software assurance standards published by the National Institute of Standards and Technologies (NIST), National Information Assurance Partnership (NIAP), and Open Web Application Security Project (OWASP).

In a Zero Trust architecture, Q-Vet enables agencies to test and validate apps that are added to their approved mobile devices. Ensuring mobile apps are credible and meet the organization's Zero Trust policies before being added to authorized devices is critical to ensure the device and the data handled by the app is open to an exploitable risk after the addition of the app into the infrastructure.

Q-MAST: Mobile Application Security Testing

In addition to Q-Vet, Quokka provides a mobile application security testing solution, Q-MAST, to assist agencies in developing their own apps. Using Q-MAST, agency developers can ensure that these apps are Zero Trust ready and meet other supply chain requirements. By providing a software Bill of Materials and testing all third-party code included in their application, organizations can establish trust in the software added to their app.

Q-Scout: Fleet-wide Device Security

Q-Scout is an intelligent, proactive security solution that safeguards the agency or organization and all of your personnel, with personal privacy at its core.

Q-Scout helps enable Zero Trust in the mobile space by solving a critical problem, determining if an end-user mobile device can be trusted to access corporate resources. With Q-Scout, proactive remediation is gained by performing an in-depth assessment of the device, applications, and configuration prior to an active risk and then adjusting the configuration or trust level to prevent the risk from materializing.

Solutions like Mobile Device Management and Identity Providers can control access to an account from a device but do not have the intelligence to determine whether the device can be trusted. Q-Scout gives your existing architecture the security intelligence and automation to enforce Zero Trust on every login from every mobile device. Additionally, Q-Scout can provide Zero Trust enforcement based on the organization's own Zero Trust policies to apply them automatically.