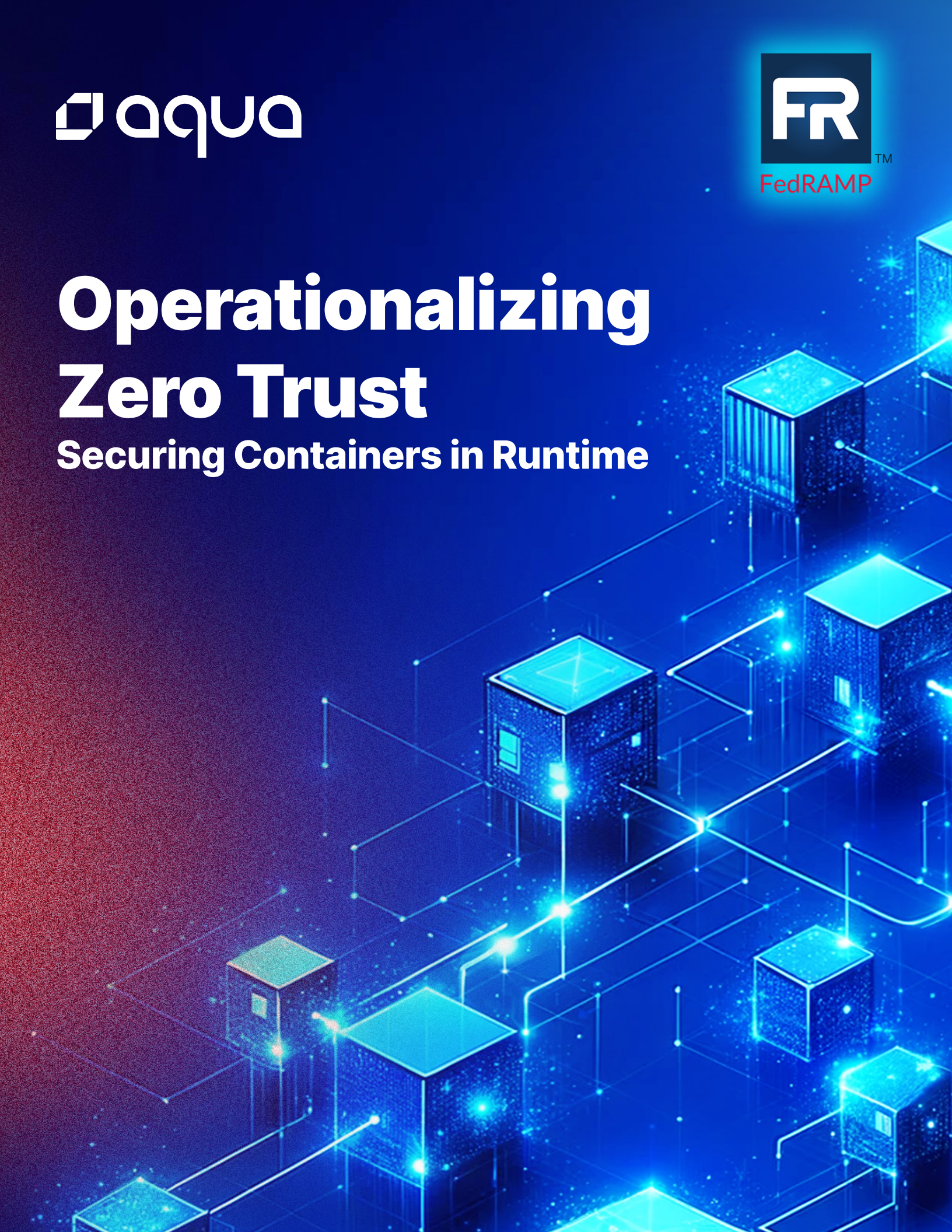
aqua

FedRAMP™

Operationalizing Zero Trust

Securing Containers in Runtime



Beyond the Perimeter:
Implementing Zero Trust for Enhanced Security

Zero Trust is a security model that has gained significant traction in recent years, particularly among federal agencies and organizations dealing with secret, confidential and sensitive data. At its core, Zero Trust is based on the principle of "never trust, always verify," which means that no user, device, application or network traffic is inherently trusted, and every access request must be authenticated and authorized before being granted. Policies should be enforced, and actions operationalized.

However, implementing Zero Trust is not just about adopting a new security philosophy; it's about operationalizing these principles in practical, actionable ways. Operationalizing Zero Trust means translating the high-level concepts into specific security controls, policies, and processes that can be implemented across an organization's IT infrastructure and workflows.

For example, consider the principle of "never trust, always verify" from the perspective of a developer working on a new application. Operationalizing this principle might involve implementing 'parameterized validation', which means that all input data is treated as untrusted and must be validated against a set of predefined criteria before being processed. This could include validating the data type, format, length, and range of values to ensure that it meets the expected requirements and does not contain any malicious or unexpected content.

Similarly, operationalizing Zero Trust in a cloud native environment might involve implementing granular access controls and network segmentation to ensure that only authorized users and services can access specific resources. This could include using role-based access control (RBAC) to define and enforce access policies based on a user's job function or level of privilege, as well as using network policies to restrict communication between different workloads and services.

At Aqua, we understand that operationalizing Zero Trust is not a one-size-fits-all proposition.
Each organization has its own unique security requirements, IT infrastructure, and business objectives, which means that the specific approach to operationalizing Zero Trust will vary depending on the context. However, by providing a clear definition and concrete examples of what operationalizing Zero Trust looks like in practice, we aim to help organizations bridge the gap between theory and implementation and achieve a more secure, resilient, and adaptive security posture.

In the following sections, we will explore some of the key challenges and opportunities associated with operationalizing Zero Trust in federal agencies, as well as how Aqua can help organizations achieve this goal in a cloud-native, containerized environment.

Zero Trust is important to Federal agencies for several reasons:

In the realm of federal government cybersecurity, the imperative for implementing Zero Trust principles arises from the ever-evolving landscape of digital threats and the criticality of safeguarding sensitive information. However, alongside this necessity lie multifaceted challenges that impede its seamless adoption. Federal agencies are confronted with many cybersecurity challenges as they strive to fortify their defenses and safeguard sensitive information, but embracing these Zero Trust principles offers a holistic solution to address these challenges effectively in runtime.

- **Zero Trust Monitoring**
  Federal agencies employ continuous monitoring to detect and prevent insider threats, adhering to Zero Trust principles.

- **Access Control Optimization**
  Agencies prioritize least privilege access, minimizing attack surfaces and enhancing security.

- **Data Encryption Focus**
  Emphasis on encryption for data protection at rest and in transit ensures comprehensive security.

- **Remote Access Security**
  Robust authentication and endpoint security measures secure remote access for employees and contractors.

- **Proactive Threat Defense**
  Zero Trust frameworks enable proactive threat detection and response to evolving cyber threats.

- **Adaptive Security Measures**
  Zero Trust's adaptive security model effectively combats advanced threats in dynamic environments.

Zero Trust offers federal agencies a comprehensive cybersecurity approach that prioritizes data protection, risk mitigation, and compliance, ultimately safeguarding critical assets and maintaining public trust but implementing zero trust has its challenges that must also be considered.

The challenges agencies face implementing Zero Trust

Federal agencies encounter an array of obstacles on the path to implementing Zero Trust principles, ranging from navigating legacy systems and infrastructure to addressing budget constraints and ingrained organizational cultures. Interoperability concerns, regulatory compliance, and complexities in data governance further compound the transition to a Zero Trust architecture. Despite these formidable challenges, federal agencies recognize that embracing Zero Trust is essential for enhancing cybersecurity resilience and protecting against emerging threats in an increasingly interconnected and dynamic digital landscape.

A strategic and holistic approach, involving collaboration between IT teams, cybersecurity experts, agency leadership, and external stakeholders is a starting place to address these Zero Trust issues. But federal agencies can enhance their cybersecurity resilience, protect critical assets, and maintain public trust in an increasingly digital and interconnected world by adopting tools that provide vigorous runtime protections.

Implementing Zero Trust with Aqua Security

Aqua Security helps organizations implement and operationalize the Zero Trust security model within their cloud native and containerized environments, enhancing their overall security posture and resilience against cyber threats.

Aqua's robust runtime protection monitors containerized and cloud native applications for suspicious activities and enforces security policies in real-time. This continuous verification of the security posture of applications and enforcement of policies is a core aspect of Zero Trust, ensuring that any deviation from the norm can be quickly detected and mitigated. By enforcing granular access controls and maintaining system integritythrough comprehensive monitoring and drift prevention, Aqua's runtime solution helps organizations operationalize Zero Trust.

Next generation runtime protection: Introducing eBPF Technology

Aqua's integration of eBPF (Extended Berkeley Packet Filter) is a testament to its commitment to upholding the principles of Zero Trust within cloud native environments. Zero Trust architectures require rigorous, continuous verification of activities at all levels, and the eBPF's advanced capabilities empower Aqua to reinforce these principles, especially within Kubernetes environments.

By utilizing eBPF, Aqua enhances its runtime protection, behavior analysis, and anomaly detection, providing a deeper level of insight and control that is critical for a Zero Trust approach. The granular visibility afforded by eBPF enables Aqua to meticulously monitor containerized workloads and swiftly respond to any sign of threat, which is paramount in a landscape where trust is never assumed. This proactive stance on threat management, characterized by early detection and mitigation, is a cornerstone of Zero Trust security.

With eBPF, Aqua utilizes eBPF programs and security policies at the kernel level, allowing for the safe execution of custom bytecode without the need for altering kernel source code or loading kernel modules. This method supports the dynamic and flexible enforcement of Zero Trust policies, facilitating the creation of a security posture that adapts to threats in real-time and maintains the rigorous standards required by Zero Trust environments. In essence, eBPF acts as a powerful ally in Aqua's arsenal, through Aqua's enhanced detection and response capabilities that align with the proactive, vigilant essence of Zero Trust.

Operationalize Zero Trust in Runtime with Aqua Security

By integrating Aqua's runtime protection, agencies can implement a robust Zero Trust framework that actively adapts to the evolving threat landscape, securing their cloud native applications against unauthorized access and sophisticated cyber threats. This ensures a proactive security posture, where every component and interaction within the system is continuously verified, aligning seamlessly with the overarching goals of the Zero Trust model to minimize risk and protect sensitive data. To architect towards Zero Trust with an "assume breach" approach, agencies should:

Adopt a Comprehensive Security Strategy

Utilize Aqua's full suite of runtime protection, drift prevention, and security controls to build a resilient defense against known and unknown threats.

Focus on Data Protection

Ensure data is secured, access is tightly controlled, and activity is monitored to protect against unauthorized access and exfiltration attempts.

Enforce Computational Access Control

Aqua's advanced policy enforcement capabilities go beyond traditional Identity and Access Management (IAM) paradigms, focusing on securing computational resources at a granular level. By strictly enforcing access permissions, Aqua ensures that every piece of code executes with the least privilege necessary, substantially reducing the workload's attack surface.
This is achieved by:

Resource Access Policies

Setting definitive policies that govern access to compute resources, ensuring that processes run with only the essential permissions they require, thus avoiding excess rights that could be exploited in the event of a breach.

UID/GID Enforcement

Assigning unique user IDs (UIDs) and group IDs (GIDs) to container processes to control access rights, segregating duties within the container environment and preventing unauthorized access or privilege escalation.

Immutable Security Stance

Adopting an immutable security model, where containers and their runtime environments are treated as unchangeable once deployed. Any attempt to alter the running state is automatically blocked, preserving the integrity of the workload.

Execution Prevention Controls

Utilizing execution prevention controls to restrict the ability to execute commands or access shell environments within running containers, thereby denying potential entry points for attackers.

Enforce Runtime

Leveraging runtime controls and adopting a Zero Trust architecture that assumes breach, organizations can significantly enhance their defense against zero-day exploits, live attacks, and insider threats.
This approach not only strengthens the security posture but also aligns with best practices for managing the complex security challenges presented by modern cloud and container environments.

Managing Risk in a Zero Trust Environment with Aqua

In a Zero Trust environment, the assumption is that threats can come from anywhere, and security is a continuous process. However, there are situations, such as pending patches for newly discovered vulnerabilities, where risk is inevitable. The period between the discovery of a vulnerability and the deployment of a fix is critical, as it leaves organizations exposed to potential exploits.

The Challenge of Inevitable Risk
Aqua's Mitigating Controls:

1. **Virtual Patching with vShield**
   Aqua's vShield offers a powerful mitigation tool by providing virtual patches to vulnerable applications or systems. This feature allows organizations to temporarily shield exposed vulnerabilities from being exploited, essentially creating a protective layer around the vulnerable code. Virtual patching is invaluable during the window between vulnerability discovery and the availability of a permanent patch.

2. **Restricting Access to Vulnerable Code**
   While awaiting a fix, Aqua can implement strict access controls to limit interactions with the vulnerable components. By leveraging Aqua's granular policy enforcement, access can be restricted only to essential operations, significantly reducing the risk of exploitation.

3. **Behavioral Anomaly Detection**
   Aqua's runtime protection capabilities include detecting behavioral anomalies that may indicate an attempt to exploit a known vulnerability. By closely monitoring for unusual activity patterns around the vulnerable areas, Aqua can provide early warnings of exploit attempts, enabling rapid response.

4. **Enhanced Monitoring and Logging**
   In a Zero Trust environment, maintaining detailed logs and continuous monitoring is key. Aqua's solutions enhance visibility into all activities, especially those targeting known vulnerabilities. This data is crucial for incident response and forensic analysis, helping organizations understand attack vectors and improve their defenses.

5. **Segmentation and Isolation**
   Utilizing Aqua's capabilities to segment networks and isolate sensitive workloads can prevent the spread of attacks. In cases where a vulnerability exists but cannot be immediately patched, isolating affected systems can limit the potential impact of an exploit.

By integrating these practices into a Zero Trust strategy, organizations can maintain a robust security posture, even in the face of unpatched vulnerabilities, aligning with the core Zero Trust principle of assuming breaches and minimizing trust.

Business Cases for Aqua's Zero-Trust Capabilities

Aqua Security's Zero Trust capabilities offer a compelling business case, especially for highly regulated industries and federal government agencies. Aqua provides organizations with the tools and frameworks necessary to implement this rigorous security approach within their cloud native environments. Aqua empowers highly regulated industries and federal government agencies to navigate the complexities of the modern cybersecurity landscape, making the operationalization of Zero Trust not just a strategic imperative but a tangible asset in the pursuit of digital transformation and security excellence.

Department of Defense (DoD) and the Criticality of Data:

- **Strategic Importance**
  For the DoD, safeguarding classified and sensitive data is paramount. The Department faces unique challenges in protecting data across highly distributed, dynamic, and multi-cloud environments, including the need to adhere to stringent security standards and regulations.

- **How Aqua can help**
  Aqua can play a crucial role in protecting DoD workloads across Kubernetes, containers, and cloud environments. By enforcing strict security policies, ensuring compliance with military-grade security standards, and providing real-time threat detection and response, Aqua helps secure the critical infrastructure and sensitive data that are vital to national security.

Aqua's Contribution to DoD's Vision

Following ongoing discussions with the Department of Defense (DoD), particularly the Navy, and insights on their security complexities, it's clear the DoD seeks and even requires a nuanced approach to cybersecurity that aligns with the mandated Zero Trust principles and supports a dynamic, interoperable DevSecOps environment. This necessitates a reference architecture that integrates OCI and CNCF principles with stringent security controls, facilitating secure, reusable, and agile application development across diverse Kubernetes platforms.
Aqua is well-positioned to aid the DoD in realizing this sophisticated cybersecurity infrastructure.
Our solutions offer:

- **Early Security Integration**
  Aqua ensures security is embedded from the outset of the development cycle, aligning with 'shift left' practices and complying with NIST and STIG requirements.

- **Uniform Security Across Environments**
  Our platform maintains consistent security management across Kubernetes orchestrators, crucial for the DoD's develop-once-deploy-anywhere strategy.

- **Streamlined RMF and cATO Processes**
  Aqua's security capabilities support RMF compliance and cATO attainment, providing essential documentation and monitoring for operational security.

- **Facilitating Secure Application Development**
  By adhering to OCI and CNCF guidelines and DoD security standards, Aqua enables the development of a DevSecOps reference architecture that promotes security, efficiency, and interoperability across the DoD ecosystem.

In essence, Aqua can significantly contribute to the DoD's efforts to navigate the complexities of a Zero Trust architecture, ensuring secure, compliant, and efficient application development and deployment across its digital landscape.

Banking Industry / Financial Services and Confidential Computing:

Strategic Importance

The banking sector faces increasing cyber threats, stringent regulatory requirements, and the need to protect highly sensitive customer data. Confidential computing emerges as a solution to secure data in use, providing an additional layer of protection and ensuring data privacy and integrity during processing.

How Aqua can help

Aqua can enhance the security posture of banking institutions by offering solutions that support confidential computing environments. By integrating and enforcing security policies that protect workloads during execution, Aqua helps banks mitigate risks, comply with financial regulations, and safeguard customer data against unauthorized access and leaks.

The applicability of Aqua's solutions extends across various critical sectors, each with unique security challenges and requirements. By addressing the specific needs of the U.S. government in response to EO 14028, protecting the DoD's critical data infrastructure, and securing sensitive financial transactions in the banking industry through confidential computing, Aqua demonstrates its capability to provide robust, flexible, and compliant security solutions. These business cases illustrate the importance of adopting advanced security measures, such as those offered by Aqua, to protect against sophisticated cyber threats, ensure regulatory compliance, and safeguard critical data across diverse and challenging environments.

Conclusion

The journey towards a fully realized Zero Trust architecture is both complex and demanding. Yet, with Aqua Security, organizations have a clear pathway to success, supported by innovative solutions that address the unique challenges of securing cloud-native ecosystems. As we look to the future, the role of solutions like Aqua in enabling Zero Trust environments will undoubtedly grow, highlighting the importance of adopting such comprehensive security strategies in today's digital world.