Advancing Zero Trust Cybersecurity in Government

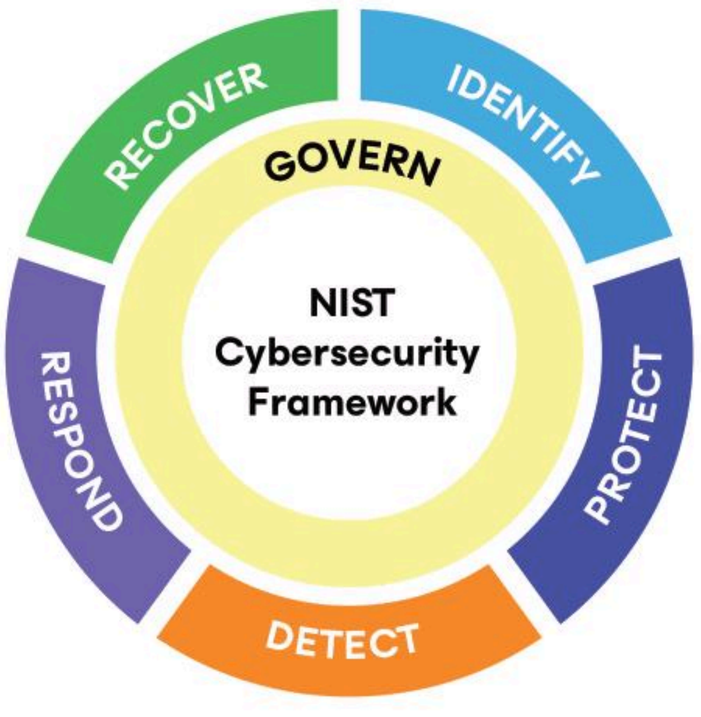
Veeam Kasten: Secure by Design

With Veeam Kasten, teams can achieve radical resilience against ransomware attacks. Our solution provides Kubernetes-native data protection that enables seamless backup and restore, disaster recovery (DR), and application mobility for Kubernetes applications at-scale. Veeam Kasten *for Kubernetes* software is secure by design, and as a cloud-native application, embodies the concept of zero trust. Kasten features also align with NIST 800-207 and FIPS 140-3 standards for data protection and Executive Order 14208 requirements for securing the software supply chain. Kasten's advanced platform delivers the following:

- **Enhanced Data Protection:** With FIPS 140-3 encryption, immutable backups, and air-gapped installations, Kasten shields data from external threats and unauthorized alterations.
- **Policy Enforcement:** Micro-segmentation and policy management tools such as OPA and Kyverno provide effective compliance.
- **Access Management:** External IAMs, role-based Access Control (RBAC), and diverse authentication protocols continuously vet user access at granular levels.
- **Secure Software Development:** Integration with Iron Bank container security and its Software Bill of Materials (SBOM) enhance tracking and risk management throughout the software development lifecycle (SDLC). Veeam Kasten images are also available from the USAF IronBank.
- **Continuous Monitoring:** Use Kasten with tools like Prometheus and Grafana, along with other SIEM systems, for proactive compliance, anomaly detection, and incident response. Audit logs from Kubernetes APIs and Kasten extended logs are available, but being cloud native, there are many built-in logs.

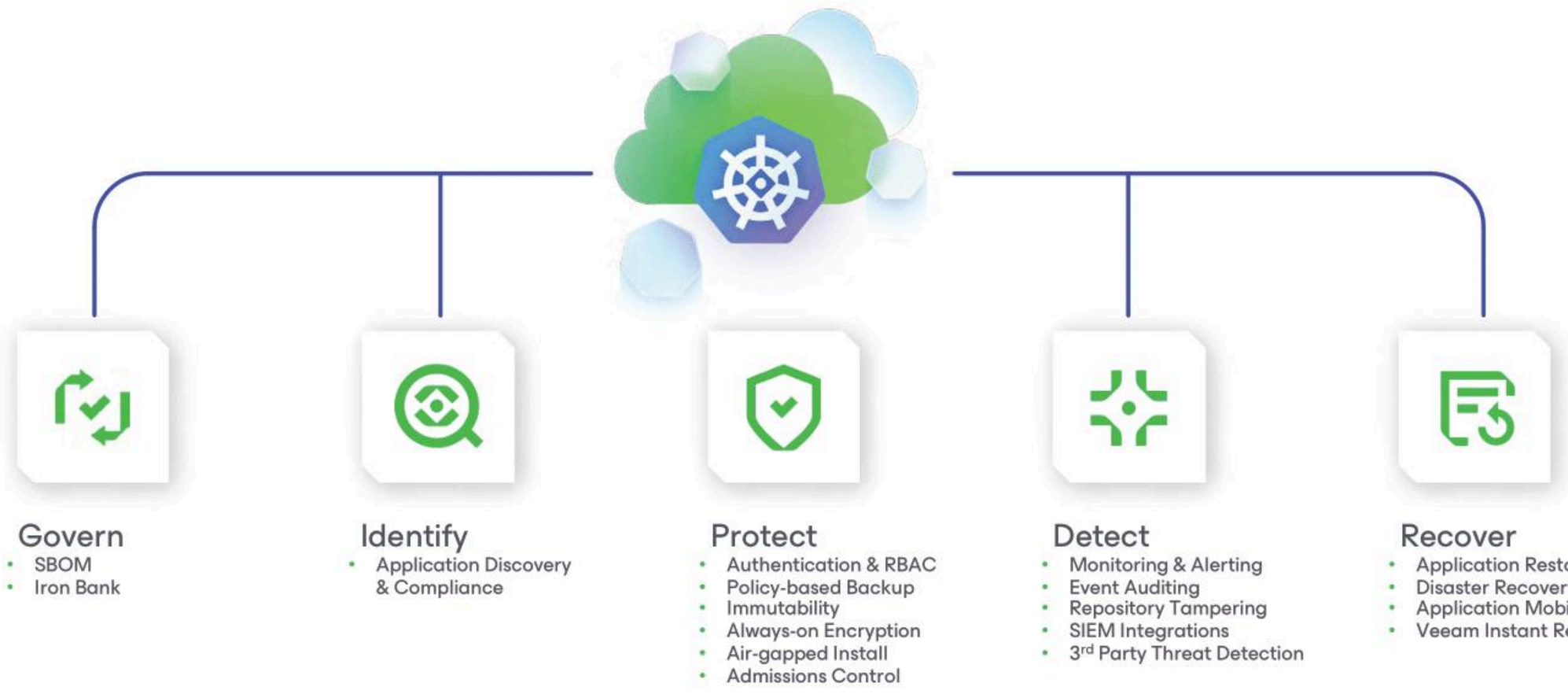
Kasten Advantages

- **Risk Reduction:** Refined access restrictions that minimize exposure to risks.
- **Oversight:** Realtime analytics to optimize threat discovery and prevention.
- **Compliance:** Meets NIST standards and broader industry regulations.
- **Automation:** Identify attacks and respond faster to prevent data loss or corruption.



Achieve zero trust: Cloud Native Kasten for Kubernetes

Kasten's implementation of Zero Trust within Kubernetes cultivates a proven, forward-thinking cybersecurity landscape. By persistently verifying credentials, imposing stringent access policies, and optimizing Kubernetes features, organizations can strengthen their data protection and ensure alignment with NIST's security recommendations. This cybersecurity strategy results in a modernized, protected, and compliant digital framework.



About Veeam Software

Veeam®, the #1 global market leader in data resilience, believes every business should be able to bounce forward after a disruption with the confidence and control of all their data whenever and wherever they need it. Veeam calls this radical resilience, and we're obsessed with creating innovative ways to help our customers achieve it. Veeam solutions are purpose-built for powering data resilience by providing data backup, data recovery, data freedom, data security, and data intelligence. With Veeam, IT and security leaders rest easy knowing that their apps and data are protected and always available across their cloud, virtual, physical, SaaS, and Kubernetes environments. Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 74% of the Global 2000, that trust Veeam to keep their businesses running. Radical resilience starts with Veeam. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

Reach out for more details:

veeam@marketplace.cgc.cloud