Zero Trust Run-time Kubernetes Security made easy with AccuKnox

THE EASIEST WAY TO HAVE THE BEST OF BOTH WORLDS: KUBERNETES + ZERO TRUST
The easiest way to have the best of both worlds: Kubernetes + Zero Trust

ISSUE

“Container usage for production deployments in enterprises is still constrained by concerns regarding security, monitoring, data management and networking.”

“Container adoption is increasing, and security must come along for the ride. Organizations value the scalability and agility that containers offer, but containers introduce new security challenges that can’t be addressed with traditional security and networking tools. Commonly accepted security tools like vulnerability scanners, network forensics, and endpoint detection and response (EDR) are too heavyweight for a container environment. Security pros need cloud native tools that are purpose-built for high scale, lightweight, ephemeral container environments.”

OPPORTUNITY

Kubernetes is a powerful orchestration technology for deploying, scaling and managing distributed applications and it has taken the industry by storm over the past few years. However, due to its inherent complexity, relatively few enterprises have been able to realize the full value of Kubernetes: manage their assets impeccably leave alone securing them.

SOLUTION

In the next few chapters, we will go over:

1. Security Challenges in Kubernetes/Containers
2. What is Zero Trust?
3. Why is Identity the New Perimeter?
4. What is Run Time Security?
5. What is Data Security?
6. How does AccuKnox deliver Run Time Security?
Containers are transient and ephemeral

EVOLUTION OF SERVER WORKLOAD ABSTRACTIONS

PHYSICAL
- Monolithic applications
- Physical servers as unit of scaling
- Life span of years

VIRTUAL MACHINES
- Hardware virtualization
- VMs as unit of scaling
- Life span of months to years

CONTAINERS
- OS Virtualization
- Applications/services as unit of scaling
- Life span of minutes to days

SERVERLESS

Source: Gartner 2019
Containers are vulnerable to zero-day attacks

Kubernetes console was vulnerable, and hackers were able to take control and find the credentials to AWS cloud. They were able to gain access to S3 buckets with sensitive data, as well as run cryptocurrency mining in Kubernetes pods.

Exploited containers allowed attackers to overwrite host runc library and gain root access to the container hosts.

An insecure Kubernetes cluster console was found by scanning publicly available IPs on kubelet TCP port 10250.

Linux kernel vulnerability CVE-2017-7308 can be used to change the current process’s namespaces into process 1’s and the host’s namespaces by calling a Linux kernel system call, allowing a full escape to host.

Source: Gartner 2019
Inter-container security is rarely enforced

Current Perimeter Defenses
*Firewalls, End Point address only North-South*  
[17% of the traffic]

Current Container Security Solutions
Do not have a mechanism to affirmatively enforce Policy Compliance
Traditional approaches to Linux, VM security like IPTables are not effective and are not scalable/cost-effective for securing large scale container workloads
Zero Trust Tenets

**Zero Trust Adage:**
Verify...then Trust...
...continuously Verify

**Ronald Reagan:**
Trust but verify.

1. The network is always assumed to be hostile
2. Assume threat actors are already inside your network
3. Network locality (segmentation) is not sufficient for deciding trust in a network
4. Every device, user and network flow is authenticated and authorized
5. Policies must be dynamic and calculated from as many sources of data as possible
6. The device is no longer the border. A user/service’ identity is the net border
7. Containers, serverless and cloud are the new disruptors of traditional security architecture

[John Kindervag who coined the term Zero Trust]
Gurus have spoken! – Embrace Zero Trust!

Embracing a Zero Trust Security Model

Executive Summary

As cybersecurity professionals defend increasingly dispersed and complex enterprise networks from sophisticated cyber threats, embracing a Zero Trust security model and the mindset necessary to design and operate a system, and according to Zero Trust principles can better position them to secure sensitive data.

Zero Trust is a security model, a set of system design principles, and a coordinated management strategy based on an acknowledgement that threats exist both inside and outside of network boundaries. The Zero Trust security model eliminates implicit trust in any one element of the system, requiring continuous verification of the operational picture via real-time information across and other system responses.

USAF CSO Emphasizes Zero Trust imperative Within DoD

U.S. Air Force Chief Software Officer (CSO) Nicolas Chaillan this week emphasized the importance of moving towards zero trust security architectures within the Department of Defense (DoD) – a process that DoD Acting CIO John Sherman has said is a top tech priority for the Pentagon.

NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly
The Future has arrived! – Identity is the New Perimeter!

Identity: the new perimeter?

If IT can have better control over an organization’s data and stronger security?

Organizations continue to focus the bulk of their security efforts on endpoints, as server and network security systems that as organizations turn to new cloud and mobile infrastructures shift control they once had over their IT assets.

If protecting the perimeter no longer provides sufficient alternatives do security practitioners have to best do? For those who are new to security, you’ve likely been told that identity, access management, and behavior analytics tools will provide you the greatest visibility and find those tools might be a challenge.

Identity Is the New Perimeter

First, it was the firewall that shielded the perimeter of our networks from outside intrusion. Firewalls are still a necessary tool in any cybersecurity system, but as more data access came from beyond the internal network, the perimeter shifted to endpoints.

With cloud computing, mobile devices, the Internet of Things (IoT) and the like, much of our information is stored and accessed far away from the original network perimeter. Protecting that data became cybersecurity’s battle cry, and endpoints became the new perimeter.

Now, there is yet another shift. Thanks to digital transformation, identity is the new perimeter.

Identity Is the New Perimeter: Turning Focus

The idea of identity as the new perimeter (and how to secure it) was a primary talking point at Identiverse 2018 earlier this summer. The running theme was
AccuKnox Zero Trust Security Platform

<table>
<thead>
<tr>
<th>Network</th>
<th>Application</th>
<th>Data</th>
<th>API</th>
<th>Serverless</th>
<th>IoT</th>
<th>5G</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTINUOUS COMPLIANCE</td>
<td>MITRE, NIST, PCI, GDPR, CCPA, HIPAA, SOC2, NERC, FERC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZERO TRUST POLICY MANAGEMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MICRO-SEGMENTATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENTERPRISE INTEGRATION</td>
<td>SIEM, SOAR, SSO/RBAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Security, Data Provenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Un-supervised learning-based Anomaly Detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPA, Kyverno – Policy Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPIFFE – Identity Management Layer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eBPF / Cilium</td>
<td>KubeArmor</td>
<td>Confidential Computing / Enclave</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRIVATE AND PUBLIC CLOUD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AccuKnox Zero Trust Security Platform

CONTINUOUS COMPLIANCE
MITRE, NIST, PCI, GDPR, CCPA, HIPAA, SOC2, NERC, FERC

ZERO TRUST POLICY MANAGEMENT

MICRO-SEGMENTATION

ENTERPRISE INTEGRATION
SIEM, SOAR, SSO/RBAC

Data Security, Data Provenance
Un-supervised learning-based Anomaly Detection

OPA, Kyverno – Policy Management
SPIFFE – Identity Management Layer

Confidential Computing / Enclave

PRIVATE AND PUBLIC CLOUD

AccuKnox is the industry’s most comprehensive Zero Trust Security platform that helps you secure your current assets (Network, Application, Data) and your strategic future assets (API, Serverless, IoT, 5G)
AccuKnox Data Security, Data Provenance

Based on 10+ years of Data Provenance research at Stanford and helps you answer the following questions:

1. Which process [e.g., app] was used to create this data object [e.g., file]?
2. When the process ran what were the other data object it wrote?
3. What data objects did the process read?
4. Could any data have flowed from this data object to that data object?
5. What is the sensitivity of a given data flow or connection between processes?
AccuKnox Data Security, Data Provenance

CONTINUOUS COMPLIANCE
MITRE, NIST, PCI, GDPR, CCPA, HIPAA, SOC2, NERC, FERC

ZERO TRUST POLICY MANAGEMENT

MICRO-SEGMENTATION

ENTERPRISE INTEGRATION
SIEM, SOAR, SSO/RBAC

Data Security, Data Provenance
Un-supervised learning-based Anomaly Detection
OPA, Kyverno – Policy Management
SPIFFE – Identity Management Layer

eBPF / Cilium
KubeArmor
Confidential Computing / Enclave

PRIVATE AND PUBLIC CLOUD
Due to the wide diversity of IoT devices the IoT security challenges center around how to provide Agentless Diagnostics in a very Heterogenous Environment. Unique aspects of IoTKnox include:

1. Passive Agent based device discovery
2. No modification to device firmware
3. Use of fingerprinting techniques to identify device make/model/application
4. Scan against well-known vulnerability database
5. Passive Agent connected to edge router
6. Can isolate a malicious device automatically
7. Anomaly Detection
8. SPIFFE Integration with last-mile protocols such as DNP3, DLMS/COSEM
AccuKnox 5G Security

U.S. 5G Open Architecture is designed to enable 3rd party application ecosystem using a microservice architecture framework.

- AccuKnox 5G Security facilitates System-level Policy Enforcement and cloud-based security management for 5G environment
- AccuKnox core technologies can be applied to ensure security compliance, monitoring, scalable policy policy generation and management

CONTINUOUS COMPLIANCE
MITRE, NIST, PCI, GDPR, CCPA, HIPAA, SOC2, NERC, FERC

ZERO TRUST POLICY MANAGEMENT

MICRO-SEGMENTATION

ENTERPRISE INTEGRATION
SIEM, SOAR, SSO/RBAC

Data Security, Data Provenance

Un-supervised learning-based Anomaly Detection

OPA, Kyverno – Policy Management

SPIFFE – Identity Management Layer

eBPF / Cilium
KubeArmor

Confidential Computing / Enclave

PRIVATE AND PUBLIC CLOUD
AccuKnox Continuous Compliance

CONTINUOUS COMPLIANCE
MITRE, NIST, PCI, GDPR, CCPA, HIPAA, SOC2, NERC, FERC

ZERO TRUST POLICY MANAGEMENT

MICRO-SEGMENTATION

ENTERPRISE INTEGRATION
SIEM, SOAR, SSO/RBAC
Data Security, Data Provenance
Un-supervised learning-based Anomaly Detection
OPA, Kyverno – Policy Management
SPIFFE – Identity Management Layer

eBPF / Cilium
KubeArmor
Confidential Computing / Enclave

PRIVATE AND PUBLIC CLOUD

Dynamic Inventory enriched with:
• K8s Metadata
• L7 identity

Out-of-the-box Templates for Industry-standard compliance frameworks (PCI, SOC2, etc.)
K8s SIG-Policy standards-based Templates
Managed via Kubernetes API and kubectl cli
Allows creation of internal Org-specific templates

Audit linked to dynamic strong L7 identity (x.509, jwt)
Audit system, network and data events
Correlation across clusters and cloud platforms

OSCAL Standards-based Evidence Reports
Easy integration with existing GRC Platforms
Accuknox UI and Dashboard
Compliance, Security, Platform and Application team roles

Remediate
Inventory
Define Controls
Audit
Report
AccuKnox Policy Management Lifecycle

CONTINUOUS COMPLIANCE
MITRE, NIST, PCI, GDPR, CCPA, HIPAA, SOC2, NERC, FERC

ZERO TRUST POLICY MANAGEMENT

MICRO-SEGMENTATION

ENTERPRISE INTEGRATION
SIEM, SOAR, SSO/RBAC

Data Security, Data Provenance
Un-supervised learning-based Anomaly Detection
OPA, Kyverno – Policy Management
SPIFFE – Identity Management Layer

eBPF / Cilium
KubeArmor
Confidential Computing / Enclave

PRIVATE AND PUBLIC CLOUD

Recommend
Auto - Generate
Stage / Audit
Preview

Unsecured East-West Access

Zero-Trust (least-privilege) whitelist Policies

Commit
# AccuKnox Policy Management Lifecycle

<table>
<thead>
<tr>
<th>Network</th>
<th>Application</th>
<th>Data</th>
<th>API</th>
<th>Serverless</th>
<th>IoT</th>
<th>5G</th>
</tr>
</thead>
</table>

## CONTINUOUS COMPLIANCE
MITRE, NIST, PCI, GDPR, CCPA, HIPAA, SOC2, NERC, FERC

## ZERO TRUST POLICY MANAGEMENT

### MICRO-SEGMENTATION

### ENTERPRISE INTEGRATION
SIEM, SOAR, SSO/RBAC

Data Security, Data Provenance

Un-supervised learning-based Anomaly Detection

OPA, Kyverno – Policy Management

SPIFFE – Identity Management Layer

eBPF / Cilium

KubeArmor

Confidential Computing / Enclave

## PRIVATE AND PUBLIC CLOUD
# AccuKnox Micro-segmentation

<table>
<thead>
<tr>
<th>Network</th>
<th>Application</th>
<th>Data</th>
<th>API</th>
<th>Serverless</th>
<th>IoT</th>
<th>5G</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTINUOUS COMPLIANCE</td>
<td>MITRE, NIST, PCI, GDPR, CCPA, HIPAA, SOC2, NERC, FERC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZERO TRUST POLICY MANAGEMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MICRO-SEGMENTATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENTERPRISE INTEGRATION</td>
<td>SIEM, SOAR, SSO/RBAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Security, Data Provenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Un-supervised learning-based Anomaly Detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPA, Kyverno – Policy Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPIFFE – Identity Management Layer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eBPF / Cilium</td>
<td>KubeArmor</td>
<td>Confidential Computing / Enclave</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRIVATE AND PUBLIC CLOUD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- IdP (OIDC)
  - Azure AD
  - Okta
  - Cloud AuthN

**Network Diagram**

![Network Diagram](image-url)
# AccuKnox Enterprise Integration

<table>
<thead>
<tr>
<th>Network</th>
<th>Application</th>
<th>Data</th>
<th>API</th>
<th>Serverless</th>
<th>IoT</th>
<th>5G</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTINUOUS COMPLIANCE</td>
<td>MITRE, NIST, PCI, GDPR, CCPA, HIPAA, SOC2, NERC, FERC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZERO TRUST POLICY MANAGEMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MICRO-SEGMENTATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENTERPRISE INTEGRATION</td>
<td>SIEM, SOAR, SSO/RBAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Security, Data Provenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Un-supervised learning-based Anomaly Detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPA, Kyverno – Policy Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPIFFE – Identity Management Layer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eBPF / Cilium</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KubeArmor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidential Computing / Enclave</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRIVATE AND PUBLIC CLOUD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

AccuKnox provides comprehensive integration with 3rd party security platforms.
AccuKnox provides un-supervised learning-based Anomaly Detection to discover malicious activity in large scale Kubernetes environments.

### AccuKnox Anomaly Detection

- **Network**
- **Application**
- **Data**
- **API**
- **Serverless**
- **IoT**
- **5G**

**CONTINUOUS COMPLIANCE**
- MITRE, NIST, PCI, GDPR, CCPA, HIPAA, SOC2, NERC, FERC

**ZERO TRUST POLICY MANAGEMENT**

**MICRO-SEGMENTATION**

**ENTERPRISE INTEGRATION**
- SIEM, SOAR, SSO/RBAC
- Data Security, Data Provenance

**Un-supervised learning-based Anomaly Detection**
- OPA, Kyverno – Policy Management
- SPIFFE – Identity Management Layer

**eBPF / Cilium**
- **KubeArmor**
- Confidential Computing / Enclave

**PRIVATE AND PUBLIC CLOUD**
AccuKnox Policy Management Foundations

<table>
<thead>
<tr>
<th>Network</th>
<th>Application</th>
<th>Data</th>
<th>API</th>
<th>Serverless</th>
<th>IoT</th>
<th>5G</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTINUED COMPLIANCE</td>
<td>MITRE, NIST, PCI, GDPR, CCPA, HIPAA, SOC2, NERC, FERC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZERO TRUST POLICY MANAGEMENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MICRO-SEGMENTATION</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENTERPRISE INTEGRATION</td>
<td>SIEM, SOAR, SSO/ RBAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Security, Data Provenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Un-supervised learning-based Anomaly Detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPA, Kyverno – Policy Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPIFFE – Identity Management Layer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eBPF / Cilium</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KubeArmor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidential Computing / Enclave</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRIVATE AND PUBLIC CLOUD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

AccuKnox leverages proven, opensource policy management foundation platforms.

OPA (Open Policy Agent) is a Declarative, Context-aware, Expressive, Fast, Portable policy management framework. It allows you to decouple policy from the service’s code so you can release, analyze, and review policies (which security and compliance teams love) without sacrificing availability or performance.

Kyverno is a policy engine designed for Kubernetes. It can validate, mutate, and generate configurations using admission controls and background scans. Kyverno policies are Kubernetes resources and do not require learning a new language. Kyverno is designed to work with tools like kubectl, kustomize, and Git.
AccuKnox Identity Management Foundations

AccuKnox uses very strong industry standard Opensource platforms like SPIFFE and SPIRE for User and Service Management, Attestation, Enforcement, etc.

SPIFFE Secure Production Identity Framework for Everyone, provides a secure identity, in the form of a specially crafted X.509 certificate, to every workload in a modern production environment. SPIFFE removes the need for application-level authentication and complex network-level ACL configuration.

SPIRE is a production-ready implementation of the SPIFFE APIs that performs node and workload attestation in order to securely issue SVIDs to workloads, and verify the SVIDs of other workloads, based on a predefined set of conditions.

SPIFFE and SPIRE were developed by Scytale, Inc which was acquired by HPE in Feb 2020.
Cilium is open-source software for providing and transparently securing network connectivity and load-balancing between application workloads such as application containers or processes. Cilium operates at Layer 3/4 to provide traditional networking and security services as well as Layer 7 to protect and secure use of modern application protocols such as HTTP, gRPC, and Kafka. Cilium is integrated into common orchestration frameworks such as Kubernetes.

A new Linux kernel technology called eBPF (enhanced Berkeley Packet Filter) is at the foundation of Cilium. It supports dynamic insertion of eBPF bytecode into the Linux kernel at various integration points such as: network IO, application sockets, and tracepoints to implement security, networking and visibility logic. eBPF is highly efficient and flexible. To learn more about eBPF, visit eBPF.io.
KubeArmor is a Container-aware Runtime Security Enforcement System. Developed and supported by AccuKnox it has received wide acclaim and great support from the opensource community.
AccuKnox Confidential Computing/Enclave

<table>
<thead>
<tr>
<th>Network</th>
<th>Application</th>
<th>Data</th>
<th>API</th>
<th>Serverless</th>
<th>IoT</th>
<th>5G</th>
</tr>
</thead>
</table>

CONTINUOUS COMPLIANCE
MITRE, NIST, PCI, GDPR, CCPA, HIPAA, SOC2, NERC, FERC

ZERO TRUST POLICY MANAGEMENT

MICRO-SEGMENTATION

ENTERPRISE INTEGRATION
SIEM, SOAR, SSO/RBAC

Data Security, Data Provenance

Un-supervised learning-based Anomaly Detection

OPA, Kyverno – Policy Management

SPIFFE – Identity Management Layer

eBPF / Cilium
KubeArmor

Confidential Computing / Enclave

PRIVATE AND PUBLIC CLOUD

Gartner opines that by 2025, 50% of large organizations will adopt privacy-enhancing computation for processing data in untrusted environments and multiparty data analytics use cases. Gartner has identified privacy-enhancing computation as a key enterprise technology trend for 2021 and enabler for processing and analyzing highly sensitive data.

The three pillars of data security involve protecting data at rest, in transit, and in use. A number of tech leaders (AMD, ARM, Facebook, Google, IBM, Microsoft, Oracle, Vmware) are developing standards and are developing opensource tools. AccuKnox will be embracing these in its efforts to deliver the most comprehensive Zero Trust solution.
# AccuKnox Zero Trust Security Platform – How do we stack up?

<table>
<thead>
<tr>
<th>Category</th>
<th>AccuKnox</th>
<th>Brand A</th>
<th>Brand B</th>
<th>Brand C</th>
<th>Brand C</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application (Container / Pod) Runtime</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Runtime application security on Kubernetes using LSM</td>
<td>✔ ✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Secure Enclaves</td>
<td>✔ ✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Recommendations and Policy Lifecycle Management</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Container and Vulnerability Scanning</td>
<td>✔ ✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Container Forensics and VAE</td>
<td>✔ ✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Container Compliance Templates</td>
<td>✔ ✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Runtime data security</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Data Provenance and Compliance templates</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kubernetes Network Policies</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Advanced Network Policy Semantics</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>SPIFFE Identity integration for AuthN</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Recommendations and Policy Lifecycle Management (Staged Policies)</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Support for L7 visibility and L7 policy controls</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Observability (Flow Viz, Telemetry, etc.)</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Network Forensics and Anomaly Detection</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Network Compliance Templates</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
**AccuKnox Zero Trust Security Platform Summary**

**IN SUMMARY, WITH ACCUKNOX YOU CAN:**

- **Isolate and protect** every kind of container workload with identity as a perimeter
- **Track tainted data** and enable data provenance in a container first world
- **Enable networking and system level restrictions** over containers to easily comply with a wide variety of compliance needs
- **Enable enterprise grade container security** with the best of breed container security technologies – eBPF and LSM
- **Build container workloads** to operate in Enclaves by leveraging Confidential computing.

**THE FOLLOWING ARE OUR KEY DIFFERENTIATORS:**

- Industry’s most Comprehensive Identity Driven Zero Trust Solution for: Containers, Functions, API, Data, IoT, 5G
- Built on proven OpenSource products: OPA, Kyverno, KubeArmor, SPIFFE, eBPF/Cilium
- Leverages seminal technologies from SRI in the areas of Anomaly Detection, Container Security and Data
- Highly differentiated, patented innovation [10+ patents]
- Future Proof Product/Tech Roadmap
- Validation by Fortune 100 companies and Silicon Valley Cloud Native Tech Leaders
- Seasoned team with a record of disciplined execution and Customer/Partner Success
About AccuKnox

AccuKnox provides a Zero Trust Run-time Kubernetes Security platform. AccuKnox is built in partnership with SRI (Stanford Research Institute) and is anchored on seminal inventions in the areas of: Container Security, Anomaly Detection and Data Provenance. AccuKnox can be deployed in Public and Private Cloud environments. Visit www.accuknox.com