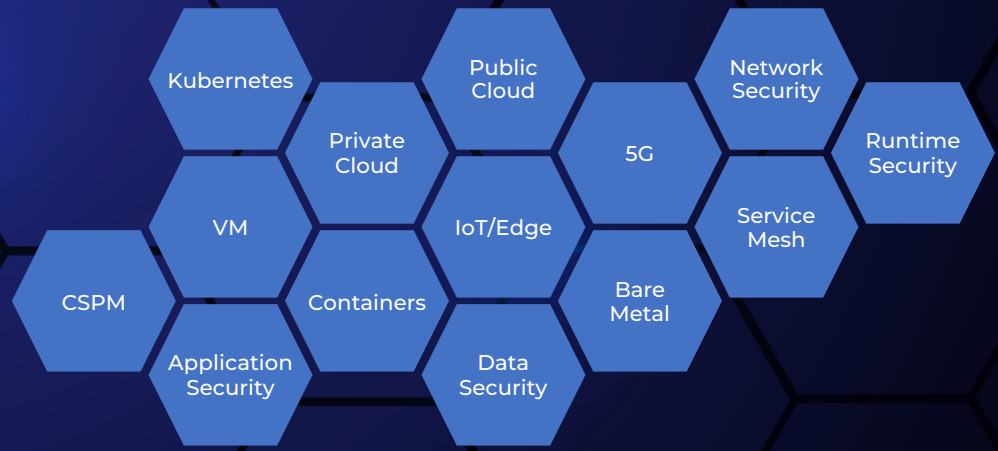
AccuKnox

Why Zero Trust CNAPP

Cloud Native Application Protection

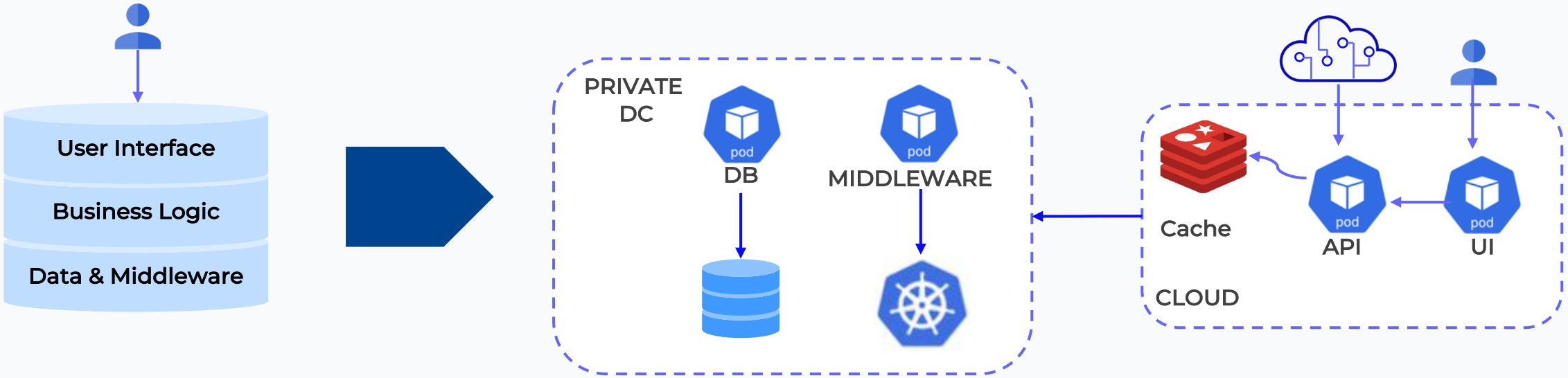


Aug 2022

In this eBook:

Modern Applications Increase the Attack Surface

- The adoption of Cloud Native (containers, micro-services, Kubernetes) means application assets are increasingly distributed - across private and public clouds, from data centers to the edge.
- Today's apps are hybrid, as mixes of technology platforms are supported, and thus have larger attack surfaces.
- Apps are deployed more frequently: from months down to multiple times a day.
- App teams are having to play larger roles in deploying & securing the apps.



AccuKnox

On-demand Cloud Native Assets Require New Security Approaches

Cloud Assets like containers and serverless functions are short lived, and often use labels and certificates instead of IP addresses. Thus, legacy security tools like IP Tables are no longer a credible way to defend them.

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

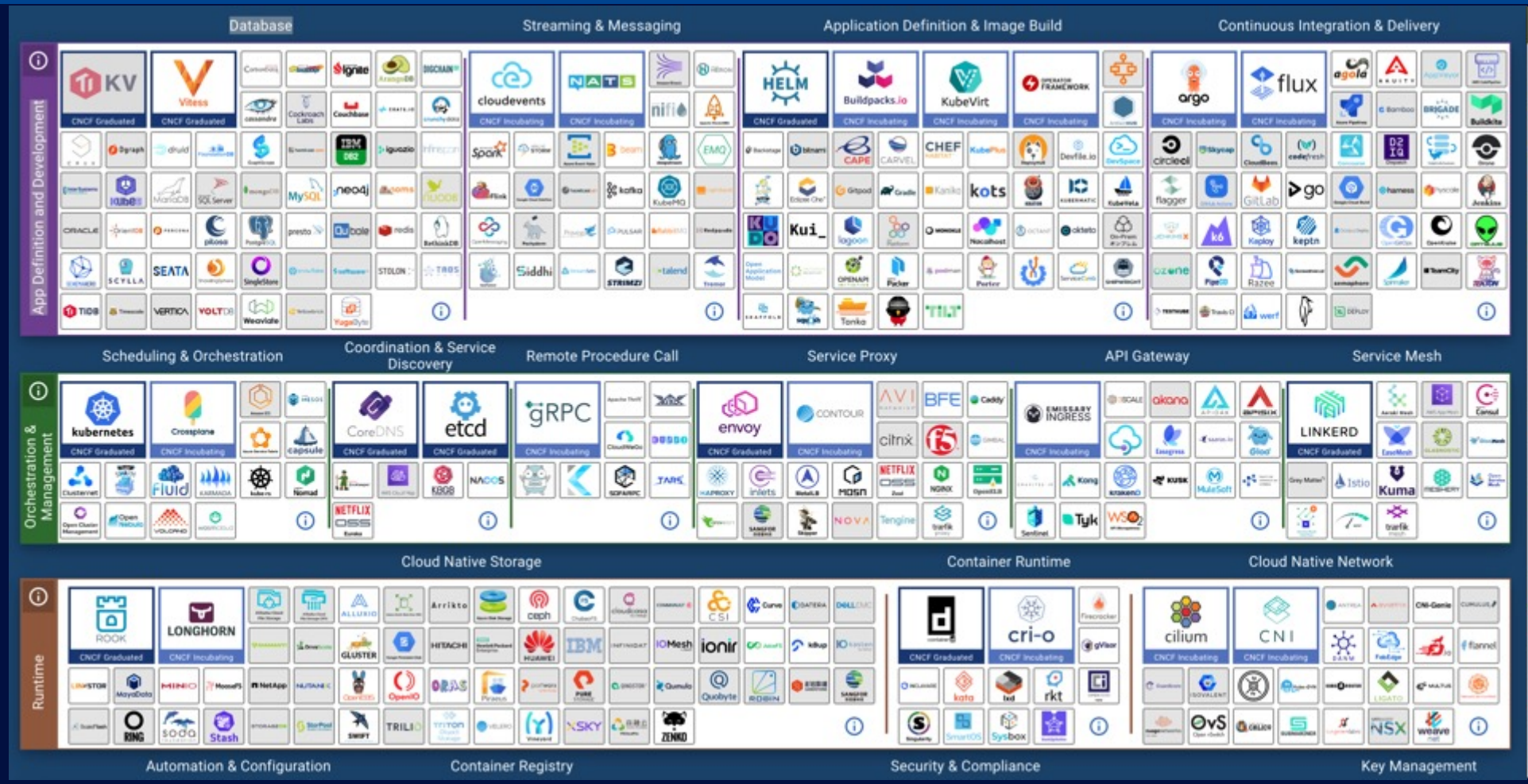
Life span of seconds to minutes

SOURCE: Gartner

AccuKnox

Almost Every App Relies on Open Source Software

- **73%** YoY growth in downloads of Open Source packages - more than 2.2 trillion [Source: Sonatype]
- **430%** growth in cyber attacks OpenSource software projects [Source: Synopsys]
- **50%** of Docker Hub Images Feature Critical Flaws [Source: InfoSecurity Group]



Target: Software Supply Chain Nation State Attacks on the rise

The recent and unfolding news about the Russian APT 29, or Cozy Bear, SolarWinds breach is a sobering reminder of the relentlessness of nation-state cyber attack campaigns, which have turned their attention to vulnerabilities created by supply chain backdoors. You can read more about Cozy Bear's techniques in our Russia threat report.

While companies across sectors have been shoring up their cybersecurity defenses with technologies such as firewalls, endpoint protection, and Network Detection and Response, these recent events call for renewed vigilance for securing the supply chain.

Indirect attacks into the supply chain now account for 40 percent of security breaches, according to the Accenture Security / Third State of Cyber Resilience Report. Indeed, the days of having well-defined data boundaries are gone, and traditional data protections are no longer sufficient to secure these ecosystems.

Nobelium, the threat actor attributed to the massive SolarWinds supply chain compromise has been once again linked to a series of attacks targeting multiple cloud solution providers, services and the hacking group continues to refine and retool its tactics at an alarming pace.

Russia using Kubernetes cluster for brute-force attacks

TechTarget

The NSA warned that Russian state-sponsored hackers launched a new container-based campaign aimed at breaching networks and stealing essential data from multiple industries.

AccuKnox

Notable Cloud Breaches

A day does not go by when we don't hear about major cyber attacks against Cloud Assets. Given that the workloads are moving to the cloud at rapid rate it is only natural that attacks are shifting to the cloud. In addition to the number of attacks the severity and sophistication of the attacks in the cloud are also very advanced.

The global cloud computing market size is estimated to value at **$405.29 Billion in 2022** and reach **$1465.81 Billion by 2028**; it is expected to grow at a **CAGR of 23.9% from 2022 to 2028**. Given this it is only logical that attackers will be increasing the volume, velocity and sophistication of their cyber attacks. Hence it is prudent to instill pertinent security measures.

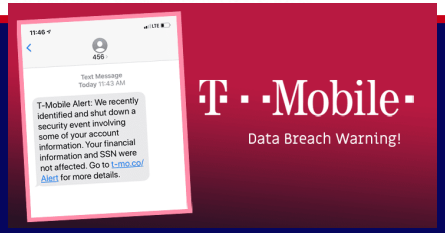
Kubernetes console was vulnerable, and hackers were able to take control and find the credentials to AWS cloud. They were able to gain access to S3 buckets with sensitive data, as well as run cryptocurrency mining in Kubernetes pods.

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

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.

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

weight watchers

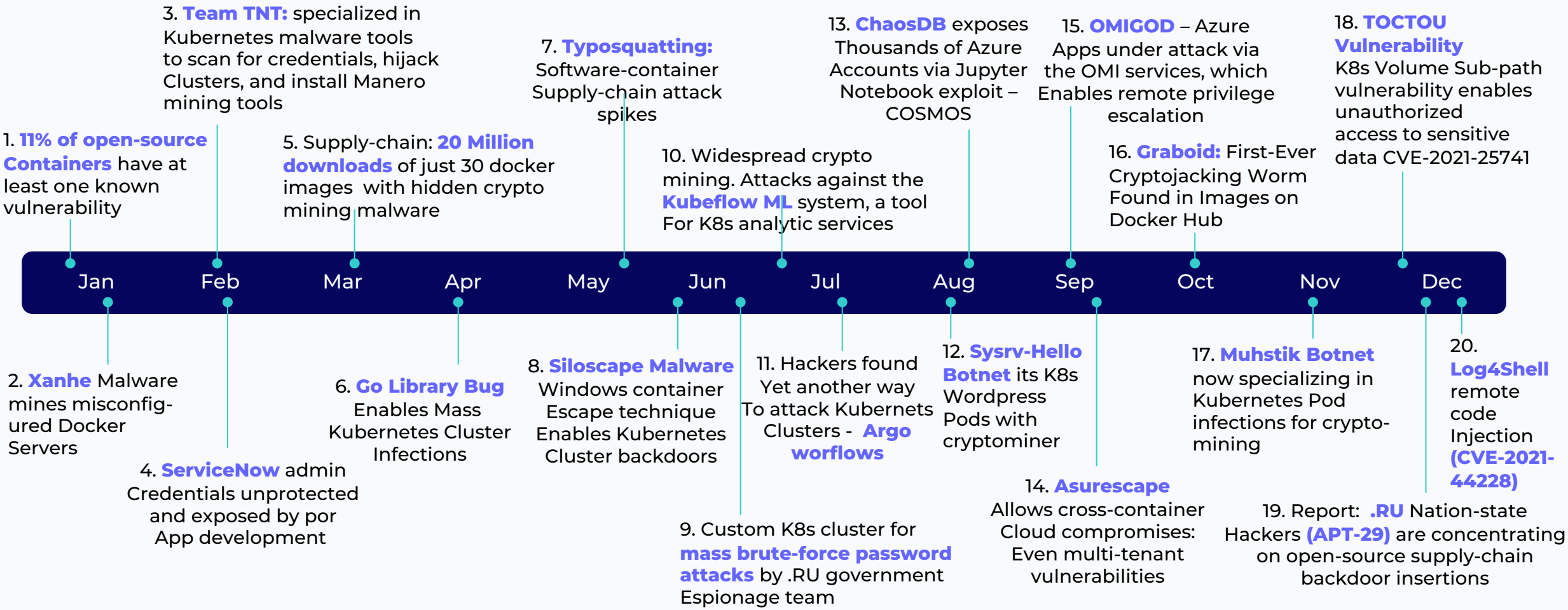


AccuKnox

Targeted Kubernetes Attacks in 2021

These are some of the major Kubernetes attacks in 2021 that we catalogued.
The sophistication of these attacks are far more than what we saw in earlier attacks.

More in our blog - https://blog.accuknox.com/2021-cloud-security-year-end-review/



ACCUKNOX

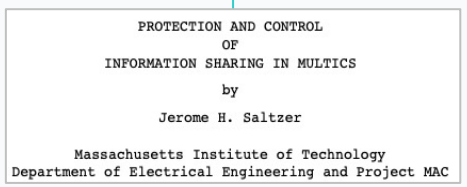
Zero Trust Evolution & Adoption Increasing

Zero Trust shifts the focus from trying to identify what is bad and stopping it, to identifying what is good and allowing it, denying all else.

Zero Trust principles were established 10 years ago, but its principles in least privilege and identity are decades old. Zero Trust is gaining increased adoption since the Solar Winds and other supply chain breaches.

1976

MIT professor, Saltzer coins the term "Least privilege" Every program should operate using the least set of privileges necessary to complete the job.



PROTECTION AND CONTROL
OF
INFORMATION SHARING IN MULTICS

by

Jerome H. Saltzer

Massachusetts Institute of Technology
Department of Electrical Engineering and Project MAC

1977

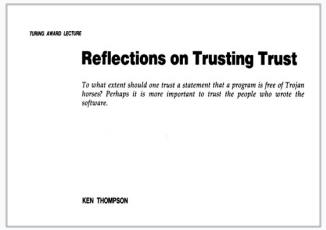
PKI

RSA (Rivest Shamir Adelman), Diffie-Helman
Invent public key infrastructure (PKI)

(PKI) is a needed to manage digital certificates and manage public-key encryption. Required for activities where simple passwords are an inadequate and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

1984

MIT Professor Ken Thompson delivers a seminal lecture on **Trusting Trust**



TURING AWARD LECTURE

Reflections on Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON

2003

UK Royal Mail organizes Jericho Forum where a new term **DE-PERIMETERIZATION** is introduced

Security must:

1. Be specific to the asset being protected
2. Pervasive, simple and scalable
3. Leverage Open Protocols
4. Transparent
5. Portable
6. Allow for separation of duties
7. Apply at rest, in transit and in use

2010

John Kindervag, Forrester coins the term Zero Trust

Tenets

1. Network is assumed to be hostile
2. Threat actors are in your network
3. Network segmentation is not enough
4. Policies must be dynamic
5. Device is no longer at the border
6. Containers, Serverless and Cloud are new disruptors

2019

SolarWinds leveraged for several high-profile breaches.

CISA issues Emergency Directive 21-01 "The compromise of SolarWinds' Orion Network Management Products poses unacceptable risks to the security of federal networks," said CISA Acting Director Brandon Wales.

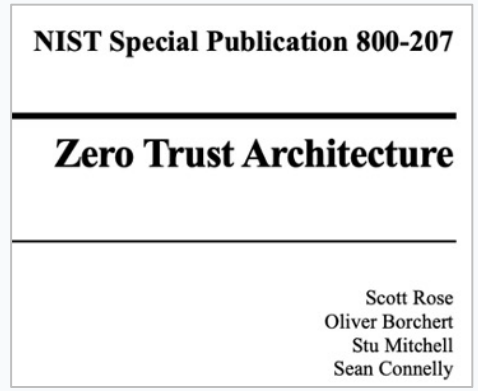
SolarWinds leads to Zero Trust Mandate

CISA issued Emergency Directive to Mitigate Threat from SolarWinds Orion Network

- The Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-01, calls on all US federal civilian agencies to review their networks for indicators of compromise and disconnect or power down SolarWinds Orion products immediately.
- "The compromise of SolarWinds' Orion Network Management Products poses unacceptable risks to the security of federal networks," said CISA Acting Director Brandon Wales. "Tonight's directive is intended to mitigate potential compromises within federal civilian networks, and we urge all our partners—in the public and private sectors—to assess their exposure to this compromise and to secure their networks against any exploitation."

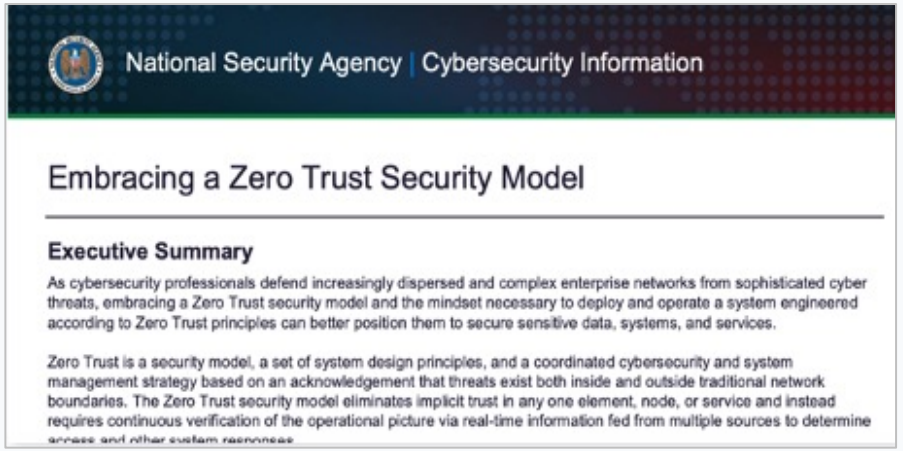
CISO Sentiment… Jan 2021

- The impact of the breach is profound. It really turned on its head a lot of conventions about cyber security.. We are now in a situation where we have to monitor the monitors.
- The attack did not have any signatures of a previous attack.. So, you got down to the code level
- 80-90% of code is being downloaded from the internet.. It is bringing DevOps security processes and making us rethink how to reinvent security


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

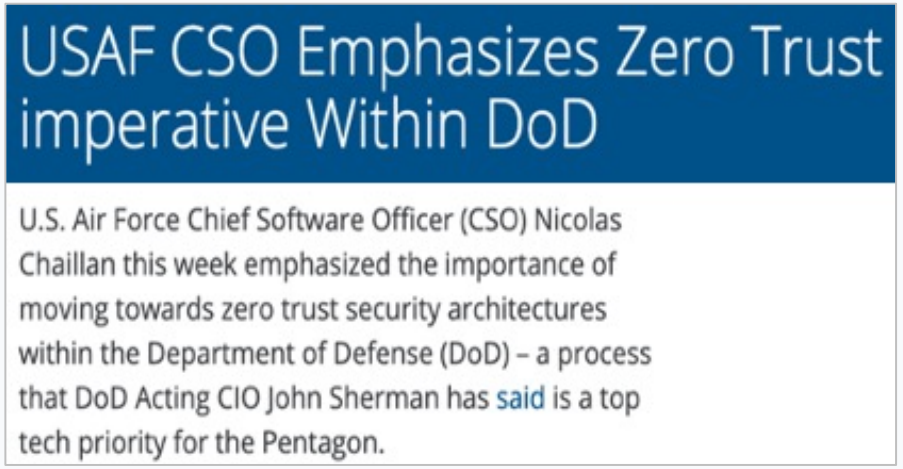

National Security Agency | Cybersecurity Information

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 deploy and operate a system engineered according to Zero Trust principles can better position them to secure sensitive data, systems, and services.

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access 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.

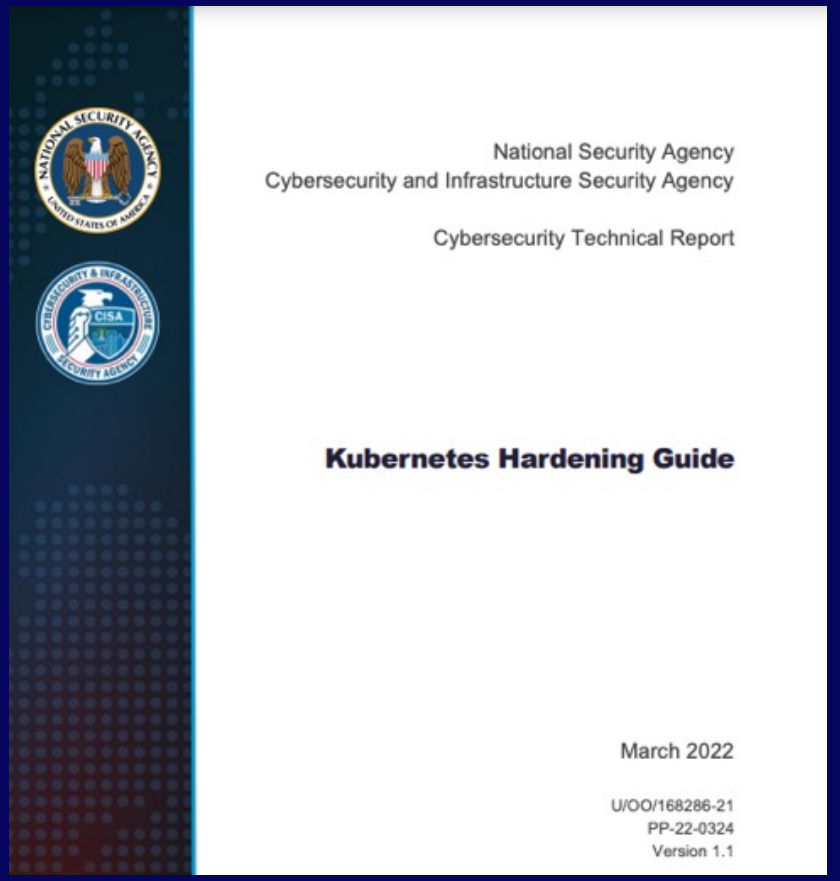
NSA & CISA Kubernetes Hardening Guide

This is a seminal guide that serves as a reference for all Cloud Security practitioners. The authors make the following salient points:

1. Scan containers and Pods for vulnerabilities or misconfigurations.
2. Run containers and Pods with the least privileges possible using technologies such as AppArmor, SELinux and Secomp. Accuknox's tooling supports such techniques easily and seamlessly.
3. Use network separation to control the amount of damage a compromise can cause.
4. Use firewalls to limit unneeded network connectivity and use encryption to protect confidentiality.
5. Use strong authentication and authorization to limit user and administrator access as well as to limit the attack surface.
6. Capture and monitor audit logs so that administrators can be alerted to potential malicious activity.
7. Periodically review all Kubernetes settings and use vulnerability scans to ensure risks are appropriately accounted for and security patches are applied.

AccuKnox addresses all of these in a very automated and efficient manner:

1. AccuKnox leverages "Identity As Perimeter" as a fundamental architectural tenet
2. AccuKnox deploys AppArmor, SELinux and Seccomp as LSM (Linux Security Modules) at the pod/container level
3. AccuKnox delivers Automated Policy Generation and fine grained control of Policy Enforcement
4. AccuKnox delivers Anomaly Detection/Continuous Compliance using un-supervised Machine Learning Technology



Runtime security

Static Security is very important but a relatively straightforward problem. This involves signature-based matching of workloads against a repository of known vulnerabilities.
Run time security on the other hand requires sophisticated techniques that form the bed rock of AccuKnox Zero Trust Security platform

> “an effective Kubernetes security tool must be able to visualize and automatically verify the safety of all connections within the Kubernetes environment, and block all unexpected activities. … With these runtime protections, even if an attacker breaks into the Kubernetes environment and starts a malicious process, that process will be immediately and automatically blocked before wreaking havoc.”

InfoWorld Nov 17, 2021

AccuKnox

Many Security Tools are Necessary but Insufficient

From vulnerability scanning, to posture management, to application testing and detection and response… there's no lack of discrete security tools. Cloud Native Application Protection Platforms, as defined by Gartner, bundles a range of different security technologies together under one heading. But this doesn't mean they're actually "integrated." Platforms in this space have largely bolted on disparate products that have been acquired. This leaves a lot of work for the buyer to do to make sense of the flood data and take appropriate action.

In addition, very few have true zero trust foundations, generating excessive amounts of noise that the SOC team has to sort out.

Even fewer have **true zero trust, runtime protection** – the key to proactive protection, reducing alert fatigue, and enabling operational resilience and continuous compliance.

DevSecOps teams need an Integrated, Zero Trust-based CNAPP that just works.

- ✓ Attack Surface Reduction
- ✓ Posture Management
- ✓ Zero Trust
- ✓ Runtime Security
- ✓ Security Observability
- ✓ Continuous Compliance
- ✓ Operational Resilience

AccuKnox

Key Capabilities of Zero Trust CNAPP

Vulnerability scanning	CSPM	CWPP	Triage and remediation
• Vulnerability visibility • Compliance • Image assurance • Serverless support • Agentless	• Monitor cloud security posture • Host security • K8s security • Serverless security • Web and API security • IAM Security • Agentless via API	• Runtime cloud workload security • Runtime networking security • Runtime observability • Serverless support • Dynamic threat analysis • Agentless	• Integrations with SIEM / SOAR • Threat feed integrations • Splunk apps

Automating Zero Trust from Dev to Runtime

AccuKnox simplifies the process of securing your workloads against software supply chain issues, vulnerabilities, misconfigurations and malicious adversaries.

Legacy and non-cloud-native security tools, add complexity, costs and delays. AccuKnox simplifies the process, from development to runtime by:

- ✔ Providing deep security observability into application behavior
- ✔ Automating zero trust policy management
- ✔ Continuous monitoring and compliance
- ✔ Anomalous behavior detection

AccuKnox

USE CASES

Zero Trust Runtime Security

Automated application hardening for cloud native applications.

AccuKnox automates the process of application hardening & firewalling to help you achieve Zero Trust/Least Privilege Security. Our unique application insights and automated policy discovery engines greatly simplify the work required to analyze applications and create effective security policies.

- AccuKnox profiles and creates a baseline of policies by observing the application (and network) graph
- AccuKnox observes interactions with the host operating system and other workloads
- Based on these, AccuKnox generates Zero Trust security policies that are enforced by the Kernel using Kernel Primitives, like AppArmor, SELinux and SecComp

Security Observability

Get deep application insights into runtime behavior. Understand what your applications - including embedded dependencies - are doing.

Get visibility into process execution, forking, network and file access. Detect changes and risky behavior in dev, staging and production - in your software supply chain.

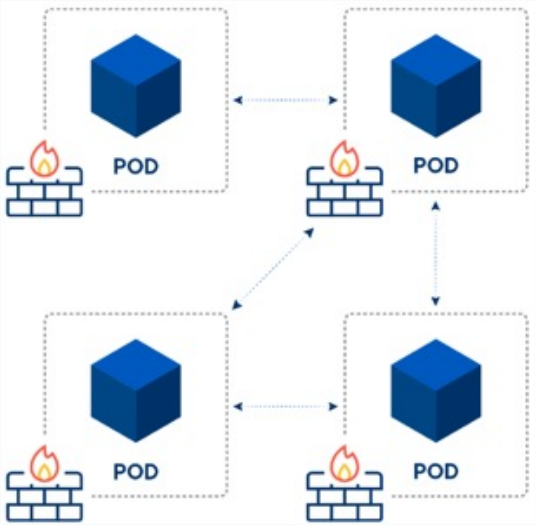
ACCUKNOX

Network Segmentation & Firewalling

Easily orchestrate network segmentation & firewalling.

Kubernetes pods and services in different namespaces can still communicate with each other unless additional separation is enforced. Manually configuring network and firewall policies is time-consuming and error prone.

AccuKnox automatically analyzes applications behavior and creates least privilege network policies to be implemented by existing, high-performance linux security modules. The network policies move as code with the application, greatly increasing the speed, control and confidence of DevSecOps teams.



Continuous Compliance

Assess & demonstrate compliance with regulatory standards like PCI & NIST.

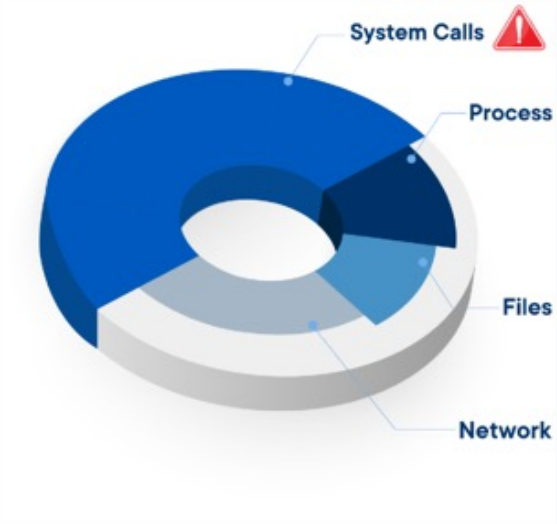
Implement policies in Audit mode to continuously monitor the workloads for deviations from NIST, PCI and other standards. Get high-value, actionable alerts for your SecOps team – or enforce Runtime Security and implement guard rails for risky behavior.

USE CASES

Anomaly Detection

Detect and protect against anomalous and malicious behavior, including policy drift, and “unknown unknowns”

AccuKnox implements Anomaly Detection using Variational Autoencoder (VAE) technology developed in partnership with the Stanford Research Institute (SRI). This artificial neural network technology uses probabilistic graphical models and variational Bayesian methods. It has been tested successfully against a number of Zero Day threats like crypto jacking, HTTP flood attacks, etc.



Vulnerability Scanning

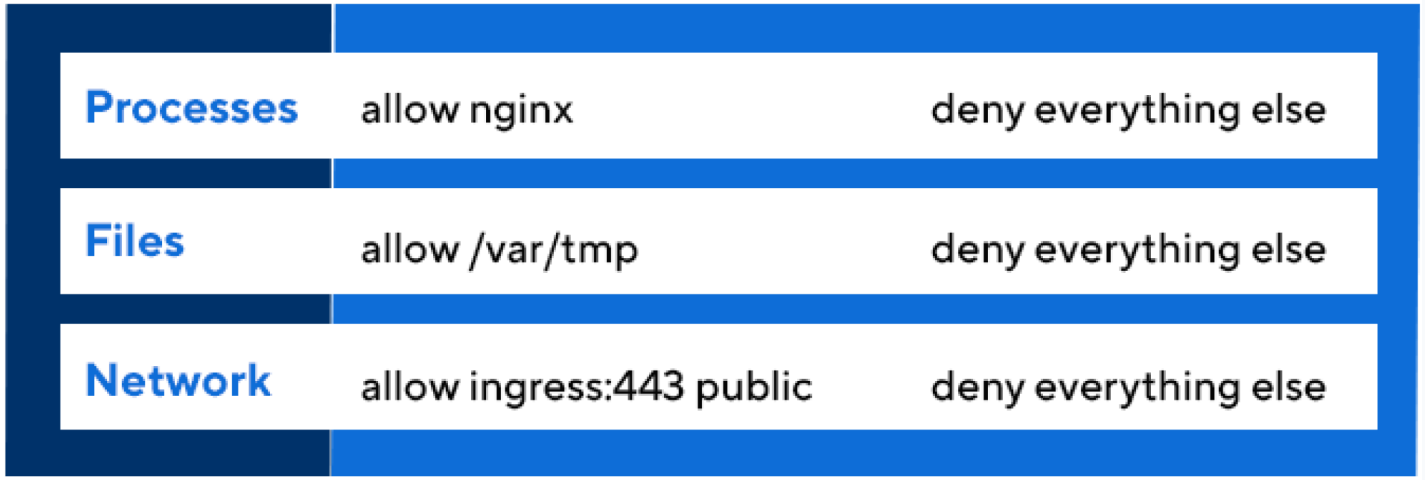
Reduce the risk of critical vulnerabilities in your environment.

The NSA and CISA Kubernetes hardening guide recommends Scanning containers and Pods for vulnerabilities or misconfigurations. AccuKnox helps you identify known vulnerabilities in images and pods before they are released into production. Understand the risks and implement monitoring, image assurance and runtime security policies to protect them.

Implementing Application Hardening, Application Firewalling

AccuKnox profiles and creates a baseline of policies by observing application at a fine grained level (Layer 3, 4, 7). Based on this AccuKnox comes up with White List, Least Privilege policies (what processes it can fork, what files it can access, acceptable network connections, etc). By denying access to everything else and allowing only these white list policies, AccuKnox delivers Application Firewalling, Application Hardening.

Sample Policy



AccuKnox

Requirement: Multi-cloud, Multi-platform Security

Monitor and protect your workloads however and wherever they run:
In Containers, Kubernetes, virtual machines, or bare metal. In private, public, hybrid cloud, edge or IoT, or even within 5G infrastructure.

AccuKnox develops API-first solutions with complete CLI and GUI support. These are available as SaaS or on-premises and support multiple platforms.

Platforms vary in specific features that are supported. Contact us to learn more about how AccuKnox can provide you with security observability and runtime protection.

ACCUKNOX

Security policy as code..

McKinsey, one of the top business and cybersecurity consulting firms noted in 2021:

1. Almost all breaches in the cloud stem from misconfiguration, rather than from attacks that compromise the underlying cloud infrastructure.

2. Traditional cybersecurity mechanisms were not designed to deliver security at the speed and agility that business leaders expect. Hence current business models require new security architectures and processes to protect their cloud workloads.

3. Infrastructure as code (IaC) has been highly effective at automating Cloud Systems deployment and streamline error-prone manual configurations. “Security as code” (SaC) is a natural progression of this concept and should be used for securing cloud workloads with speed and agility.

https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/security-as-code-the-best-and-maybe-only-path-to-securing-cloud-applications-and-systems

Zero Trust CNAPP Should Empower DevSecOps Teams

Developers

Gain critical insights into application behavior, validating 3rd party and open source software concerns
Address concerns from security via GitOps – without meetings
Enable security teams to implement specific controls with full visibility and approvals

Security

Set baseline security policies that move with workloads
Gain Security Visibility into changes in vulnerabilities and attack surface
Get real-time alerts to security incidents
Validate compliance with PCI, CIS Standards Quickly and confidently respond to CVEs and zero-day fire drills

Ops

Accelerate release cycles and reduce complexity of coordinating security and code changes
Automate and orchestrate workflows
Improve uptime and reliability with real-time telemetry
Agentless deployment reduces costs & complexity

AccuKnox Zero Trust – CNAPP

AccuKnox is one of the most comprehensive and modern platforms for implementing Zero Trust security in Cloud Native environments. Combining Static Security, Run-time Security, Remediation and Continuous Compliance, AccuKnox allows organizations to get to Zero Trust security and stay there in the most efficient and risk mitigated manner

PHASE	STATIC		RUN TIME		REMEDIATION		CONTINUOUS COMPLIANCE	
MODULES	Vulnerability Management	CSPM Cloud Security Posture Management	Observability	Anomaly Detection	SIEM Integration	SOAR Integration	Compliance, Governance Framework	
COMPLIANCE CONTROLS	Image Assurance Policies		Cloud Configuration Controls		MITRE		Workload Specific Controls	Dynamic Threat Analysis
	Cloud Controls – NIST, CIS and Hardening							
TOOLS	Workload Discovery	Workload Identification	SBOM Generation	Policies (auto-discovery, templates, workload specific recommendations)	Policy auto approval	Alert based on existing controls	3rd party thread feeds	

ACCUKNOX

Why AccuKnox

- One of the industry's most comprehensive Zero Trust CNAPP platforms
- Supports:
  - Public Clouds (AWS, GCP, Azure) and Private Clouds (OpenStack, Tanzu)
  - Modern (K8, Serverless) workloads
  - Traditional workloads (Virtual Machine, Bare Metal)
  - Futuristic workloads (IoT/Edge, 5G)
- Delivers Static and Runtime Security
- Solution anchored on innovations in Cloud Security, AI/ML-based Anomaly Detection (15+ patents)
- OpenSource, DevSecOps led delivery
- Ongoing R&D partnership with Stanford Research Institute

AccuKnox

Learn More at:

www.AccuKnox.com