HCLSoftware

Securing the Mission:

Integrating Application and Endpoint Security Across the Operational Lifecycle

HCLSoftware

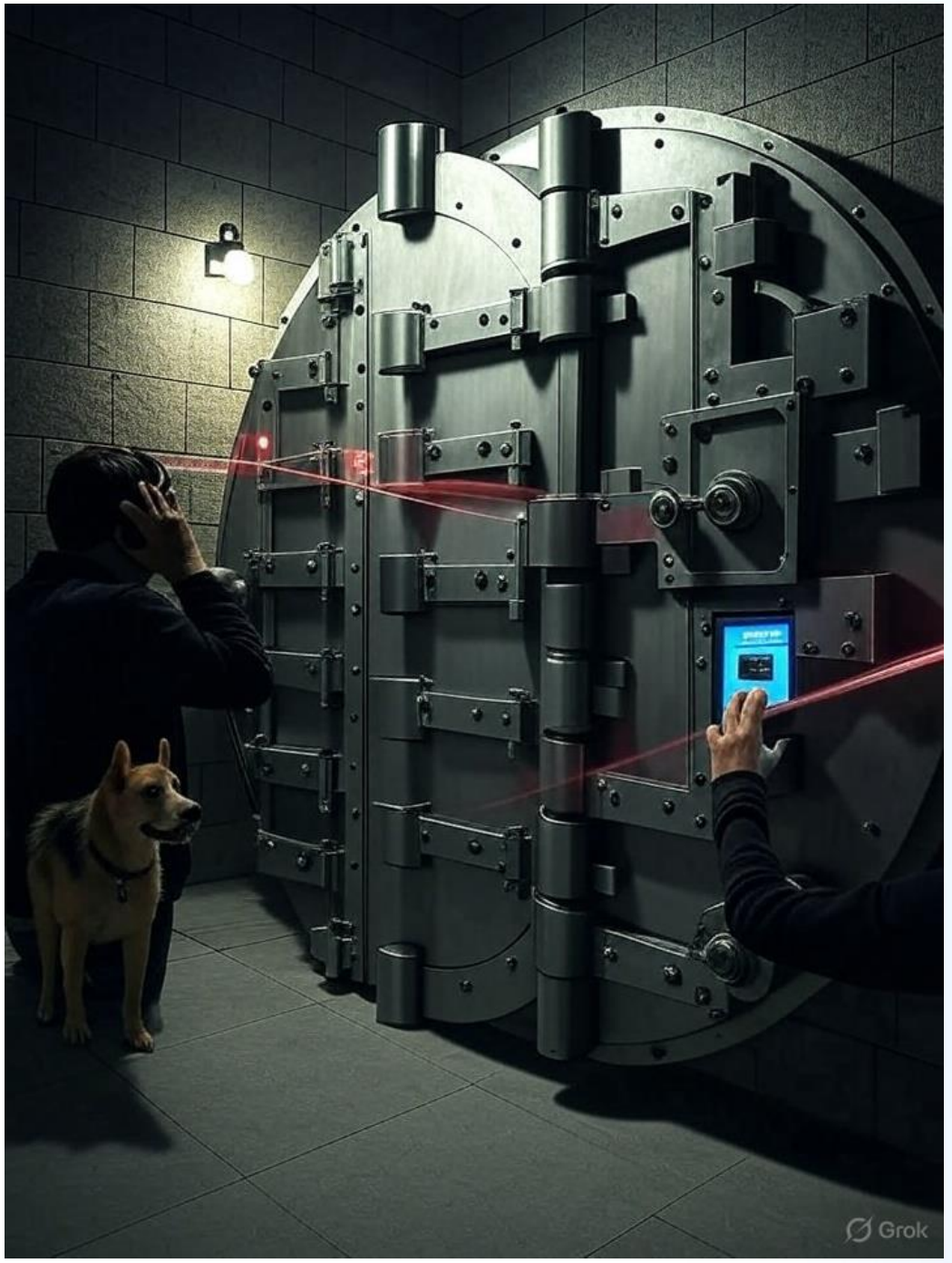
Speaker:
Rob Cuddy
HCLSoftware
rob.cuddy@hclfederal.com

Agenda

.

01	Level Set on Zero Trust	00
02	Inside Threats	00
03	Outside Threats	00
04	Visibility for Rapid Response	00

What did YOU think of when you first heard Zero Trust?



What We Think – Our Point of View on Zero Trust

- Traditional perimeter-based responses don't cut it anymore
  - You need faster – and better – responses

- KNOW, MONITOR and MAINTAIN security posture
  - Remove inherent trust relationships in IT networks
  - Assume no connection, device or identity is to be trusted, regardless of location.
  - Continuous diagnostics and monitoring, dynamic authentication, authorization and validation every user, device, application and connection - before granting access to a resource
    - Knowledge that goes beyond just an inventory.
    - Monitoring that goes beyond alerts
    - Visibility that leads to action

- In practice
  - Eliminate components that enable adversaries
  - Behavioral and Agentic: New technologies (e.g. LLMs) mean new unique threats and threat vectors
    - Go beyond traditional SAST and DAST to leverage AI for dynamic contextual testing

41-50K

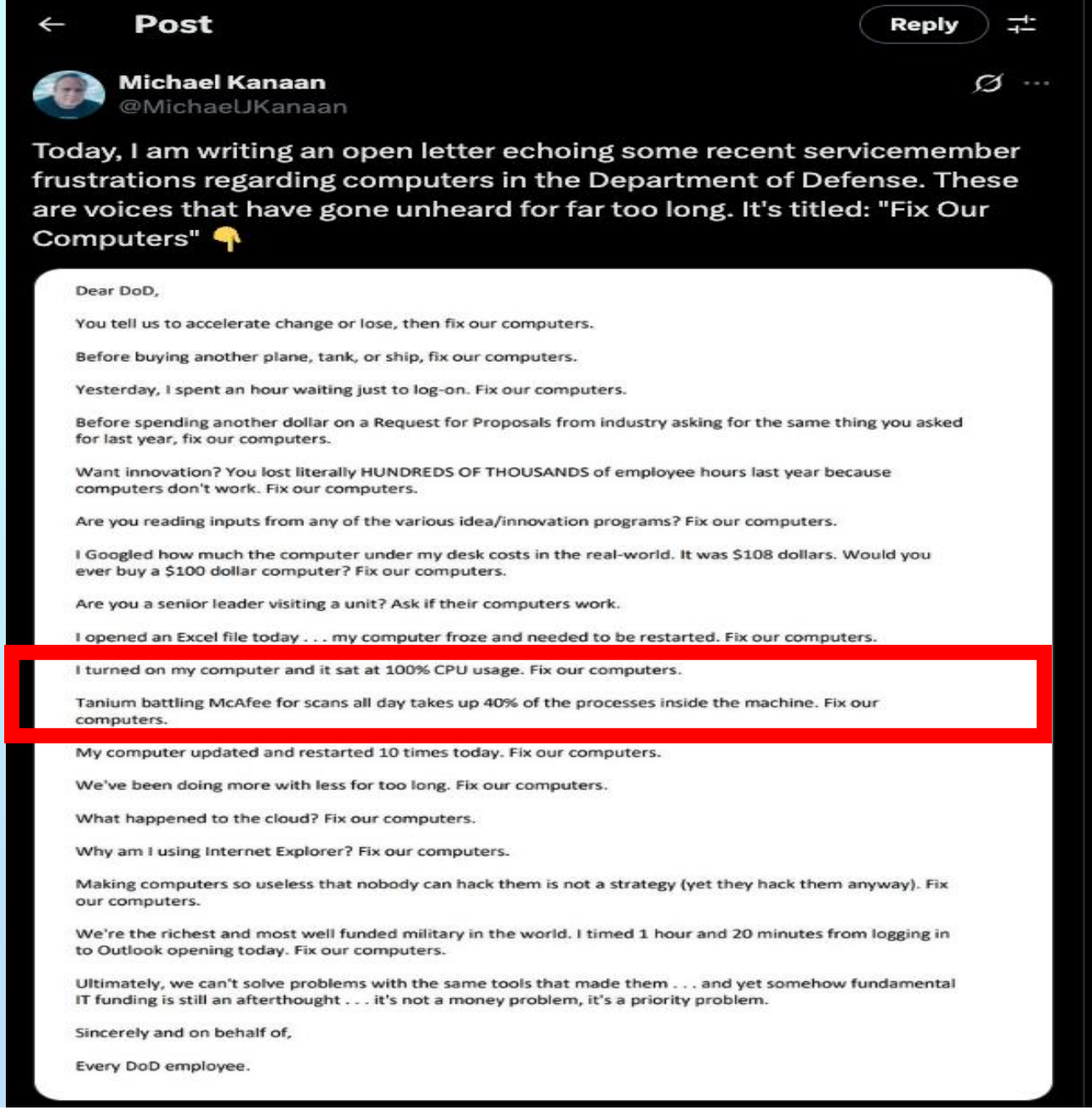
new weaknesses expected in 2025 – Forum of Incident Response and Security, from 2025 Application Security Benchmark by OX Security

95+%

AppSec alerts that are informational – 2025 Application Security Benchmark by OX Security

Why Care?

Anyone relate?



Where We Fit

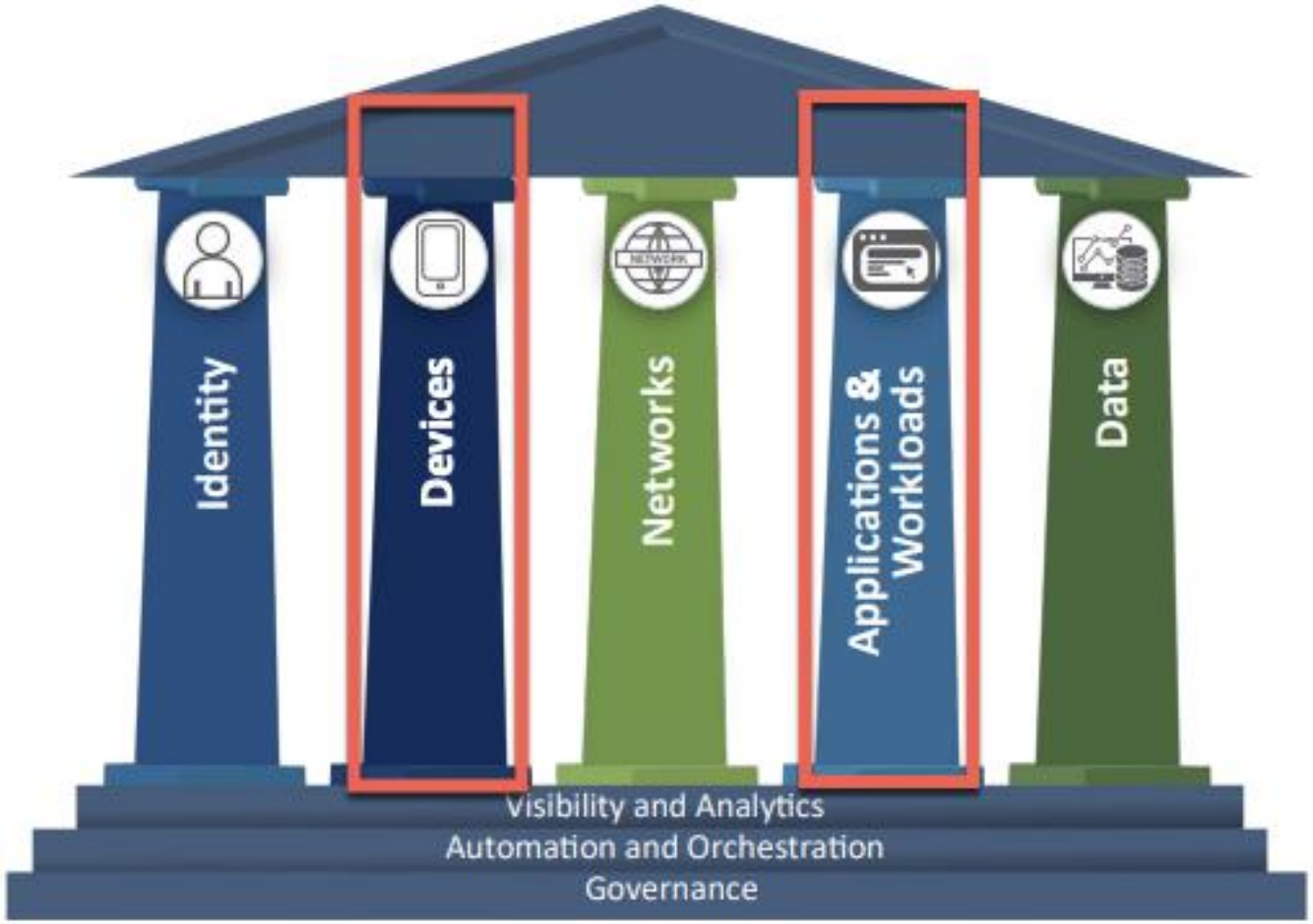


Figure 1: Zero Trust Maturity Model Pillars[8]

Principles from CISA: Applications

Table 5: Applications and Workloads

Function	Traditional	Initial	Advanced	Optimal
Application Threat Protections (Formerly Threat Protections)	Agency threat protections have minimal integration with application workflows, applying general purpose protections for known threats.	Agency integrates threat protections into mission critical application workflows, applying protections against known threats and some application-specific threats.	Agency integrates threat protections into all application workflows, protecting against some application-specific and targeted threats.	Agency integrates advanced threat protections into all application workflows, offering real-time visibility and content-aware protections against sophisticated attacks tailored to applications.
Accessible Applications (Formerly Accessibility)	Agency makes some mission critical applications[32] available only over private networks and protected public network connections (e.g., VPN) with monitoring.	Agency makes some of their applicable mission critical applications available over open public networks to authorized users with need via brokered connections.	Agency makes most of their applicable mission critical applications available over open public network connections to authorized users as needed.	Agency makes all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed.
Secure Application Development and Deployment Workflow (New Function)	Agency has ad hoc development, testing, and production environments with non-robust code deployment mechanisms.	Agency provides infrastructure for development, testing, and production environments (including automation) with formal code deployment mechanisms through CI/CD pipelines and requisite access controls in support of least privilege principles.	Agency uses distinct and coordinated teams for development, security, and operations while removing developer access to production environment for code deployment.	Agency leverages immutable workloads where feasible, only allowing changes to take effect through redeployment, and removes administrator access to deployment environments in favor of automated processes for code deployment.
Application Security Testing (Formerly Application Security)	Agency performs application security testing prior to deployment, primarily via manual testing methods.	Agency begins to use static and dynamic (i.e., application is executing) testing methods to perform security testing, including manual expert analysis, prior to application deployment.	Agency integrates application security testing into the application development and deployment process, including the use of periodic dynamic testing methods.	Agency integrates application security testing throughout the software development lifecycle across the enterprise with routine automated testing of deployed applications.

Principles from CISA: Devices

Table 3: Devices Pillar

Function	Traditional	Initial	Advanced	Optimal
Policy Enforcement & Compliance Monitoring (New Function)	Agency has limited, if any, visibility (i.e., ability to inspect device behavior) into device compliance with few methods of enforcing policies or managing software, configurations, or vulnerabilities.	Agency receives self-reported device characteristics (e.g., keys, tokens, users, etc., on the device) but has limited enforcement mechanisms. Agency has a preliminary, basic process in place to approve software use and push updates and configuration changes to devices.	Agency has verified insights (i.e., an administrator can inspect and verify the data on device) on initial access to device and enforces compliance for most devices and virtual assets. Agency uses automated methods to manage devices and virtual assets, approve software, and identify vulnerabilities and install patches.	Agency continuously verifies insights and enforces compliance throughout the lifetime of devices and virtual assets. Agency integrates device, software, configuration, and vulnerability management across all agency environments, including for virtual assets.
Asset & Supply Chain Risk Management (New Function)	Agency does not track physical or virtual assets in an enterprise-wide or cross-vendor manner and manages its own supply chain acquisition of devices and services in ad hoc fashion with a limited view of enterprise risks.	Agency tracks all physical and some virtual assets and manages supply chain risks by establishing policies and control baselines according to federal recommendations using a robust framework, (e.g., NIST SCRM.)[25]	Agency begins to develop a comprehensive enterprise view of physical and virtual assets via automated processes that can function across multiple vendors to verify acquisitions, track development cycles, and provide third-party assessments.	Agency has a comprehensive, at- or near-real-time view of all assets across vendors and service providers, automates its supply chain risk management as applicable, builds operations that tolerate supply chain failures, and incorporates best practices.
Resource Access (Formerly Data Access)	Agency does not require visibility into devices or virtual assets used to access resources.	Agency requires some devices or virtual assets to report characteristics then use this information to approve resource access.	Agency's initial resource access considers verified device or virtual asset insights.	Agency's resource access considers real-time risk analytics within devices and virtual assets.

Why We Care: Better Help To Empower the Warfighter
Accelerate delivery of critical software capabilities

Challenges from Commission on Software Defined Warfare

Enable Security at Speed

"There is a major shortfall of software pipelines, talent and resources to meet the demand for software-defined warfare within DoD organizations."

Support A Diverse Industrial Base

"The absence of a software-centric culture across the DoD impedes the employment of modern DevSecOps, which fosters rapid iterations"

Recommendations:

Working with testers and certifiers to understand cybersecurity, integration and other factors to assess the risks and processes of using the software in the defense domain

"… These factories should enable increased speed and quality of deploying code to various environments while maintaining interoperability and cybersecurity…"

HCLSoftware

Inside Threats

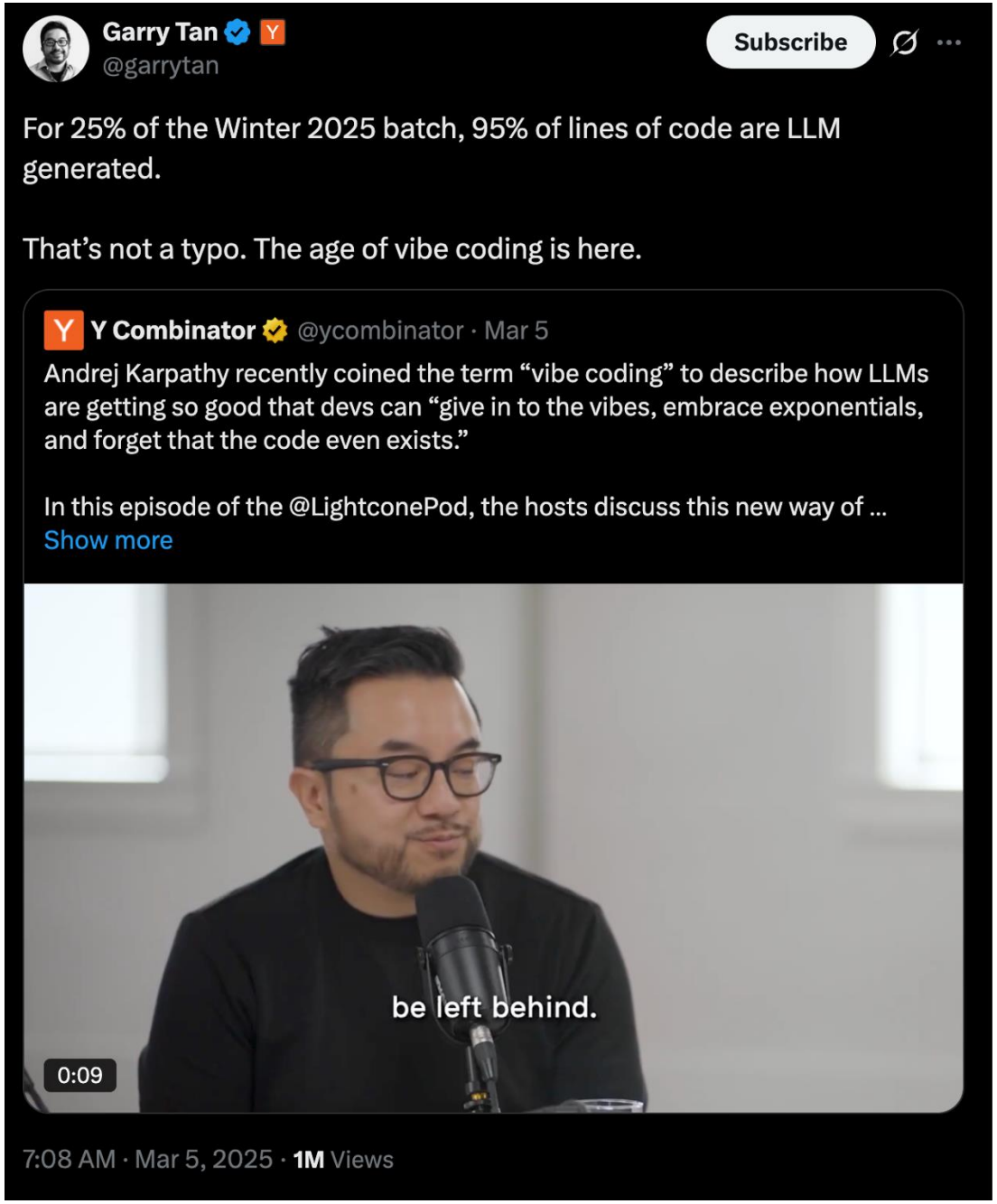
Big AppSec Threat Areas Today

Vibe coding

66%

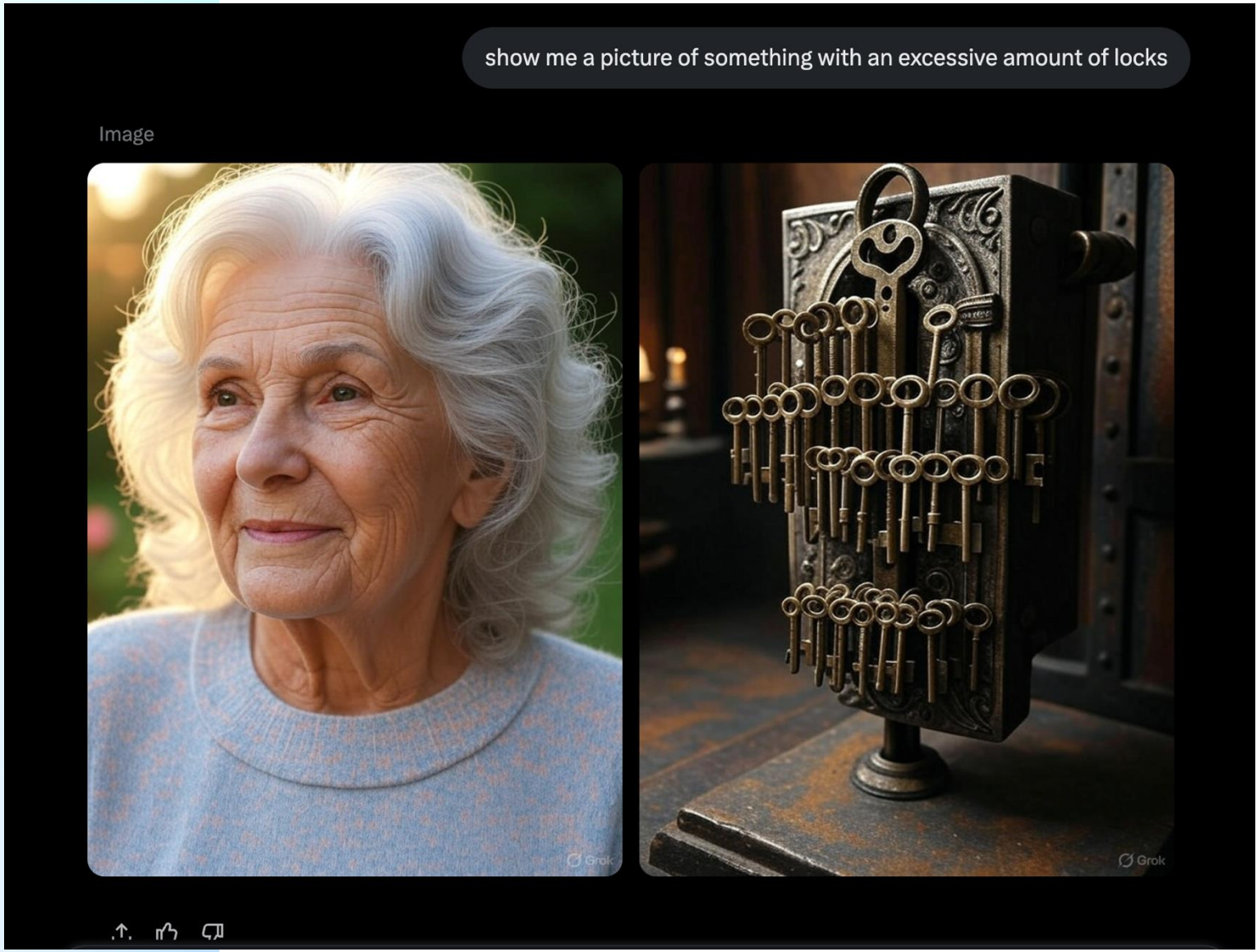
Percentage of developers who say they do not trust the output or answers

Source: 2024 Stack Overflow Developer Survey
Response on Challenges with AI at Work

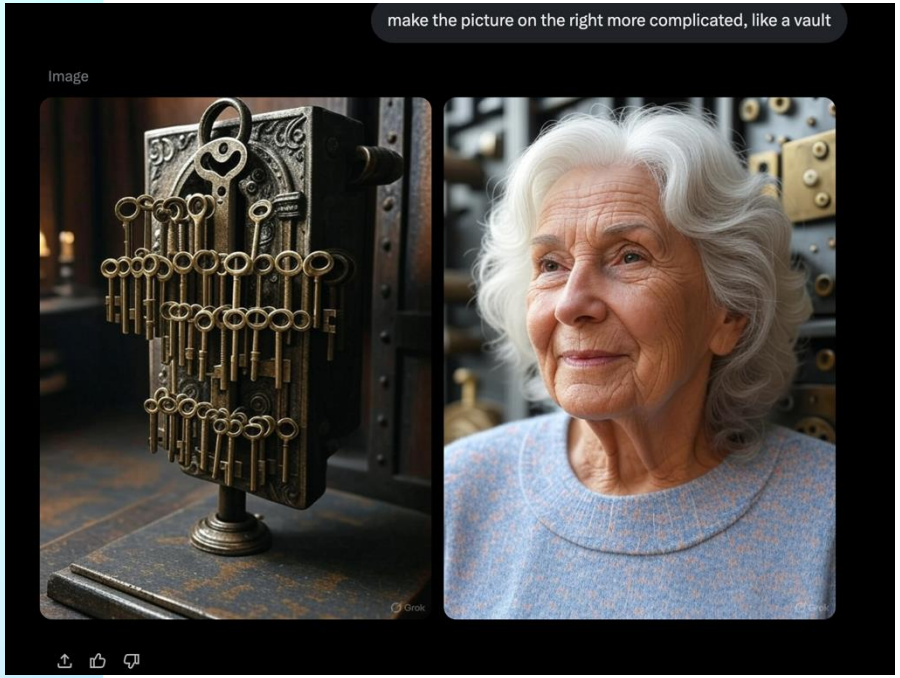


Funny Example of How I Know We Still Have a Long Way to Go…

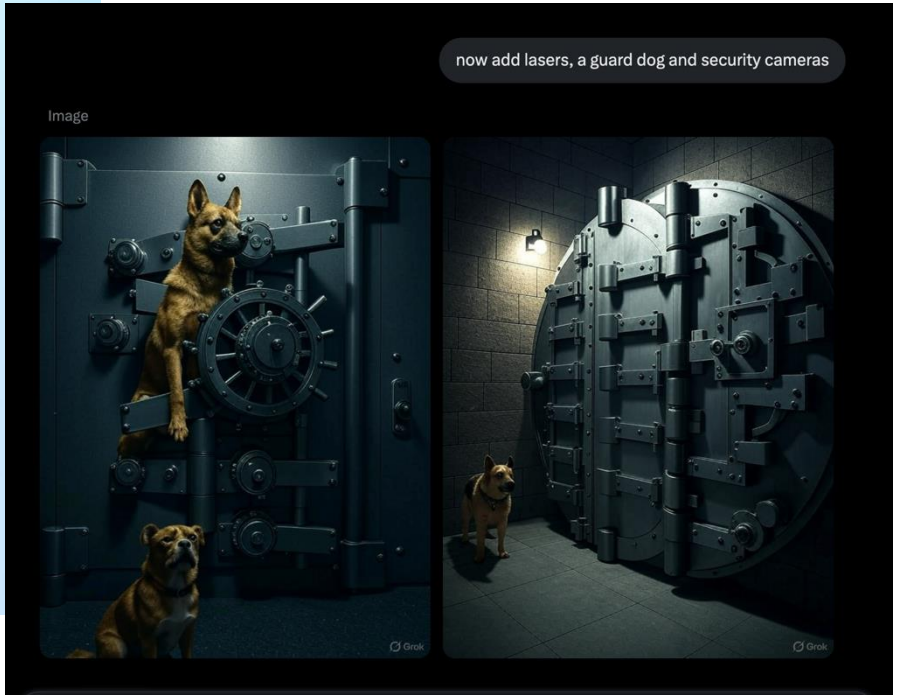
Remember that Zero trust image from earlier? This is the first prompt that I tried…



… And the 2nd attempt didn't go much better…



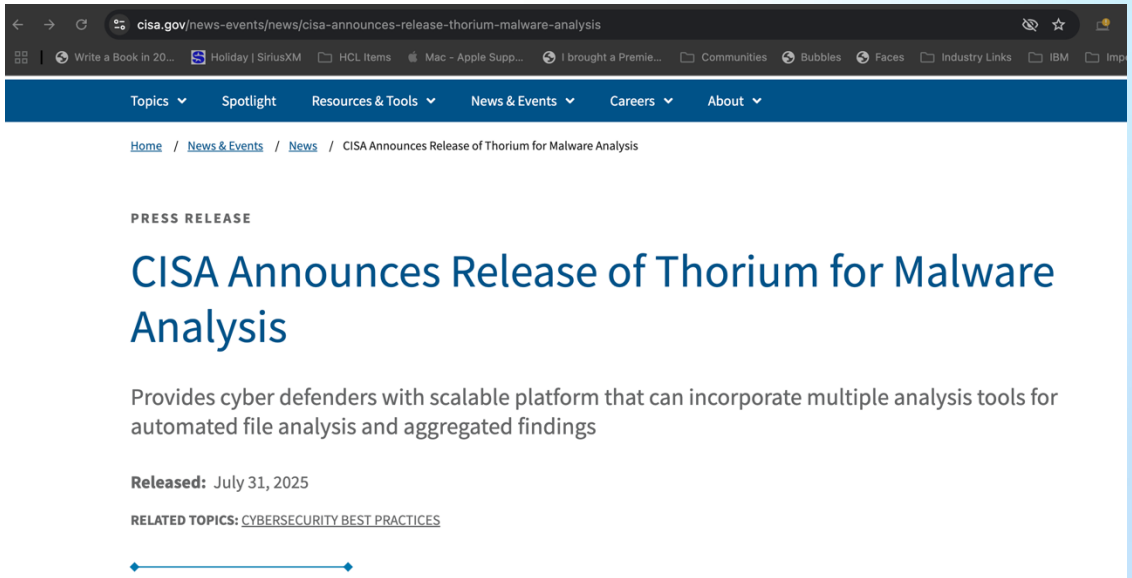
… After an attempt to show a complicated vault, this was my favorite one …

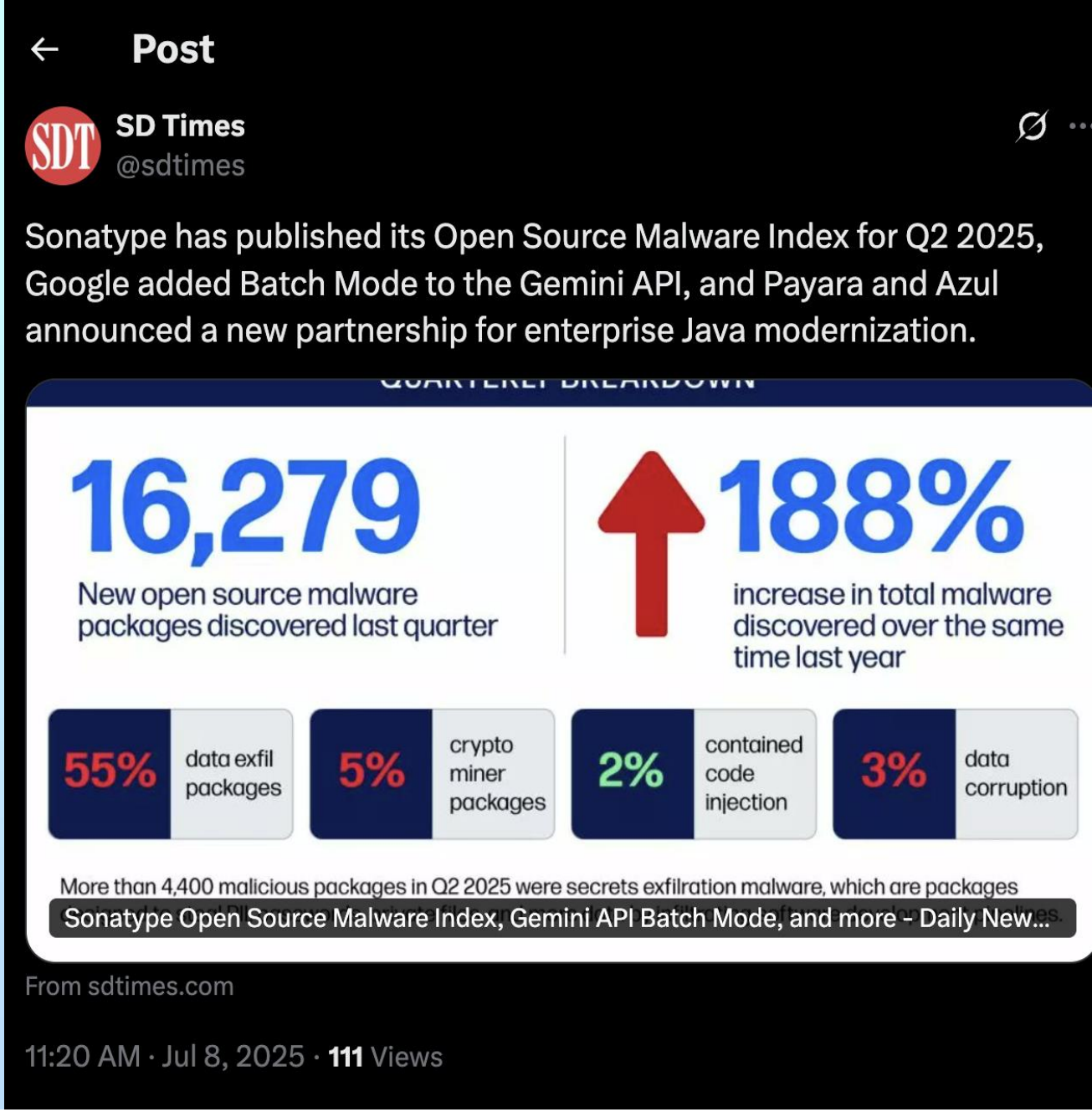


Big AppSec Threat Areas Today

Open Source:

Still enough of a problem that CISA announced a new forensics utility to help





Big AppSec Threat Areas Today

APIs:

Percentage of CISOs with full visibility and tracking for API Landscape

19%

Percentage and Frequency at which APIs are updated …

75%

every 2 weeks

BUT

Percentage of Organizations that have a Continuous auditing Frequency for their APIs

34%

Big AppSec Threat Areas Today

Software Supply Chain:

45%

organizations worldwide expected to experience attacks on their software supply chains
3x rise from 2021.
Source: Gartner Cybersecurity Trends

Equally, a recent study by Juniper estimates cyberattacks targeting software supply-chain could cost organizations an estimated $81 billion in lost revenue and damages annually by 2026.

NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PUBLICATIONS

NIST SP 800-218

Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities

Date Published: February 2022

Supersedes: CSWP 13 (04/23/2020)

Author(s)

Murugiah Souppaya (NIST), Karen Scarfone (Scarfone Cybersecurity), Donna Dodson

Abstract

Few software development life cycle (SDLC) models explicitly address software security in detail, so secure software development practices usually need to be added to each SDLC model to ensure that the software being developed is well-secured. This document recommends the Secure Software Development Framework (SSDF) – a core set of high-level secure software development practices that can be integrated into each SDLC implementation. Following these practices should help software producers reduce the number of vulnerabilities in released software, mitigate the potential impact of the exploitation of undetected or unaddressed vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences. Because the framework provides a common vocabulary for secure software development, software purchasers and consumers can also use it to foster communications with suppliers in acquisition processes and other management activities.

DOCUMENTATION

Publication:

https://doi.org/10.6028/NIST.SP.800-218

Download URL

Potential updates (xlsx)

Translations

Supplemental Material:

SP 800-218 Table in Excel (xlsx)

Delta from April 2020 paper (docx)

Delta from September 2021 public draft (docx)

SSDF Project homepage

Executive Order 14028, Improving the Nation's Cybersecurity

Publication Parts:

SP 800-218A

HCLSoftware

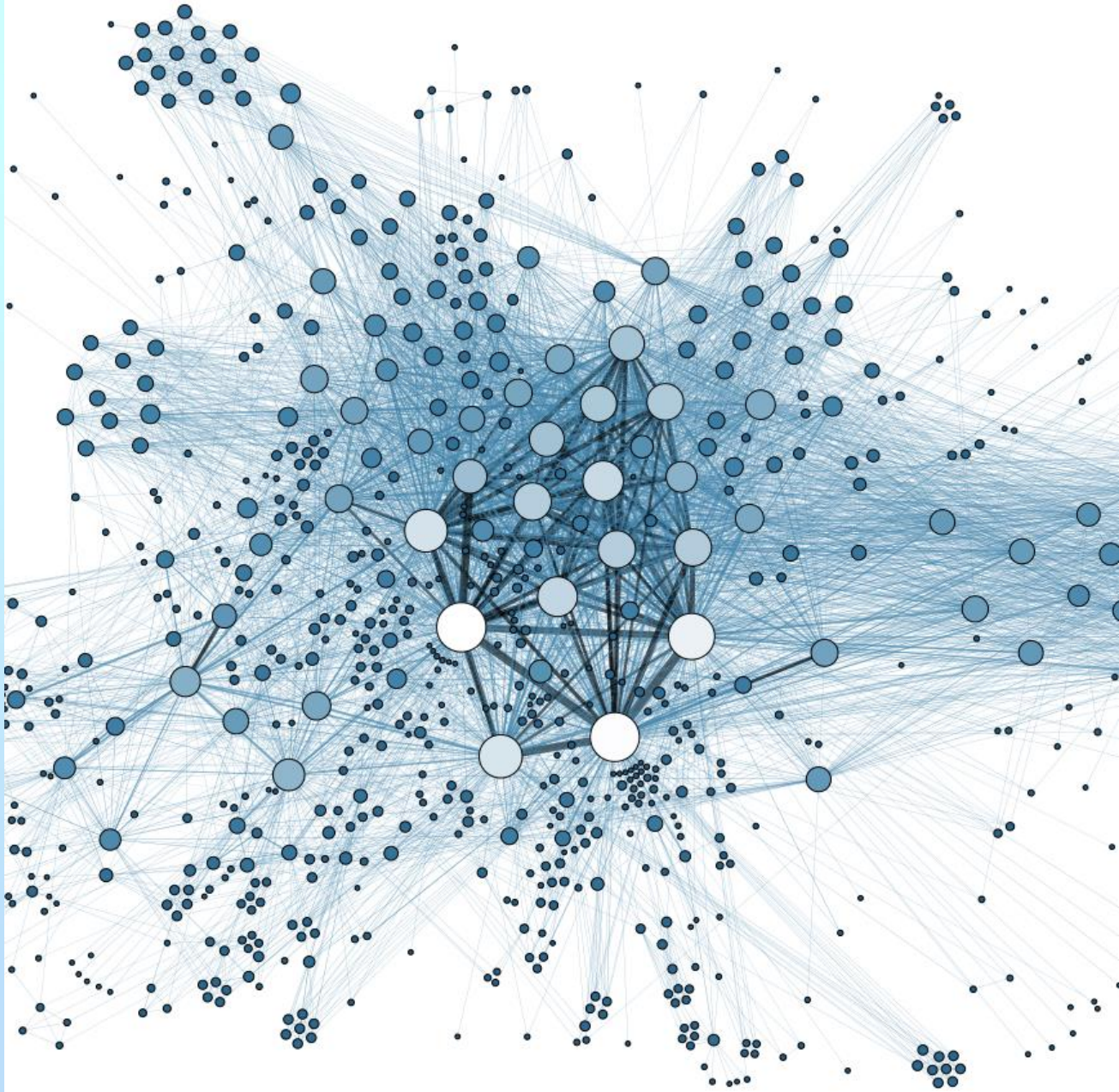
Outside Threats

Big Threats Today:

Who's Using What?

&

It's All Connected!

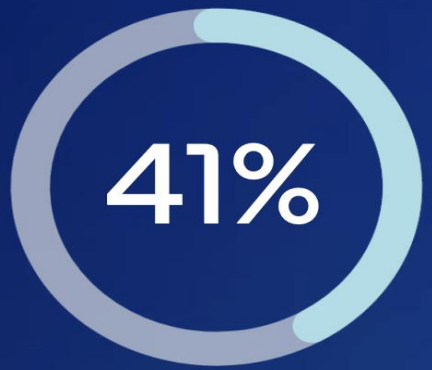


Prepare Your Endpoints For Zero Trust Compliance

Its core concept of "never trust, always verify" helps you discover vulnerable endpoints to mitigate threats.

3 Reasons Zero Trust is Gaining Steam:

of 815 enterprise executives say they will use Zero Trust network architecture for all endpoints by 2026[1]

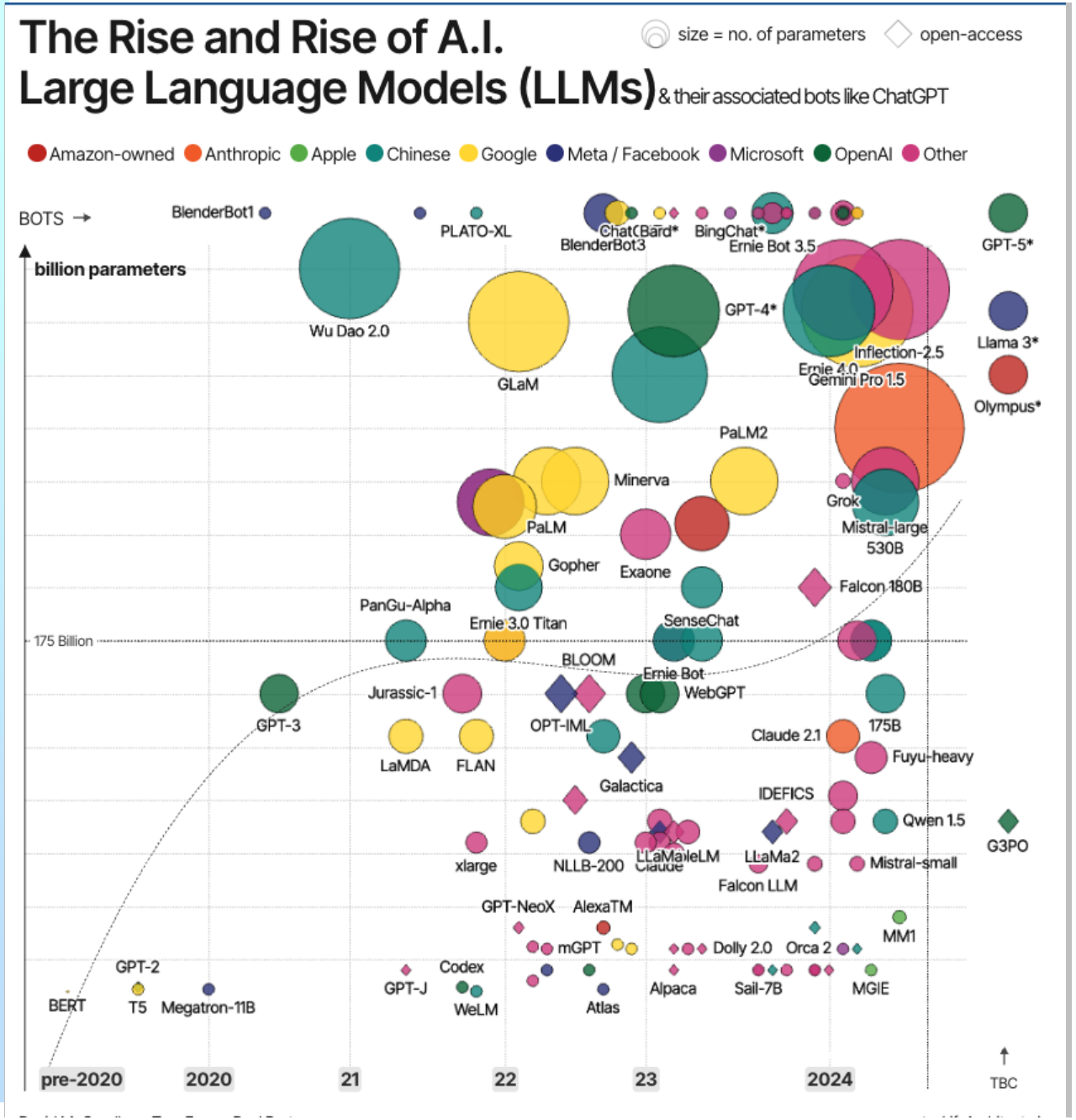


of organizations surveyed in 2022 reported they have already deployed a Zero Trust approach, compared to 35% in 2021[2]

of 300 IT decision-makers cited ransomware threats, and 53% cited remote worker risks as top Zero Trust drivers[3]

HCLSoftware

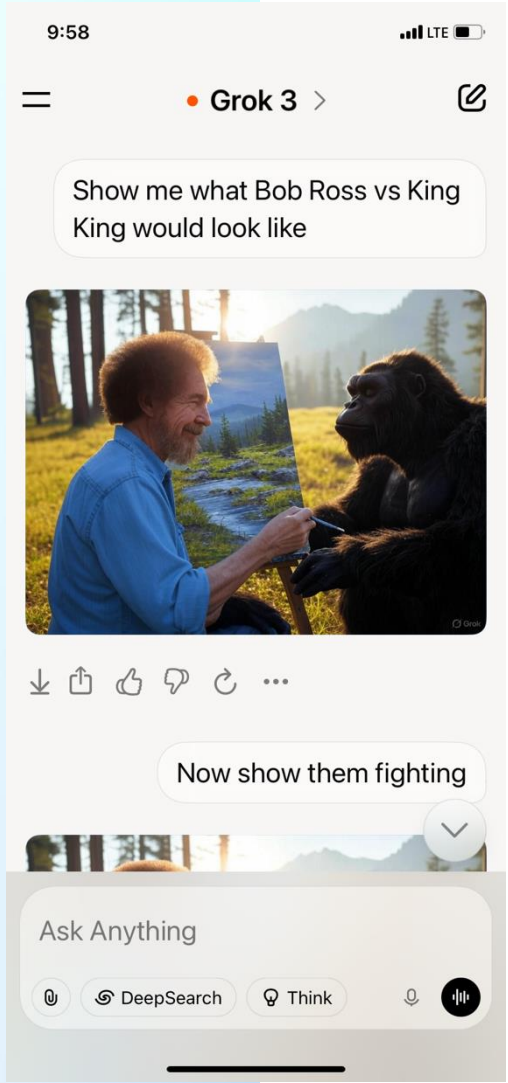
Where'd *THAT* Prompt Come From?

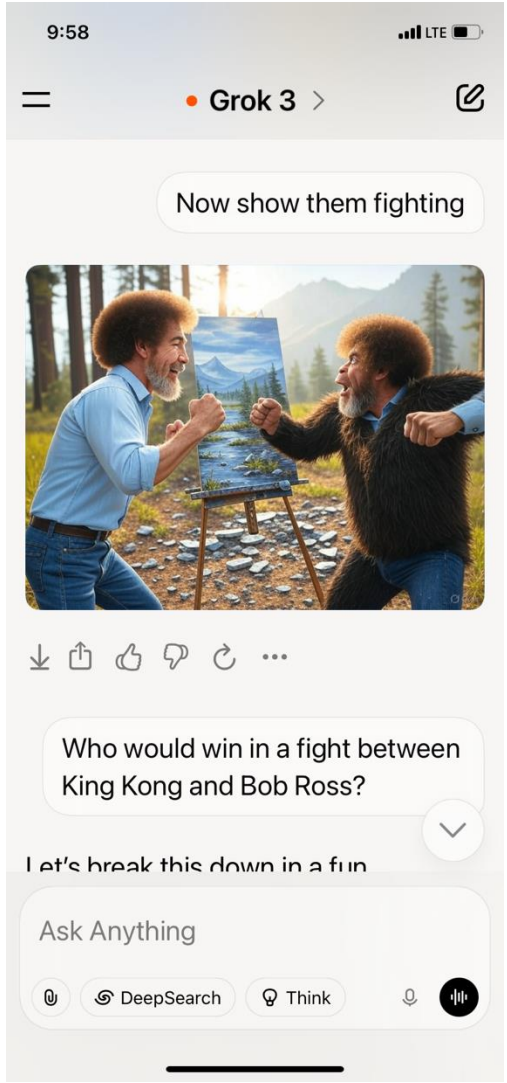


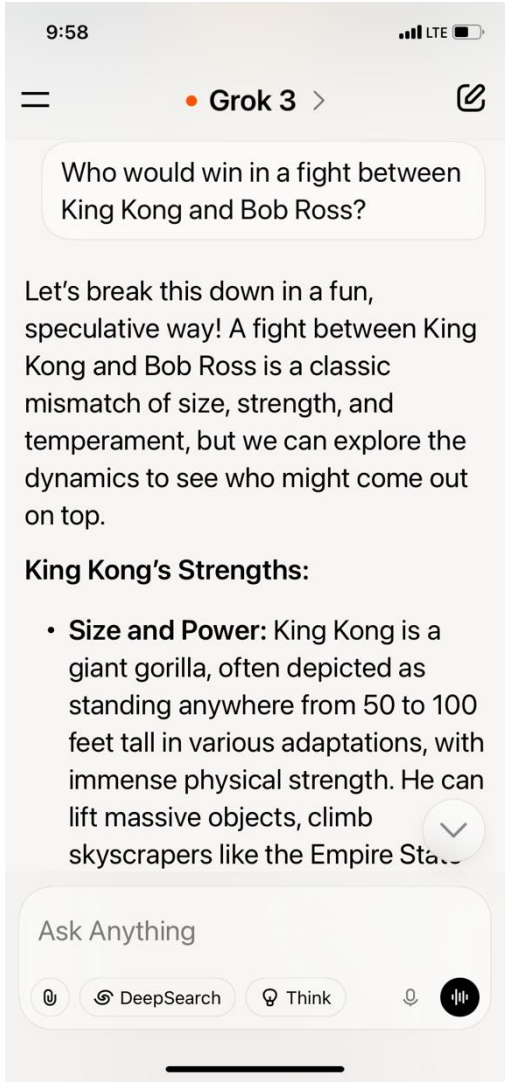
Why is Resource Protection So Important?

What'cha talkin' 'bout Willis?

Did Someone Say Hallucinations?







HCLSoftware

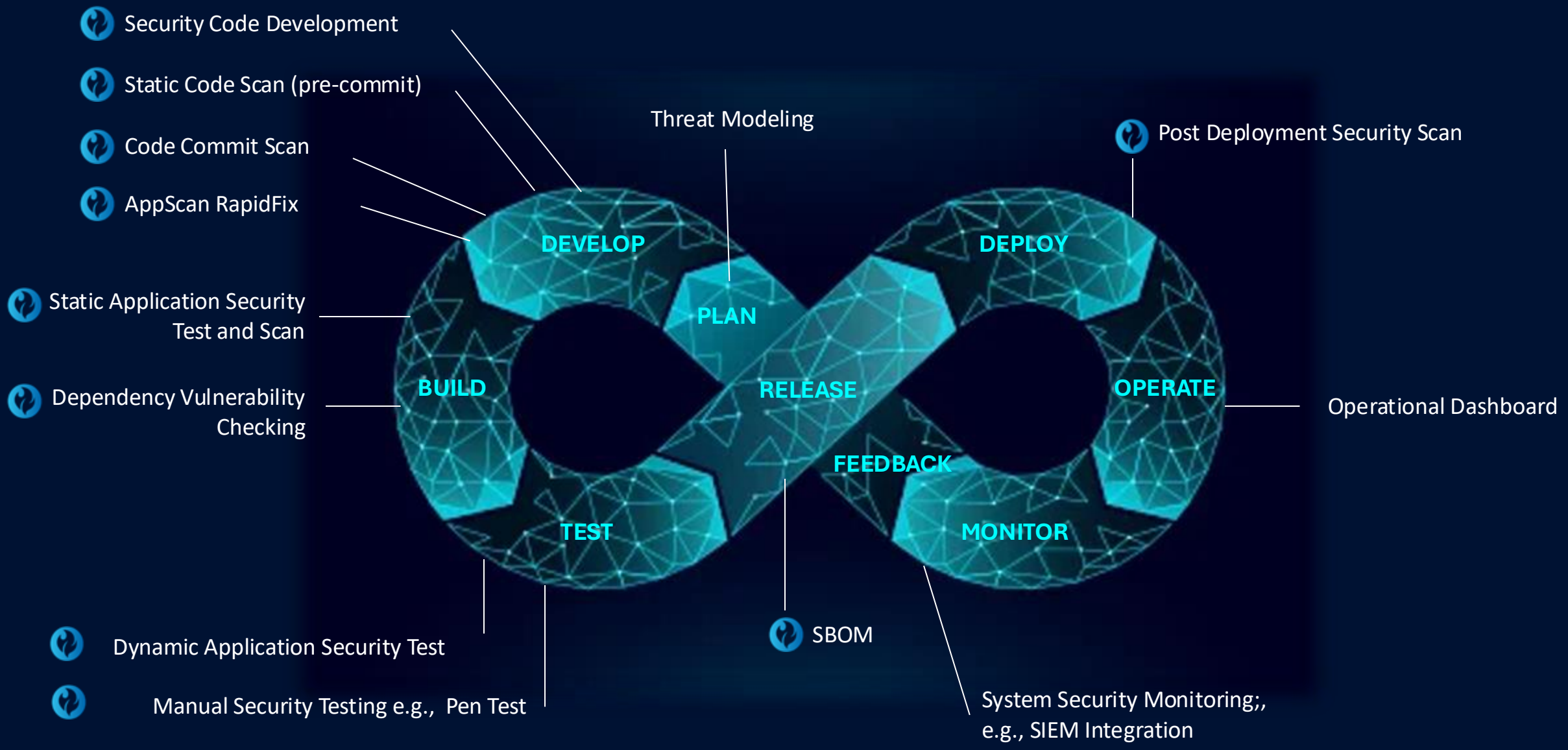
But Rob, what do we DO???

How We Can Help

HCLSoftware

Raise Visibility for Rapid Response

HCL AppScan 360º:
A Scalable Application Security Platform



Report data in real-time and build a score-based trust algorithm.

Proactively monitor and measure the security posture and integrity of all owned and unmanaged devices connecting to your resources.

HCL BigFix

CAPABILITIES

Automatically apply patches and update configurations that aren't secure.

Instantly change access policies and close endpoints.

Automatically collect telemetry about the state of assets, network infrastructure, and communications to improve your security posture,

Continuous Diagnostics and Mitigation for Endpoints

- Collect telemetry to assess endpoint security and integrity
- Update Device configurations and settings AUTOMATICALLY
- Change access policies dynamically to isolate vulnerable or compromised resources

As a leader in endpoint management, here's how BigFix supports Zero Trust per the NIST 800-207 compliance standard:

- 2.1.5 – Continuously **measure and monitor** the integrity and security posture of your owned and associated assets.

- 2.1.7 – **Collect as much information** as possible about the current state of assets, network infrastructure and communications and use this information to improve your security posture.

- 3.0 – Deploy a **Continuous Diagnostics and Mitigation (CDM)** system to gather information about the current state of your enterprise assets, and **apply necessary updates** to configuration and software components.

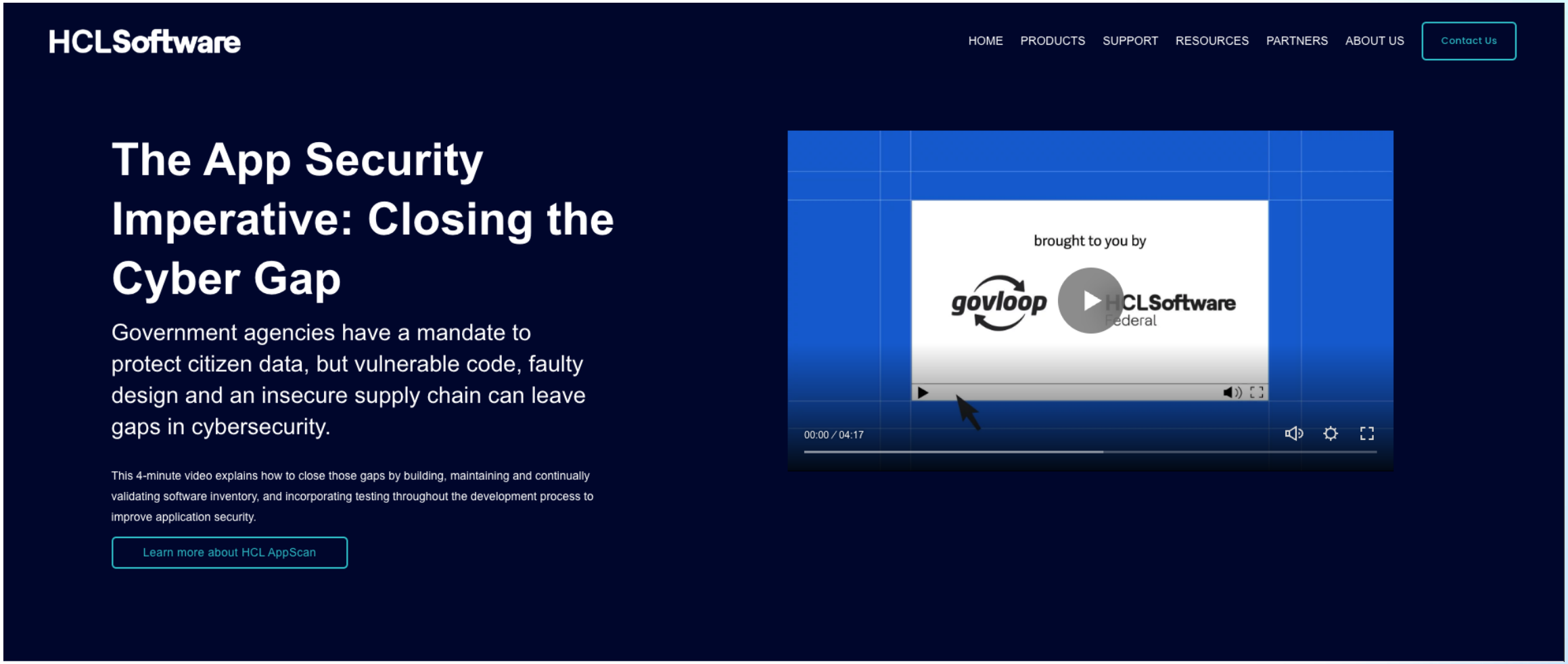
- 3.1 – Deploy an industry compliance system to ensure the enterprise remains compliant with any regulatory requirements.

- 3.3 – Feed information into your enterprise's ZTA Trust Algorithm, to provide known status updates and **ensure continuous policy enforcement**.

Big Fix stands ready to help you meet **industry-specific policy requirements** to ensure regulatory compliance, all through the lens of Zero Trust.

How to Contact Us – visit us at hclfederal.com

Check out our new video: https://www.hclfederal.com/govloop-appsec



HCLSoftware