Trinity Cyber

Compliance and Mandates Overview

Gartner
COOL VENDOR 2020

Trinity Cyber Helps You Comply

Trinity Cyber’s cutting edge technology addresses imposed requirements to improve security for federal agencies including mandates to run break and inspect technology at agency network edges, directives to mitigate against CISA’s Known Exploited Vulnerability (KEV) catalog, executive orders and other unfunded mandates. We have outlined each general area and how Trinity Cyber can help your agency immediately comply with evolving requirements.

The Biden Administration's Executive Order on Cybersecurity

On May 12, 2021, the Biden Administration issued an executive order on improving the nation's cybersecurity. Trinity Cyber delivers powerful technology that can protect federal agencies from the threats highlighted in the Biden Administration's executive order on cybersecurity.

We are uniquely positioned to assist agencies in addressing many aspects of the Executive Order.

Zero Trust

- Trinity Cyber advances Zero Trust initiatives allowing organizations to manage their network security under the assumption everything entering their environment is already compromised.
- Our game-changing technology identifies and removes malicious tactics and content from your Internet traffic before it infiltrates your network with powerful, automated responses beyond block and alert.
- We not only detect and neutralize individual attacks, we also uncover the strategies and methods used by the attackers.

Hunting Capability

- In addition to our active sensor, Trinity Cyber performs continuous, passive, deep content threat hunting and detection on network traffic – beyond log entry.
- Threat hunting is foundational to our threat discovery capabilities. Our service comes with a team of analysts and malware reverse engineers that develop and deploy customized active formulas to efficiently expose and neutralize threats.
- Our team continuously monitors network traffic to uncover and disrupt the strategies and methods used by attackers.
- Our continuous approach to threat hunting and monitoring is vital to the creation of the formulas we employ to protect your enterprise.

Reduced Supply Chain Risk

- Internet traffic protected by the Trinity Cyber solution is moved through our infrastructure at Internet Layer 2.
- All our code development, command and control, and storage/processing of client-specific (or derived) data occurs on a private, self-hosted, out-of-band network with all transport CNSA/Suite B encrypted.
- Through this approach, we reduce the risk of third-party supply chain compromise, decrease the potential risk of attacks, and minimize potential corruption or vulnerabilities caused by an insecure code base.

Code Security Assurance

- Trinity Cyber writes and deploys its own code on a segregated network.
- We take secure coding seriously and apply stringent secure coding principles, techniques, and processes into all offerings we produce.
- A few examples of our rigorous code quality practices include automated static and dynamic code quality tools enforcing defensive coding standards and a robust peer review before code merges.

CISA Binding Operational Directive (BOD) 22-01 – Reducing the Significant Risk of Known Exploited Vulnerabilities

- On November 3, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) issued Binding Operational Directive (BOD) 22-01, establishing timeframes for civilian agencies to implement remediations for nearly 300 vulnerabilities actively exploited by known adversaries.
- By adding Trinity Cyber to your existing Managed Trusted Internet Protocol Service (MTIPS) or Trusted Internet Connection (TIC), your agency will have 95% of network-based CVEs, which equates to more than half of the 300 vulnerabilities in the BOD fully mitigated overnight.
- Trinity Cyber focuses soley on tactics, techniques, and procedures (TTPs) – which adversaries rarely (if ever) change. Traditional Intrusion Prevention Systems (IPS), Next Generation Firewalls (NGFW) and Secure Web Gateways (SWG) use static indicators of compromise (IOCs) that are regularly evaded, require constant updating, generate alerts baed on inferences, and produce high false positive rates.

EO 14028 – Improving the Nations Cybersecurity

- Public and private threat sharing – Trinity Cyber's service line offers a unique opportunity for agencies to share threat information without compromising sensitive information.
- Modernize and improve security – Trinity Cyber's technology is the first to deeply inspect and edit full session Internet traffic – at line rate speed and in both directions –to remove or alter hacking techniques.
- Improve supply chain security – Trinity Cyber's unique out-of-band management, completely managed service, and ground-up developed software provide the ultimate in supply chain protection.
- Improve incident detection – Trinity Cyber is true threat detection and automated prevention.
- Improve investigation and remediation – Trinity Cyber remediates the threats in real-time reducing alert fatigue and backlog.

M-21-31 – Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

- Capture outlined log information – Our solution meets the logging requirements of M-21-31.
- Inspect encrypted data (break and inspect) – This is a key tenant of the Trinity Cyber solution and enables agencies to meet and exceed Event Logging tier 2 requirements for implementation of encrypted traffic inspection.
- Automation – Trinity Cyber automates the threat prevention.

CISA BOD 22-01 – Reducing the Significant Risk of Known Exploited Vulnerabilities

- Trinity Cyber mitigates 95% of the current (and continuously growing) list, allowing operators time to test and apply patches on their schedule.

CISA Emergency Directive 22-03 – Mitigate VMware Vulnerabilities

- Trinity Cyber mitigates 95% of the current and growing list of network observable vulnerabilities.

M-22-09 – Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

- Identity – Trinity Cyber adds Zero Trust to Internet access by allowing organizations to manage their network security under the assumption everything entering and exiting their environment is already compromised.
- Devices – Prevention and detection of incidents on devices – Trinity Cyber prevents incidents before they get to the device.
- Applications and Workloads – Rather than operating at the application layer, Trinity Cyber does deep full content, full session inspection at Layer 2 and assumes Zero Trust down to the byte level.
- Data – Trinity Cyber provides full logging of its cyber-mitigation actions and can natively integrate with the most popular SIEM and SOAR tools through APIs or pre-built connectors.

M-19-26 – Update to the Trusted Internet Connections (TIC) Initiative

- One of the tenants of this memo is agencies performing full packet capture and leveraging SaaS solutions. Trinity Cyber and our partners can provide both functions.
- As a carrier grade threat mitigation and prevention solution, Trinity Cyber has been architected to sit at the TIC Internet Access Points (IAPs) of your organization to offer full inspection and protection of your inbound and outbound data.
- Because Trinity Cyber's solution set sits inline and performs actions automatically with sub-second latency, it facilitates the delivery of mission capabilities.

For more information about how Trinity Cyber can help you achieve compliance quickly, contact us today at **info@trinitycyber.com**.

About Trinity Cyber

Trinity Cyber, Inc. is a U.S. based corporation that invents and operates technology to solve the most difficult cyber security challenges. We invented and patented the Trinity Cyber Engine the first technology to deeply inspect and edit full session Internet traffic—at line rate speed and in both directions—to remove or alter hacking techniques. Our products and services range across several multi-billion-dollar segments. We are solving the biggest challenges for customers today with better security, virtual vulnerability mitigation, reduced alert fatigue and fewer false positives.

Gartner

COOL
VENDOR
2020

Trinity Cyber was named a Cool Vendor in Gartner’s Cool Vendors in Network and Endpoint Security, Mark Harris, Rob Smith, et al., Sept. 30, 2020.
The GARTNER COOL VENDOR badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

trinitycyber.com