DEVICE AUTHORITY™
Edge to Enterprise IoT Security

Protect your legacy devices against the heightened threat of cybercrime

"The trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced."
U.S. Presidential Executive Order, May 2021

We couldn't have said it better ourselves! The modern approach to cybersecurity is Zero Trust – don't place all faith into a single component, ensure you have a backup, spread risk and authenticate often. Typical IoT solutions & devices rely on standard approaches to authentication, such as PKI certificates, which offers a way to verify device identity for network systems & applications.

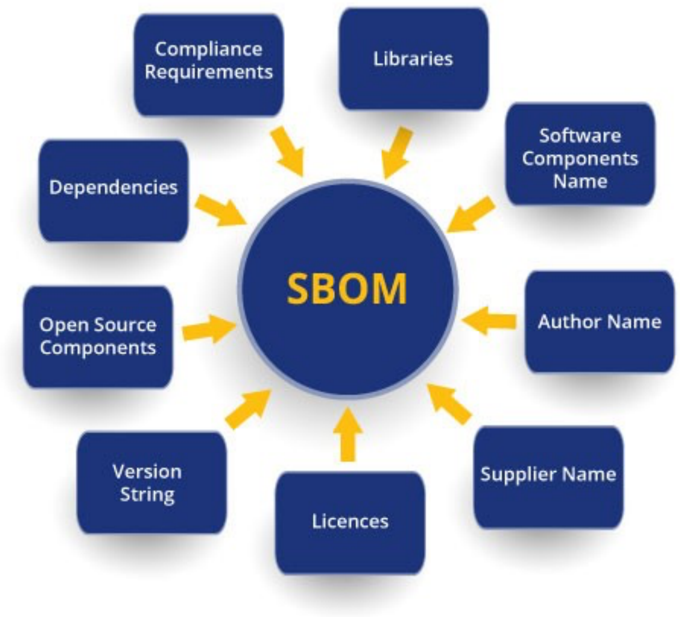
However, many other systemic issues such as firmware bugs, cloning, or missed maintenance SLAs can mean the device and its data is not trustworthy. A device with a legitimate certificate can still pose serious security and compliance risks to an organization since rogue software or malfunctioning equipment will have privileged access to the network and enterprise resources.

Rogue or malfunctioning software is difficult to spot, and often stems from the lack of transparency in development of commercial software. A one-shot security evaluation or pen test is not enough – proof of security and safety must accompany *any* software throughout its useful lifespan.

Biden's Executive Order calls to equip federal users with a new defense that will deliver trust through transparency: the SBOM.

What is an SBoM?

- A Software Bill Of Materials (SBOM) is a list of components in a piece of software.
- SBOMs allow the **manufacturer** of a product to make sure those components are up to date and to respond quickly to new vulnerabilities.
- **Buyers** can use an SBOM to perform vulnerability or license analysis, both of which can be used to evaluate risk in a product.



For example, the Ripple20 vulnerability was found to affect a Transmission Control Protocol/Internet Protocol (TCP/ICP) software library developed by Treck Inc used in its networking software for embedded systems. This left thousands of IOT devices in home, enterprise and medical settings vulnerable and whilst Treck provided a patch and made an effort to contact some people and organisations who used the software, it could not find them all.

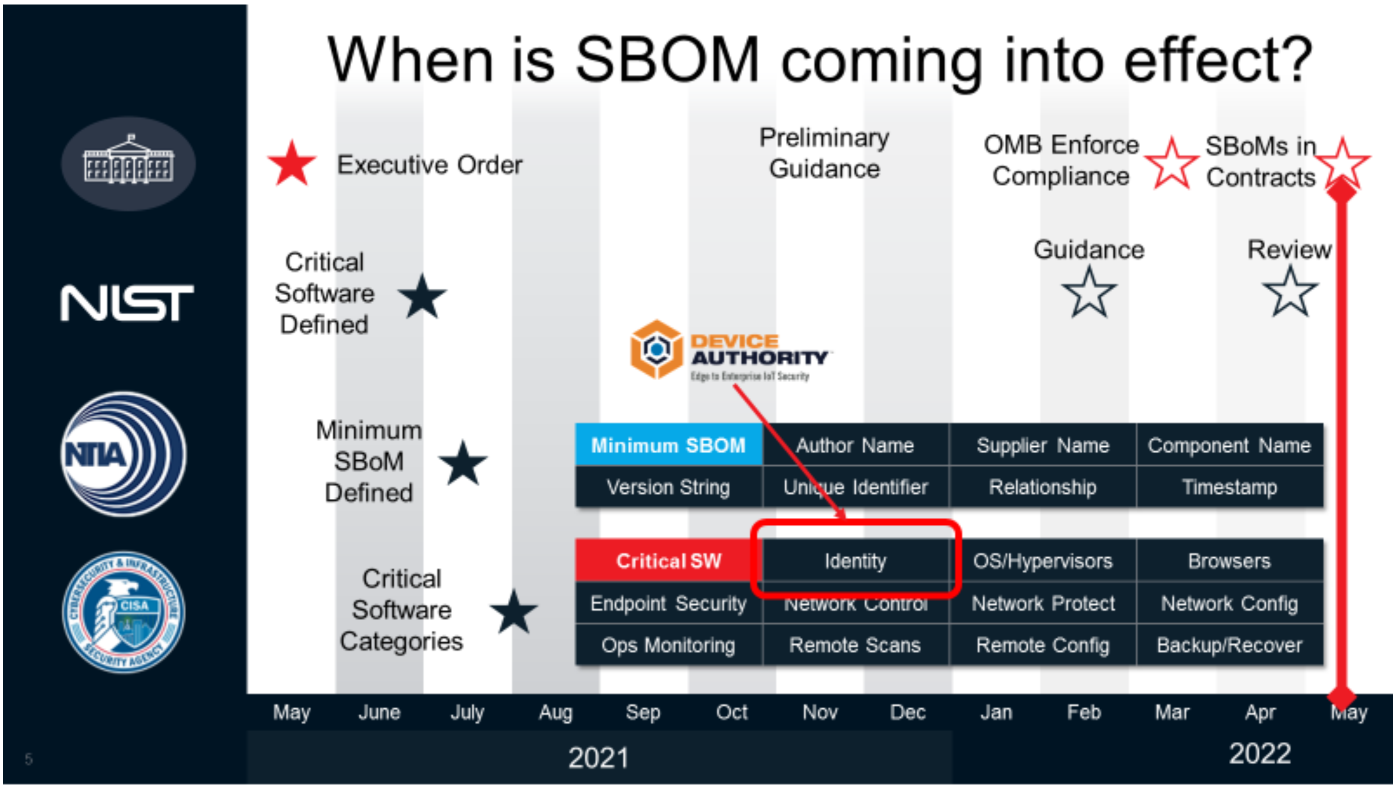
In this instance, an SBOM would have made it easier and more timely for individuals and organisations to know that their device contained vulnerable code, thus minimising the impact or potential opportunity for the device to be breached.

What does the Executive Order call for?

SBOMs	Collaboration	Zero Trust
Transparency of Supply Chains for Critical Software	Shared Threat Intelligence for Critical Infrastructure	Verify THEN trust IAM of Things
Cyclone DX, SPDX, SWID	VEX	AuthN & AuthZ

- It relates to the trustworthiness and transparency in **ALL** digital infrastructure - **IT, OT, IoT, IIoT**.
- Anything that runs software is in scope – cloud services, on-prem application servers and connected things – all systems that **provide critical functions.**

When is it happening?



When is SBOM coming into effect?

Executive Order

Critical Software Defined

Minimum SBoM Defined

Critical Software Categories

Preliminary Guidance

OMB Enforce Compliance

SBoMs in Contracts

Guidance

Review

Minimum SBOM	Author Name	Supplier Name	Component Name
Version String	Unique Identifier	Relationship	Timestamp

Critical SW	Identity	OS/Hypervisors	Browsers
Endpoint Security	Network Control	Network Protect	Network Config
Ops Monitoring	Remote Scans	Remote Config	Backup/Recover

Where should I start?

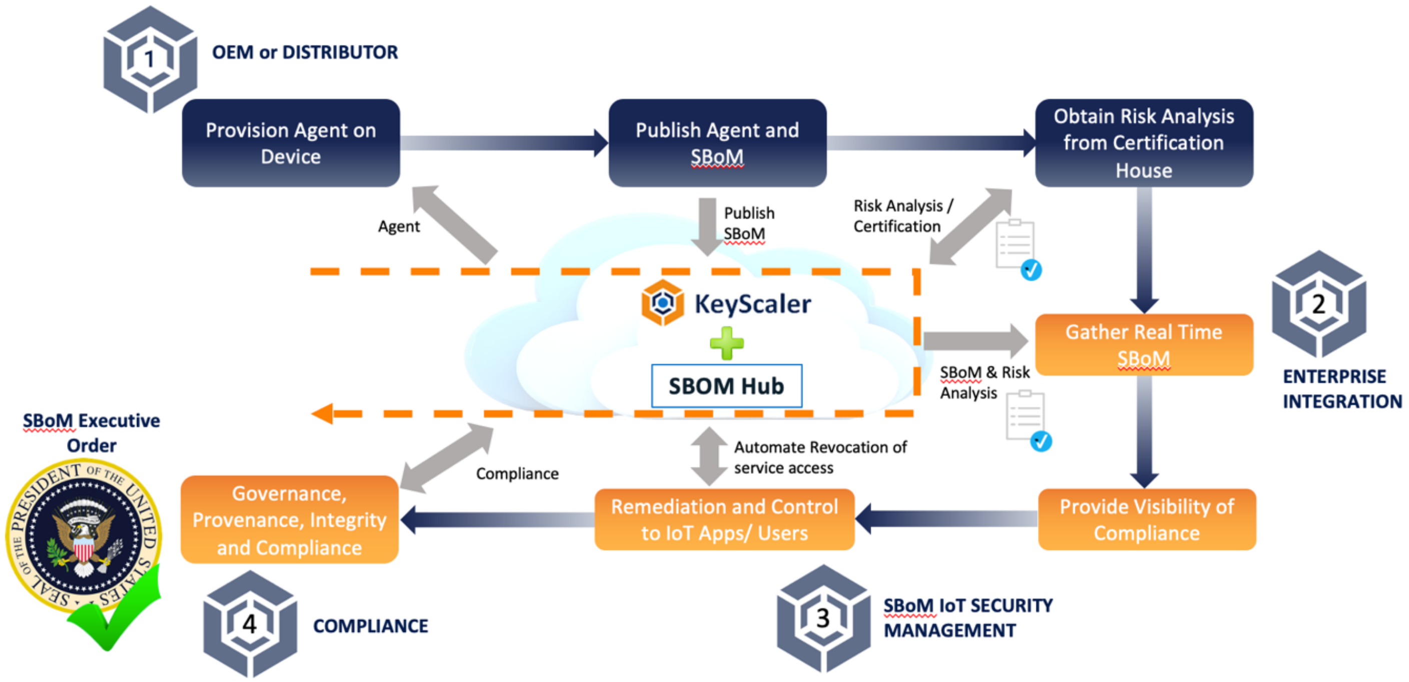
NIST has recently released the 2nd draft proposal of SP 800-161 which covers the key components of the Executive Order and what vendors need to consider from an SBOM perspective. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-draft2.pdf)

If you look at the requirements for SBOM and Cyber Security in the supply chain, then it boils down to providing a living document that accompanies any software either directly or through a public website to help identify and mitigate risk on a **recurring** basis for any and all software components in use.

Ultimately each vendor needs to consider the following:

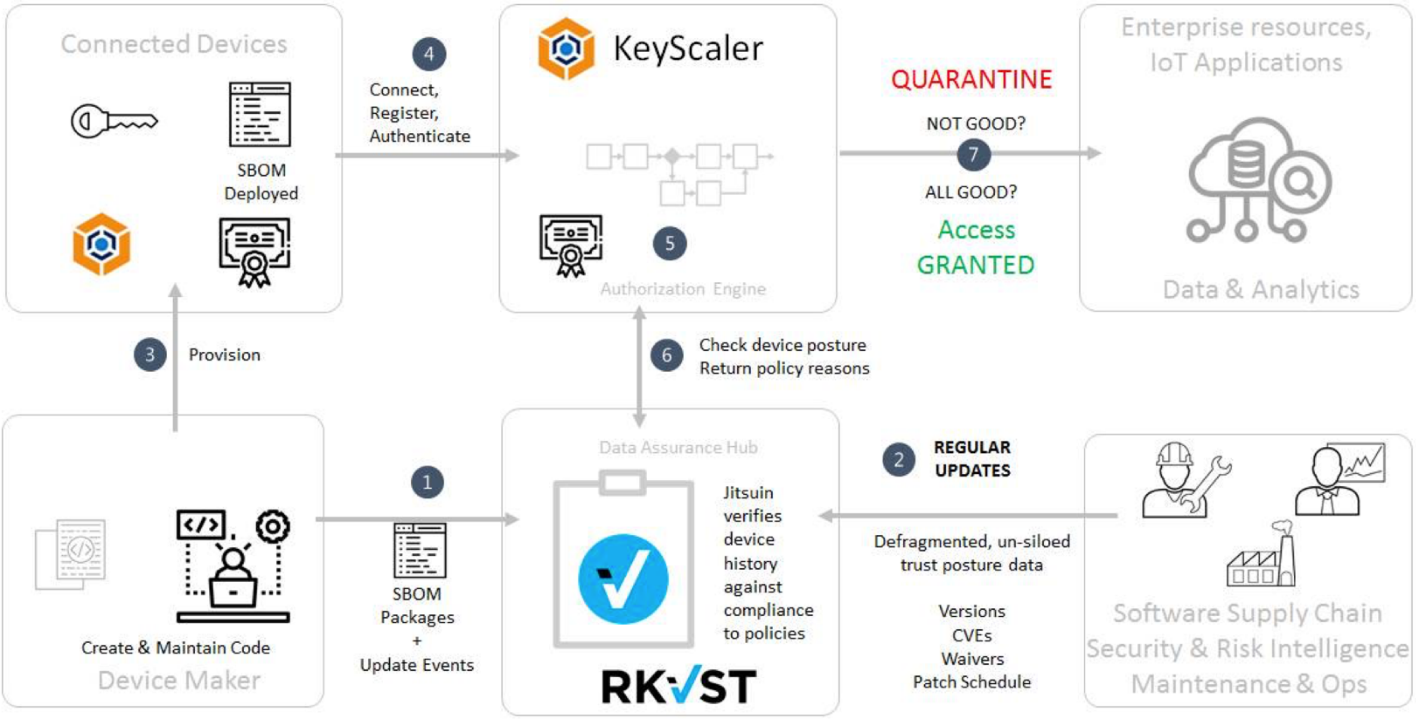
- Assurance, integrity, provenance, and transparency of SBOM data to build trust
- Provide governance on the complex sharing and privacy rules of data assets between multiple organizations
- Enable continuous tracking and automated reporting of compliance to policies
- Connectivity to operational security systems that can automatically act on SBOM data

Let’s look at an example solution for SBOM Management and Compliance for IoT, which can give you the automation required for IoT Scale:


1
OEM or DISTRIBUTOR
Provision Agent on Device
Publish Agent and SBoM
Obtain Risk Analysis from Certification House
Agent
Publish SBoM
Risk Analysis / Certification
KeyScaler
SBOM Hub
Gather Real Time SBoM
SBoM & Risk Analysis
2
ENTERPRISE INTEGRATION
SBoM Executive Order
Compliance
Automate Revocation of service access
Governance, Provenance, Integrity and Compliance
Remediation and Control to IoT Apps/ Users
Provide Visibility of Compliance
4
COMPLIANCE
3
SBoM IoT SECURITY MANAGEMENT

The diagram above lays out the fundamental key steps, where there are 2 areas of focus. Firstly, in blue are the configuration steps required, secondly the real time steps once a device is in "operation", coloured in Orange.

Let's look at a practical example for IoT, what solutions could help to meet the EO SBOM challenges:



Step 1:

- The device maker and software provider publishes the defined SBOM to a SBOM Data Hub, an example here could be Jitsuin SBOM Data Hub – RKVST. SBOMs are published according to SPDX, Cyclone DX or SWID formats.

Step 2:

- Software supply chain, Security risk intelligence and maintenance functions submit CVEs, Waivers, Patch schedule etc to the RKVST.
- Obtain a Risk analysis of your device from a certified house

Step 3:

- As part of the firmware installation on the IoT Device, the KeyScaler software agent is enabled.
- This can either be done by building in the software through the standard production processes before the device has been deployed or the KeyScaler software could be deployed as part of the next upgrade cycle i.e. through a retrofit / brownfield deployment model to support legacy devices.

Step 4:

- Once the device has powered on and in operation, it can now authenticate, register and connect to KeyScaler.
- Through policy KeyScaler can automate the provision identities, tokens and keys to the device and IoT Application e.g. provision and manage PKI x.509 Certs to Azure IoT Hub.

Step 5:

- Throughout the lifetime of the device, every time the device "checks in" and authenticates to KeyScaler, KeyScaler can request the devices to provide its current SBOM data (as set out in policy), this can then be used to validate against authorized published SBOM data i.e. what's been published and assessed through the Data Hub.

Step 6:

- Validating the current IoT Device SBOM data, through a Rest API call to the Jitsuin SBOM Data Hub

Step 7:

- The final step here is to perform some level of remediation if required.

This type of solution provides a Zero Trust capability for IoT Deployments to meet the requirements set out in the Executive Order. This provides

- Providing Visibility & SBOM status across all assets, with continuous tracking & automated reporting against policy
- Delivers real-time Zero Trust defence with assured SBOMs
- Operational efficiency & Automation at scale, with remediation controls into IoT/Cloud Apps
- Reduces Risk – Mitigating compromised device data from entering critical enterprise infrastructure
- Improves trust & Security in the supply chain – Integrity, provenance and transparency
- Enables customers to be compliant & meet Joe Biden's EO
- Lower administration fees & mitigate fines

sales@deviceauthority.com

www.deviceauthority.com

© 2022 Device Authority. All rights reserved.

DEVICE AUTHORITY™
Edge to Enterprise IoT Security