Use Case Overview

Polymer Proof

Blockchain Powered Software Supply Chain Security

COVAX DATA

Covax Data's Polymer Proof is a multi-use data integrity solution built on our proprietary form of blockchain called Polymer Chain. Polymer Chain is a lightweight, highly-performant, energy efficient form of blockchain technology designed for high throughput environments.

Software supply chain attacks are becoming more common and more severe. It has become such an issue that Executive Order 14028 was issued by the President specifically relating to these types of attacks. For the victims, these attacks can cripple critical infrastructure, causing widespread harm reaching far beyond the target. For the application provider whose software was used to carryout the attacks, the effects can reach into the millions of dollars for remediation and lost business. To adequately prevent these attacks, both the components and the full production version of the code need to be protected.

> "The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended." - Executive Order | May 12, 2021

How are these attacks carried out?

Software supply chain attacks generally come through one of two threat vectors - either the attackers infiltrate an application provider's network to insert malicious code prior to release, or the attackers publish fraudulent updates, such as open source libraries or spoofed updates, into which the victims are tricked or enticed to install. Regardless of the method employed, the impact to the victim and the application provider is the same.

What are some examples of these attacks?

The most obvious example, is the SolarWinds breach of 2020. In this case, approximately 36,000 customers were tricked into installing malicious code in the form of a software update. The breach cost the company $18 million dollars in just the first three months.

Another example, often overlooked in this context, is ransomware. Ransomware is an executable that, amongst other things, locks-up the victim's network and/or devices by encrypting files. In exchange for money - the ransom - the attacker provides the key required to decrypt the files to return to normal operation...or do they? The interesting thing about ransomware is that it is never named ransomware.exe, it is always disguised as something else, which is a very subtle yet effective form of social engineering.

AICPA SOC

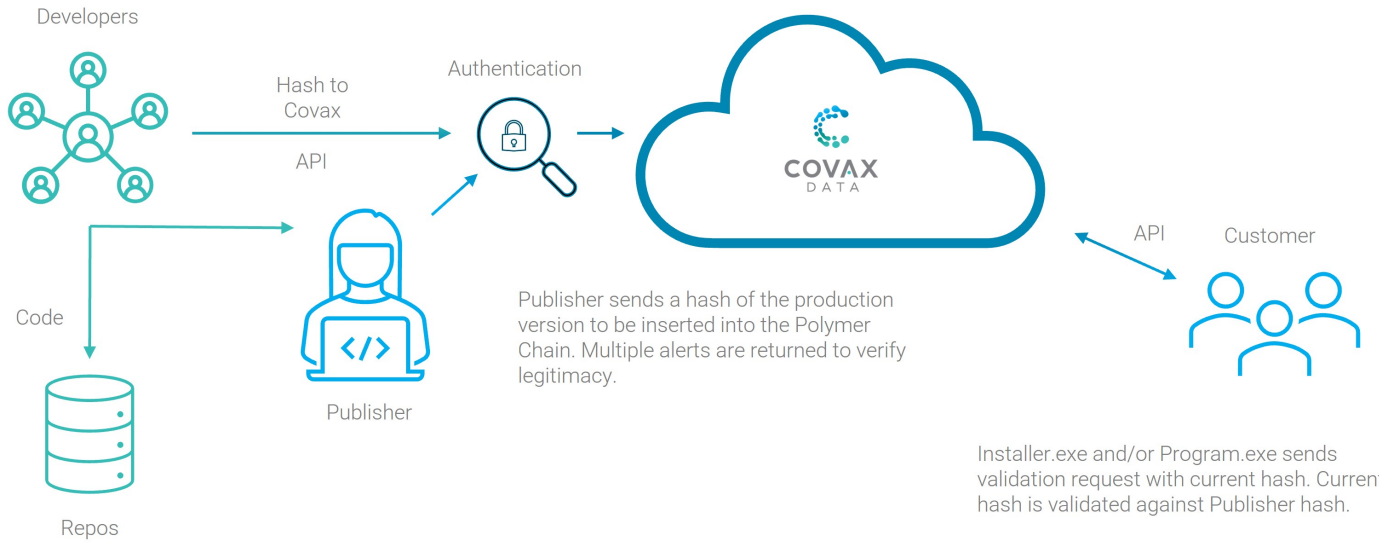
Covax Data is SOC-2 Certified
www.aicpa.org/soc4so

aws

How does Polymer Proof protect against supply chain attacks?

Polymer Proof is a data integrity solution that provides a proof of state validation on request. As such, application providers, and even application end-user organizations, can commit a hash of the trusted code to our blockchain. From this, the installer, the application itself, or an agent on the device, can hash the code and send it for validation against the trusted hash in our blockchain. If the hashes match, the code has not been tampered with and the process can proceed, if the hashes do not match, it is a sign the code may have been altered and the process should not proceed.

Figure 1.0



How does Polymer Proof solution work?

At its core, Polymer Proof is simply a set of open API's through which our customers can connect to the Polymer Chain. This allows the commitment and validation of data to our blockchain. As you can see in Figure 1.0, on the application provider side, an authentication layer is added. The application provider can utilize the solution in a number ways - from securing the production package to having developers sign their work as it is pushed to repos - the entire development process can be secured end-to-end.

Once a software version, patch, or hotfix is compiled, reviewed, and pushed to production, a hash is sent to the Polymer Chain as a source of truth. From here, based on the flexibility and performance requirements of the solution, the end-user validation can be configured to run at install, on program startup, or any other schedule. The application developer will simply embed an API call into the process to validate the present version against the signed version in the Polymer Chain. This process provides both the application provider and the end-user client assurance that the version of the software being installed is a legitimate solution from the provider.

For the CISO, CSO, and CTO at the end-user client level, the utility of Polymer Proof can be just as profound. Even if the application provider is not utilizing the Covax solution, your environment can still be configured to leverage the capabilities of the platform. With best practices in place to verify the authenticity of software packages, the same hashes that the application provider can commit to the blockchain can be commited by the end-user. At this time, the local agent can be programmed to run periodically to validate the build, or the set of approved programs can be validated during boot. This mechanism can prevent malware such as ransomware from being authorized to run on a user's machine.