WHITEPAPER

COVAX DATA

POLYMER DATA SECURITY

Product Overview

INTRODUCTION

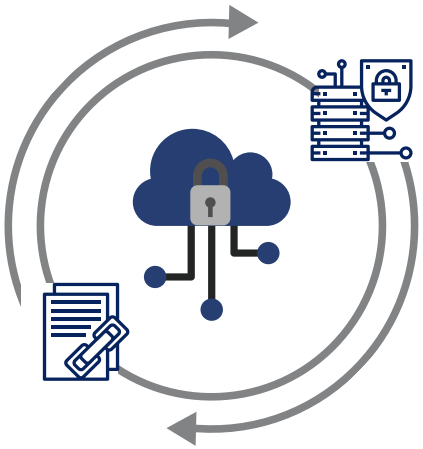
This is the Age of Information where data is the gold of our time. Like gold, data needs to be protected. Unlike gold data loses its value if it is locked away and inaccessible. The challenges to securing data – protecting it from unauthorized use or alteration – are unlike the challenges to securing any other commodity. Data can be moved and replicated - literally at the speed of light. The value of data can be taken without the owner losing access and the owner can lose access without losing possession. Data cannot be locked away in a vault. It needs to be accessible 24 hours a day, and it needs to be accessible from virtually anywhere.

Industry standard data security "Best Practices" focus on controlling access to data. These "Best Practices" attempt to protect data by working from the outside in. If a bad actor defeats the access controls, they can steal or destroy, just as if they had cracked a safe and walked away with the gold. The phrase "Best Practices" is a misnomer. It refers to what is common knowledge and common practice. Controlling access to data is a necessary component of data security but it is not sufficient. By itself, data access control is not a "Best Practice." In today's world, where fiber optic networks span the globe and data access at the speed of light is available even at the home, a new vision of data security is required.

Imagine a thief who has picked the locks to a gold vault only to find, not gold, but the quarks that make up the protons, that make up the element of gold. Imagine further these quarks are mixed with quarks from an unknown number of other elements. Imagine further that the only way to re-assemble the right quarks, and only the right quarks, into the element of gold is to enter the vault during business hours with a photo ID and an iris scan and the permission of the vault owner. This is how Covax Polymer secures data. It links the structure of the data to the characteristics of the attempt to access it. With Covax Polymer, protected data only exists in valuable form when it is accessed in the right way, at the right time, from the right device, by the right person, for the right reason. When it comes to protecting the most valuable commodity of our time, data, Covax Polymer presents an entirely new vision. Covax Polymer is defining tomorrow's Data Security "Best Practices" today.

DATA SECURITY IS CYBER SECURITY – CYBER SECURITY IS DATA SECURITY

Data Security is a frequently used term of relatively recent origin. It is often thought as a discipline of Cyber Security – another frequently used term of relatively recent origin. Both terms tend to obfuscate rather than illuminate. In order to solve a problem, one must first define the problem. The more precisely a problem is defined the more rapidly a solution can be developed and implemented. Precision of problem definition requires a precise lexicon.



The Cambridge dictionary defines Cyber Security as "things that are done to protect a person, organization, or country, and their computer information against crime or attacks carried out using the internet." Meanwhile, Merriam-Webster defines Cyber Security as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack." The first definition is quite expansive regarding what is being protected and quite restrictive on the mechanism of attack. The second definition is very restrictive regarding what is being protected while virtually unlimited on the mechanism of attack. Neither definition provides the clarity and focus necessary to enable an enterprise to develop a plan that is appropriately targeted and cost-effectively implemented. For example, both terms qualify the universe of concern to systems that are either "on the internet" or can be attacked "using the internet." The common understanding among telecommunications professionals is that networks that operate over private circuits are not "on the internet." Accordingly, this definition would exclude networks such as the Department of Defense SIPRNet and JWICS.

For our purposes, we define a Cyber System as a system comprised of two or more endpoints which generate and transmit, receive and process or store, data via the use of electronic devices coupled with programmable logic. This definition serves several purposes. First, it defines the boundaries of concern by eliminating standalone devices that cannot transmit or receive data and/or connected devices that do not involve computational logic. Second, it does not exclude devices from the domain based upon (SIPRNet vs. internet) business concerns. Finally, it fuses data with the systems that produce and process it into a single logical entity. After all, data is the raison d'etre for every computer device and system. Accordingly, it is counter-productive to think of Data Security as a subset, or appendage, to any other element of the cyber world.

With the above definition of Cyber System we can define Cyber Security as: the state of being free from the danger of unsanctioned manipulation of data as it traverses, or rests within, a Cyber System. With this definition of Cyber Security we have a very focused framework for achieving a clearly defined goal. Moreover, we have a more effective and efficient mechanism for implementing the framework than industry "best practices" provide. The framework consists of three questions:

WHAT DATA DOES THIS COMPONENT UTILIZE?	HOW CAN THIS DATA BE MANIPULATED?	HOW CAN UNSANCTIONED DATA MANIPULATION BE PREVENTED?

The simplicity of this framework for Cyber Security is self-evident. The efficiency of the framework derives from the fact that the component engineers and operators are the best equipped to execute the framework. It is not necessary, and, perhaps, counterproductive, to engage Cyber Security specialists with any component of the Cyber System. This simple framework can be applied to operating systems developers (and pushed down into the kernel components), router & NIC firmware, application software, storage systems, etc. Thus, data security is incorporated organically into every component of a Cyber System.

BEYOND DATA SECURITY: INFORMATION CONTROL

The term "data security" is a misnomer. As commonly used, it references measures taken to secure information – not data. This is because the words "data" and "information" are often considered synonymous. They are not. Data can exist without information. Information cannot exist without data. Information is the fusion of data and metadata. When the difference between data and information is not fully appreciated efforts to achieve "data security" will be sub-optimal.

Consider the data "10". A computer scientist might think it represents "two" under the assumption that the "1" and the "0" are binary digits.

INFORMATION IS THE FUSION OF DATA AND METADATA

DATA	NUMERAL SYSTEM	DECIMAL VALUE
0 0 0 0 0 0 **1 0**	DECIMAL	= TEN (10)
0 0 0 0 0 0 **1 0**	BINARY	= TWO (2)
0 0 0 0 0 0 **1 0**	OCTAL	= EIGHT (8)
0 0 0 0 0 0 **1 0**	HEXADECIMAL	= 16
0 0 0 0 0 0 **1 0 0**	DECIMAL	= 100
0 0 0 0 0 0 **1 0 0**	BINARY	= FOUR (4)
0 0 0 0 0 0 **1 0 0**	OCTAL	= 64
0 0 0 0 0 0 **1 0 0**	HEXADECIMAL	= 256

Most people probably think "ten" because a base 10 number system is what they normally encounter. Some might think "16" if they commonly deal with hexadecimal values. The data "10", by itself, effectively provides no information. In fact, it might provide disinformation. The data "10", when combined with the metadata that it is a string of binary digits, yields the information that it represents a value of 2 in the decimal number system. That information, however, may be misleading. If the data "10" is a subset of the string "100", and that string represents binary digits, then the information it represents is a value of 4 in the decimal number system – not "two". Data, separated from metadata, can be unintelligible. Data, combined with metadata, is information.

When this distinction is not fully appreciated, and data and metadata are treated the same, the opportunity to optimize Cyber Security efforts is lost. In fact, one of the most powerful tools for controlling information is simply discarded.

This understanding of the difference between data and information highlights the need for a more precise term than data security or Cyber Security. The term "Information Security", although close, does not meet the need for a term that fully expresses the desired state, and does not pollute the design process with external concerns.

The SANS Institute, a professional association of 165,000 security professionals, defines "Information Security" as the "processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private, and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption…" Unfortunately, this definition extends beyond the realm of Cyber Systems and thereby distracts our focus. Additionally, this definition does not distinguish between data and information.

Moreover, "secure" means "free from danger or threat" and that understanding does not allow for the needs of compliance reporting and data authentication. If it cannot be proven that information is what it is purported to be, or it cannot be proven that access has been appropriately restricted, the information can lose practical value.

In light of the preceding, Covax Data has adopted the following definition of Information Control:

Information Control is the paradigm that provides for the sanctioned use of cyber information, the provenance of the information, and the provenance that only sanctioned use has occurred.

ESSENTIAL COMPONENTS OF INFORMATION CONTROL

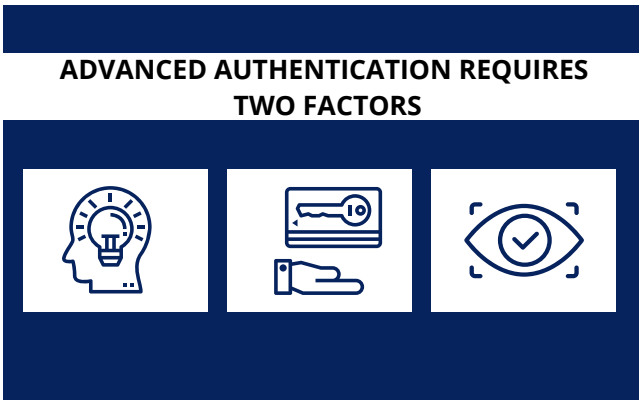
There are four essential components of Information Control. These are Authentication, Authorization, Integrity, and Provenance. Covax Data's insight into the necessity of discriminating between data and information cascades into similar insight into each of these essential components. Following is an examination of each of these essential components and how the typical implementation of these components is data-centric – not information-centric. The examination of each component will introduce the insights incorporated into Covax Polymer that enable it to go beyond data security and provide Information Control.

AUTHENTICATION

The definition of Information Control requires that access to information be sanctioned. This means that access can only be granted when there has been official approval for the access and that approval, to have any meaning, must be attached to an identity. Authentication is the process whereby an entity asserts its identity and that identity is authenticated as being who, or what, the entity claims to be.

The most basic level of authentication involves the use of one or more databases of identities with associated passwords. The identity seeking access asserts their identity by entering a user ID and then proves they are who they say they are by entering a password. If the identity is not in the database, or the password supplied does not match the password in the database, access is denied. This two-factor system is as weak as it is simple. Users tend to create passwords that are easily remembered and, therefore, as easily cracked. Even where strong password policies have been implemented, such as requirements for a minimum number of characters, upper and lower case, and a mix of letters, numbers, and special characters, two-factor authentication is relatively easily defeated by nominally sophisticated adversaries. These realities have spawned a virtual arms race between those seeking effective Information Control and those who seek unsanctioned access.

An early escalation intended to harden the authentication process was to introduce Multi Factor Authentication (MFA). This requires that the entity seeking access provide a physical proof of their identity in addition to the knowledge proof of providing the correct password. A typical implementation would be to send a code to the user's cell phone which would be delivered out of band of the system to which access is requested. The user then enters the code into the system, as they did their password, and if it matches, the user is authenticated.



Another escalation of the Information Control arms war involves the expansion of End Point Security (EPS). Moving beyond installation of anti-virus and malware software to protect the device from which access is requested, EPS defines the device to be an attribute of the identity. Thus, if User A seeks access from User B's device, or an unknown device, authentication fails and access is not granted.

While MFA and EPS, separately and combined, improve the effectiveness of the authentication process, they both are vulnerable by the fact that devices can be cloned and spoofed. Moreover, they are both vulnerable by the fact that users can be coerced, bribed, and extorted. Ensuring that an identity is what it claims to be and is operating from the device(s) approved for that identity, does not ensure that the information being accessed is being done so for a sanctioned purpose.

The reality of the foregoing deficiencies in the Authentication component have led to the incorporation of User Entity Behavior Analytics (UEBA) into the authentication process. UEBA essentially maps the identity's usage profile to more effectively manage authentication when an authentication request deviates from normal circumstances. If Tom seeks access from Paris, when he works in Chicago, UEBA can decline authentication. UEBA is an extremely powerful tool because it can become ever more precise by employing machine learning and fueling the learning with effectively unlimited training data.

Effective Information Control ensures that information is accessed "in the right way, at the right time, from the right device, by the right person, for the right reason." The last clause, for the right reason, is not typically addressed by the authentication process. This is because the data security paradigm is ordered to controlling access to data and has no conceptual framework for controlling the use of Information. **Covax Polymer provides the ability to control how information is used.**

AUTHORIZATION

The Authorization component of Information Control is inextricably tied to the Authentication component. Every data security system develops a set of policies that determine what each identity is sanctioned, or permitted, to access. These policies can be applied to an individual identity or to a class of identities. Identities can be included in one or more classes.

The net effect is that, upon authentication, each identity is given permission to access all the information permitted by all the classes of which the identity is a member. Consider an enterprise that has Information Set 1 – 5. Class A provides access to Information Set 1 and Information Set 2; Class B provides access to Information Set 3; and Class C provides access to Information Set 4 and Information Set 5.

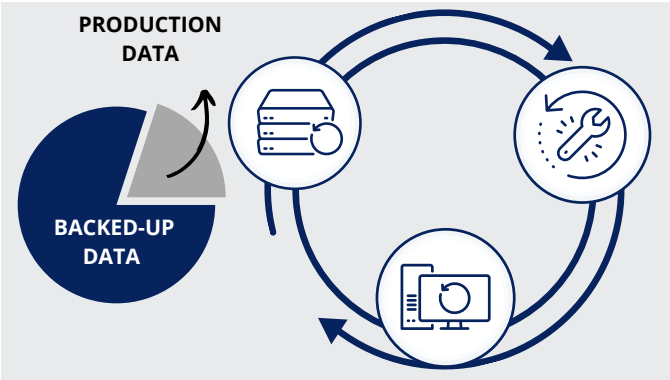
STATEMENT	RESULT
SELECT	**Allows user to search for rows in a table**
INSERT	**Allows user to insert rows in a table**
UPDATE	**Allows user to update rows in a table**
DELETE	**Allows user to delete rows in a table**
ALL	**Provides user all privileges**

Identity A is a member of Class A and C; therefore, they can access Information Sets 1, 2, 4 & 5. Identity B is only a member of Class B; therefore, Identity B can only access Information Set 3.

There are many commercial software packages that facilitate the management of linking authorizations to identities. These packages provide necessary functionality. However, all that functionality is only relevant with regard to information access attempts made through the Authentication/Authorization components. There is a very large segment of the Cyber Security market that is focused on defeating attacks that attempt to bypass the Authentication/Authorization components entirely. The existence of this market segment highlights the inadequacy of the data security paradigm and underscores the need for Polymer's unique Information Control paradigm. We will examine some of the systems that attempt to deal with threats that bypass the Authentication/Authorization process. In doing so we will see how the existence of these market segments prove the need for Covax Polymer.

Intrusion Detection System (IDS) – An IDS seeks to detect unwanted access to a system. Typically, they scan incoming network packets, or scan files stored on a system, to match the "signature" or byte pattern of known threats. When a threat is detected, they trigger alerts according to defined policy. Alternatively, IDS systems may operate by detecting anomalies in network traffic or files. An example might be an OS level driver file with a size that differs from the file contained in an official, signed, distribution. IDS systems do not, themselves, prevent intrusions but the alerts they raise can provide the information needed to improve policies, locate and limit current intrusions, and prevent repeat intrusions.

I*ntrusion Prevention System (IPS)* – An IPS seeks to prevent unwanted access to a system by detecting known attacks (as discovered by an IDS) and proactively respond by dropping packets or blocking the source address. IPS systems developed as extensions of IDS and now often appear as integrated products.



One strategy to protect against unsanctioned access to information from the live production system and backup copies is to encrypt the data on the production system. This prevents effective use of the data even when a system has been breached and the attacker has defeated the authentication and authorization protections. However, this imposes additional costs in Time to Recover and cost to store the back-up data.

Copying large amounts of data can be very time consuming, thereby increasing the Time to Recover. To offset this, back-up systems often create a reference copy and then perform incremental backups that contain only the data that has changed since the last backup. When data is stored in an encrypted state, even a small change can result in wholesale changes to the encrypted data. This reality often renders incremental backup systems practically impossible. **Covax Polymer supports data security by facilitating Continuity of Operations and Disaster Recovery - enabling encryption of production data while preserving the ability to perform incremental backups.**

Even when data is only accessed in accordance with policy it is still possible for it to escape the control of typical data security systems. In addition to preserving the availability of information and restricting its access to sanctioned identities, the preservation of information integrity requires that sanctioned access be limited to the purpose for which the identity's access was granted. Improper use need not be malicious to be harmful. In 2006, a Department of Veterans Affairs VA contractor had copied the data of over 26 million veterans onto his laptop. That action was not proscribed by any policy. The laptop was stolen from the contractor's home resulting in the exposure of the confidential information of all of these veterans. This is one of the most extreme examples of what is known as data leakage. **With Covax Polymer, even if an entire data store is copied, Polymer prevents it from being exposed.**

PROVENANCE

Information is generated for a purpose. In many cases, such as government, health, financial, manufacturing, legal, and other activities, that purpose is subject to regulatory requirements. In these cases, the information owner may be required to prove that there has been no unauthorized access of the information. In other cases, it may be required that certain reviews or approvals occurred at the proper time or in the proper sequence. Even without a regulatory requirement, an enterprise may find it necessary to establish provenance for forensic purposes.

Typically, this required provenance is established in one of two ways. The first, especially relevant where regulatory requirements are high, is through the use of specialized access-logging software tailored to the specifics of the industry. Such systems essentially create and maintain a ledger of activity and any approvals that are required to certify or justify the activity. The second method of establishing provenance is through reconstruction. This method establishes application and system log configurations that record the necessary information. However, this method usually does not add additional controls and does not provide an interface that generates time and status reports tailored to a specific purpose. This method is more suited for ad hoc provenance requirements or forensic purposes.

Both of these approaches suffer from the separation of provenance from information. They circle around the information but do not intrinsically fuse information access and provenance. This separation opens the door for forging the provenance. With enough planning, or advance notice, system and application logs can be recreated; specialized ledgers can be altered. Such actions may leave trace evidence and may be discoverable but are unlikely to be discovered absent a reason to suspect they have occurred. **Covax Polymer eliminates this possibility. With Polymer, data does not become information until the access has been sanctioned, and access is sanctioned simultaneously with the provenance being unalterably recorded**.

Security Information and Event Management (SIEM) – SIEM grew out of log analysis programs to become a form of IDS with a different focus. SIEM systems focus on event analysis, such as failed login attempts, access from unexpected IP's etc., to detect incipient or ongoing attacks. Where IDS can detect successful attacks SIEM can identify attempted attacks and potentially provide intelligence on the attacker.

Deception Technology (DT) – Deception technology is an attack mitigation and counter-intelligence technology. It involves salting a system with imposter files that would never be touched by a legitimate system user. Access of an imposter file triggers an alert that the system has been compromised without alerting the intruder. The use of DT provides counter-intelligence capability by enabling the host system to monitor the attacker in order to shed light on their identity and intentions.

Remote Monitoring & Management (RMM) – RMM is the outsourcing of IDS, IPS, SIEM, and other related technologies to a third party specializing in protecting cyber systems. RMM providers can cost-effectively provide highly specialized personnel and 24/7/365 monitoring and response that might be cost-prohibitive to many organizations.

The market for these technologies runs into billions of dollars annually. The existence of these products demonstrates that Cyber Systems will be breached with potential losses exceeding those same billions annually. Adversaries who manage to breach a system, bypassing the Authentication/Authorization process, can gain unsanctioned access to Information. **Only Covax Polymer is designed to render these breaches ineffectual.**

INTEGRITY

From the Information Technology perspective, Integrity means that an object is in an unimpaired condition or a state of being complete or undivided. Preserving the integrity of information means preserving the sanctioned, and only sanctioned, access to information that is both uncorrupted and undiluted. Cyber Systems can be penetrated despite the multi-billion dollar annual effort to prevent it. Therefore, information must be available to sanctioned users while simultaneously being unavailable to bad actors who have gained access to the system in circumvention of the Authentication and Authorization components.

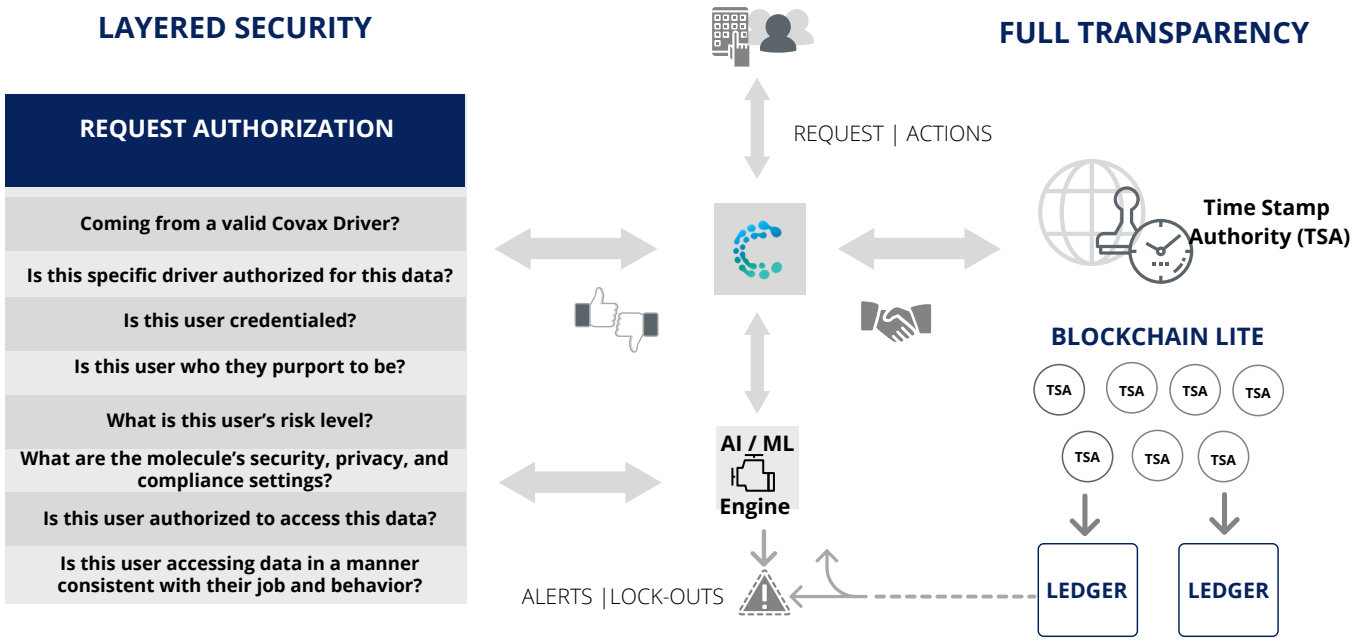
The first aspect of this two-part requirement, sanctioned access, is addressed through Continuity of Operations and Disaster Recovery planning. These disciplines determine the Time to Recover from an outage, denial of service, or a disaster, and the Recovery Point to be restored. An enterprise that requires zero downtime and a no-loss Recovery Point will require expensive duplication of infrastructure. An enterprise that is willing to accept some period of system downtime and a Recovery Point that loses some transactional information, will have proportionally lower expenses. The spectrum of possible implementations is infinite, but in every case where an enterprise requires a non-zero level of downtime, or a non-zero level of transaction loss, some measure of duplicate data is required. The result is one or more additional copies of data that can potentially be accessed by skirting the Authentication/Authorization process. This unavoidably increases the attack vectors for non-sanctioned access to data.

Unless the data is replicated for instantaneous hot-failover, it may exist outside of the normal Authentication and Authorization components. Copies of databases, document stores, and other repositories need to be restored en masse, and therefore cannot be constrained by the strictures of access policies. Without additional protections, backup data is afforded far less protection than live, production data.

COVAX POLYMER

The predominant mindset of what constitutes "best practices" for "data security" is broadly and deeply flawed. The flaws derive from a failure to appreciate the distinction between data and information. These "best practices" also ignore the elephant in the room: data can never be completely secured without losing its value. As soon as data is exposed via any Cyber System, it can potentially be used in ways the owner does not wish it to be used. Current "best practices" attempt to make data very difficult to access in unsanctioned ways, but simply do not address the issue of what happens when such unsanctioned access occurs even though the result can be catastrophic. Today's "best practices" do not address an authorized user using data in an unauthorized way. Today's "best practices" do not address an unauthorized user breaching the network. If an attacker reaches the data, they get the information that is supposed to be protected.

Polymer is rooted in the superior paradigm of Information Control. It is based on the fact that data provides no information without metadata and that information can be ephemeral. With Polymer, Authentication, Authorization, Integrity, and Provenance are combined to create the atomic fusion of data and metadata that is information. With Polymer, information dissolves to data when any of the elements of Authentication, Authorization, or Provenance are removed.



Polymer exists as three components that combine to enable the fusion of data and metadata. These components are the Polymer Molecule, Polymer Prism, and the Polymer Chain of Custody. The purpose and functionality of each is described below.

POLYMER MOLECULES

The core of Covax Polymer is the Polymer Molecule. A physical molecule is an electrically neutral group of two or more atoms held together by chemical bonds. Polymer's Molecule is similar to its physical analogue. Defined in the Polymer Molecule Manager, a Polymer Molecule is a virtual container with very specialized properties. A Polymer Molecule can be as small as a single byte or as many terabytes as fit on available storage.

Storage can be local or cloud. It expands or contracts as necessary. The atoms of the molecule are the different pieces of information that are put into it. There can be any number of molecules and what information is put into which molecule is defined through the Polymer Molecule Manager.

The most unique and powerful property of a Polymer Molecule is that it transforms information into data when it is put into the molecule. When information is passed to the molecule, it catalyzes a reaction which effectively shatters it into many pieces, much like splitting an atom, encrypts each piece separately, and then writes it as data. The recipe that controls this disaggregation then evaporates and is not stored as part of the molecule. Any hostile entity that manages to defeat all of the cyber security defenses, and manages to copy the molecule, even in whole, will only have access to encrypted chunks of data, of unknown length, without any way to link one encrypted chunk to another encrypted chunk. They will not have information. They will have data that has no meaning.

The reverse of this process occurs when information needs to exist. Polymer applies the recipe to the molecule that pulls together the shattered pieces, decrypts them, and returns the requested information.

The fusion of Polymer Molecule with Polymer Prism defeats brute force hacking attempts through traditional and AI-driven methods (as will be explained in the discussion of Prism). In this regard, it is important to note that Polymer Molecule provides Information Control even when the target data is offline and accessible to the hackers, such as when they have successfully stolen Molecules. In this case, brute force attacks can theoretically be successful as the attacker may eventually be able to get to the data contained within a Molecule. However, this data would not provide information. The attack would have to be successfully executed against each one of the encrypted Molecules which contain the shattered pieces of information. A lifetime of attacks would still prove fruitless as they still would not be able to glean the valuable information from it. They would only perhaps have millions of strings of data with no way to tell how, or if, any of the data was related. Without an ability to reassemble the strings of data in the proper order, the attacker has no access to the information.

Finally, the Polymer Molecule structure allows for incremental backups of encrypted data sets for those organizations using file-level backup solutions. While this is typically not an issue for block-level backup solutions, or for single file encryption, when multiple files, folders, objects, etc., are encrypted within the same “container,” file-level system backup solutions cannot understand where, specifically, changes have occurred. This results in the potential for repeated massive backups for otherwise small changes. Polymer Molecule eliminates this impediment to cost-effective back-ups for ensuring information integrity.

With respect to Polymer Prism, Polymer Molecules are fused to Polymer Chain of Custody. The creation of a Polymer Molecule automatically creates an immutable record in Polymer Chain of Custody. This record initiates an immutable chain of provenance for every piece of information put into the molecule. Polymer Molecules cannot exist without immutable Provenance.

POLYMER PRISM (AUTH)

In the terms of standard "best practices," Polymer Prism provides Authentication and Authorization (A&A) services. These "best practices" view A&A as two sequential hurdles which, when overcome, result in access to information. That concept is obsolete. The modern world experiences change at the speed of light. In less time than a human user can process that his A&A was successful, a hacker on the other side of the world could have breached a router and hijacked the session. A&A needs to be fused with policy declarations fueled by machine learning and AI in a way that results in A&A effectively becoming a constantly evaluated state. Polymer Prism provides this fusion.

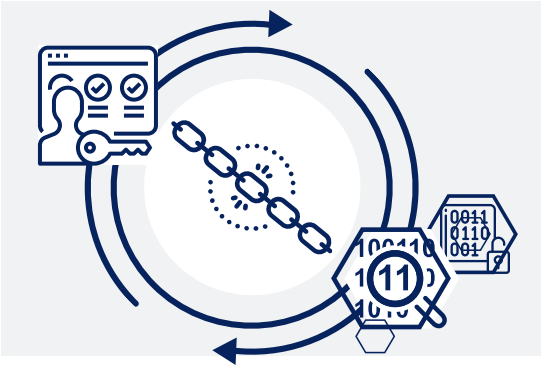
An ordinary beam of light appears white to the naked eye. Introduce a prism at the proper angle and the light is refracted into infinite gradations of the color scale. Take away the prism and the colors disappear even though the light remains. Polymer Prism performs the standard "best practices" for authenticating a user. The user (or system) asserts an Identity and proves that Identity with the correct password as well as various multi factor proofs. This results in a session with whatever privileges have been assigned to that Identity. The first two hurdles have been overcome, resulting in access to information. A&A has done its job. Where these "best practices" end, Polymer Prism is just beginning.

The end result of "best practice" A&A is a state of privileges being granted to a user. The end result of A&A with Polymer Prism is a context of Identity (Authentication) and privileges (Authorization) which is evaluated in real-time against fluid variables to determine whether the requested action should be permitted. The determination of whether to grant the requested access to information is not as simple as that provided by typical A&A systems. The question is not whether the light is on or off. The question is whether we can see when the light is blue or green – or red.

Polymer Prism is a decision engine that controls actions on the data, leveraging both traditional and AI/ML-powered protocols. This system is responsible for enforcing policy and rules, authenticating users, and validating their requests. Every action on Polymer protected data must receive real-time approval from Polymer Prism. When a request is made, Prism brings together inputs from multiple components to effectuate the most accurate decision possible based on the information at the time. However, should new information become available as a user is engaging the data, the session may be revoked.

Polymer incorporates User and Entity Behavior Analytics ("UEBA") powered by artificial intelligence and machine learning to supplement the authorization decision. Geographic location, time of day, and system analytics are all factors that can and should be utilized in rendering a decision. In addition to UEBA, Polymer analyzes other data points available at the time of the request - including information provided by third-party independent systems. Misuse of information by authorized users is one of the more challenging types of attacks to recognize and defeat. Viewing each request to execute an action on information within the context of current activity, as well as the user's historical behaviors, enables Polymer Prism to provide the most effective protection possible against misuse by authorized users.

POLYMER CHAIN OF CUSTODY



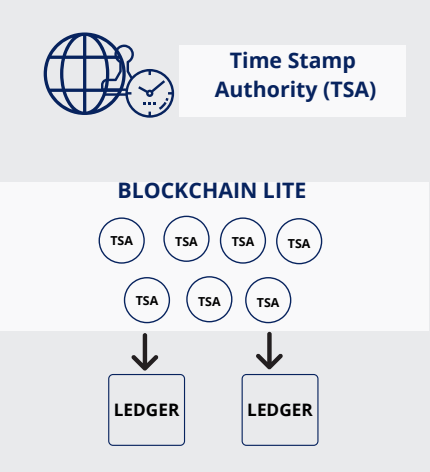
In regulated environments, information may be perfectly valid but unable to serve its purpose. In fact, where regulatory compliance is strictly enforced, information can have a negative value if it is not accompanied by proof that it has been generated and accessed only in ways consistent with regulations. Penalties for unauthorized access to medical records under HIPAA, for instance, or social media data under GPDR, can be substantial.Outside of regulatory requirements, an immutable record of who accessed what data when, and what they did with it, provides valuable intelligence for incident response and system analysis. Polymer Molecules are fused with Polymer Chain of Custody and enabled and validated via Polymer Prism such that information access can only occur with simultaneous recording of the access. This capability is unique to Polymer and is based upon Covax Data's patented "blockchain lite" technology.

Blockchain technology is relatively new and, while its value is undeniable, its proper use is often misunderstood. The pioneer application of block-chain technology, Bitcoin, uses blockchain to create a public, distributed, ledger that records transfer of bitcoin between accounts. It protects the integrity of the ledger by decentralizing the cryptographic hash computations among multiple independent third parties who must all agree on the result before the transaction is confirmed and included into the ledger. These third-party processors earn fees from the transacting parties – not from any "owner" of the ledger. These parties can be independent because no one owns Bitcoin. This is where many products misuse blockchain. They apply it to their privately controlled ledgers and use their privately controlled transaction processors to compute the required hash. This nullifies any validity of the private blockchain because the protection against forgery requires that no processor can control more than 50% of processing capability.

Polymer Chain of Custody uses Covax Data's patented blockchain-lite technology that provides the same immutability of the Bitcoin ledger without the computational resource requirements of standard blockchain-style technologies. Our innovative approach creates a digital record – Polymer Chain of Custody – that is far more robust than traditional logs or audit trails. Covax has created a cloud-based framework of micro-services that create a distributed architecture for securing ledger transactions. These micro-services are called Time Stamp Authorities ("TSAs"). TSA's verify the continuing validation of previously granted authorizations. When the authorization is affirmed it completes the handshake between Polymer Prism, Polymer Molecule, and Polymer Chain of Custody. This handshake is required for every action requested on a Polymer Molecule. For an action to occur on a Polymer Molecule, the Covax driver at the particular data access point must successfully handshake with a TSA. This required handshake cannot occur without updating the Chain of Custody, while conversely, an action cannot be carried out on a data molecule without the correct handshake response. Thus, Chain of Custody becomes one with the information to be controlled.

TSA's also provide an important extension to the concepts of Authentication and Authorization. The requirement for a TSA handshake for each action on a Polymer module transforms Authentication and Authorization from a single point in time binary decisions to a continual evaluation. TSA's enable the inclusion of UEBA data into validation of Authentication and Authorization decisions for each action on a Polymer module. It is not enough to decide that Person A is actually Person A.

Information Control requires that the behavior of Person A be consistent with expected and accepted behavior. A bank manager who opens a bank vault during normal business hours does not raise alarms. A bank manager who opens a bank vault at 3:00 am should raise alarms.



The response to such suspicious behavior is controlled by policy and can range from simply creating a log entry to terminating the session or suspending all access privileges. **Only Polymer's TSA architecture provides this comprehensive and critical protection against improper access of information by trusted users.**

The Polymer Chain of Custody's ledger can be monitored in real-time by the Covax AI engine, and by administrators via their dashboard. Users can also monitor the ledgers for the molecules they are authorized to access through the Molecule Manager. Alerts can be pushed based on rules or anomalies as determined by artificial intelligence, with access being revocable at any time either through AI or manual intervention. Conversely, Polymer Chain of Custody feeds valuable data into machine learning models to allow artificial intelligence to detect and respond to anomalous data activities, including such activities from trusted sources.

Finally, Polymer Chain of Custody provides for full life-cycle control of information with the implementation of Digital Shredder capability. In addition to controlling access to information and documenting that access, many compliance regimes require the destruction of information under defined circumstances. An example might be a requirement that social media account records be destroyed upon the user's request as is the case with GDPR article 17. The Covax Data digital shredder renders destruction absolute and permanent by completely sanitizing the digital record, pairing with the chain of custody to provide an auditable compliant record that the data, and all copies, have been destroyed.

The fusion of Polymer Chain of Custody, Polymer Molecules, and Polymer Prism results in irrefutable provenance of the authentication, authorization, and integrity of every action on all information protected by Polymer.

DEPLOYMENT AND CONFIGURATION

Covax Data's mission is to make Information Control available to all companies from the sole proprietor to the largest enterprises and agencies. Therefore, Polymer was designed to be easily deployed, configured, and administered. Polymer protects information where it currently resides while providing the flexibility to move it to a public or private cloud, or any other storage option. Polymer acts like a HazMat suit for data. Once the suit is put on, the wearer can move about without compromising protection. Polymer is easier to deploy than a HazMat suit.

Polymer is deployed, primarily, as a Software-as-a-Service ("SaaS") solution with the ability to deploy the SaaS infrastructure in on-premise and private cloud configurations. Where Polymer is deployed strictly as SaaS, it only requires the installation of a thin client driver on the user endpoint devices and the file servers where data is accessed, whether physical or virtual. These drivers can be pushed out using any of the available IT workload automation tools such as Chef, Puppet, Terraform, etc.

To further simplify the deployment process Polymer can leverage existing LDAP or Active Directory installations to create Polymer accounts and even email customized activation instructions to all users. **Deployment of Polymer cannot be any less burdensome without sacrificing the unparalleled information control Polymer provides.**

Configuration of Polymer is designed to enable administrators to mix their perfect blend of control and convenience. Information Control is, ultimately, a challenge of conflict resolution. On the one hand, there are people who need instantaneous access to information. On the other, there are people who should never have access to the information. In between is a full spectrum of users and information that need varying amounts of transparency and opaqueness. The typical "data security" approach to this challenge is to provide an ever more complex matrix of parameters and profiles that enable administrators to define ever more specific inputs that result in an access granted or an access denied decision. Paradoxically, the finer the level of granularity that an authentication and authorization system provides, the greater the probability that a rule will be defined that produces the opposite decision as intended. **Polymer provides the capability to define fine-grained access rules while minimizing the need to use the capability.**

As discussed previously, Polymer fuses the handshake provided by the TSA's with the Authentication and Authorization of Polymer Prism, and the armor of Polymer Molecules as a basic rule for access. In addition, both Polymer Prism and the TSA's incorporate UEBA data into the decision process. This brings the benefits of AI/ML into both the front side (authentication) and the back side (authorization) of the access process and applies these in a continual manner. **Accordingly, if the initial configuration of Polymer is nothing more than a replication of existing security profiles, Polymer provides significantly improved authentication and authorization decisions.**

The minimal configuration of Polymer consists simply of installing the drivers, creating the Polymer Molecules, and moving data into the Molecules. Polymer can be configured for any type of operating environment – Windows, Linux, Mac, and combinations thereof – and any type of architecture – on-premises, private cloud, public cloud, hybrid cloud, and remote work. The thin client is a specialized driver that resides in ring 0 of the OS kernel where it behaves as the enforcer of policies and decisions. At this level, the Polymer driver has direct access to the hardware.

This enables the driver to control all reading or writing of data in a Molecule. Control is attached to the Molecule – not the Molecule's location - which means that Polymer Molecules can be moved within your ecosystem, yet are rendered useless when removed from your ecosystem. This means that an installation of Polymer, even with no additional configuration, provides Information Control unavailable in any other product.

CONCLUSION

The concept of "data security" is an inadequate paradigm for securing information assets in modern times. Polymer provides Information Control which leverages the distinction between data and information. By fusing Authentication, Authorization, Integrity, and Provenance, Polymer makes information ephemeral – existing only when needed and dissolving to simple data when at rest. Covax Polymer goes beyond data security and provides for genuine Information Control.