Validian Technology & Solutions Overview

The Cyber Objective - Protecting Data & Digital Assets Regardless

Validian protects applications, and critical data and digital assets ("Data"), from the ongoing onslaught by hackers, malware and other internal and external malicious parties, even when perimeter & Zero Trust cyber security, networks and devices have been breached or otherwise compromised.

While perimeter cyber security and Zero Trust cyber security are very sophisticated and should continue to be used, they are technologically incapable of preventing breaches of, and/or protecting, Data, even when enhanced by Artificial Intelligence. Given the increasing sophistication and mutation of cyber attacks exploiting Artificial Intelligence, perimeter and Zero Trust cyber security will always be breached or bypassed whereupon applications, Data and critical infrastructure will be improperly accessed and/or stolen.

ValidianProtect Technology

Validian's unique Application & Data Protection Software, **ValidianProtect**, is a powerful, flexible, scalable and rapidly integrated cyber security middleware that quickly builds, deploys and manages Trusted Distributed Applications & Solutions on centralized or decentralized networks, to seal off the application and the Data therein from threats posed by malicious parties.

Validian's technology protects applications and Data **seamlessly** against exposure and risks with additional unique features and in an increasing number of areas not otherwise protected by other cyber security measures. **Validian protects applications and Data even if all perimeter and Zero Trust cybersecurity has been breached and if the network or devices have been otherwise compromised regardless of the form of cyberattack including by hackers or malicious insiders or by phishing, vishing, ransomware, spyware, malware, viruses and zero-day vulnerabilities.**

ValidianProtect Solutions

Validian technology includes **ValidianProtect Software Development Kits (SDKs**) that enable any developer, with or without cybersecurity expertise or experience, to **rapidly** integrate any of ValidianProtect's features & capabilities into a new, existing or legacy compiled or web application that uses one of MSFT Windows, Android, Linux or Apple operating systems for client-server, server-to-server or peer-to-peer architectures on mobile and non-mobile devices.

Validian has used its **ValidianProtect** software to build the following solutions, which can also be used in combinations to create other **ValidianProtect** solutions:

- **Integrated Factor Multi-Factor Authentication (IMFA)** comprises the integration of multiple device, application instance &/or browser identities with each other and with multiple user factors for authentication during log-in and/or critical application actions over secure channels. This is in contrast to the 2 or 3 factors over penetrable channels used by most other MFA approaches that are readily bypassed.
    - **IMFA** ensures that critical applications, Data and critical infrastructure can only be accessed and used by designated and authenticated end users, web and compiled applications, browsers, devices, operating systems and technology platforms

- **ValidianProtect Dynamically Changing Policies (Credentials, Encryption Algorithms, Encryption Keys)**
    - dynamically changing credentials on demand, where the enterprise (government or commercial) administrator(s) can instantly revoke and/or change and reissue the credentials for any combination of endpoints and individuals. These newly reissued credentials are changed and reissued to all respective endpoints **in a matter of seconds**. These credentials are key based not password based and cannot be stolen to be exploited by malicious intruders or malware.
    - dynamically changing algorithms wherein the enterprise (government or commercial administrators) can instantly change the encryption algorithm (selection of 26 standard encryption algorithms, 7 FIPS encryption algorithms or the enterprise's

choice of adding any others). The newly reissued algorithm is changed and reissued to all respective endpoints in a matter of seconds.
    - dynamically changing private keys (for encryption and decryption of Data) on demand or on schedule in increments of 1 second totaling up to weeks or months although we suggest using a matter of minutes at most). Each newly reissued respective private key is changed and reissued to all respective endpoints in a matter of seconds. These keys cannot be stolen to be exploited by malicious intruders or malware.

- **Validian-Protected Databases**

  ValidianProtect encrypts data and tables in databases, using its policy-driven encryption algorithms and application-controlled keys. There are also special provisions for maintaining integrity, so that data in databases cannot be improperly accessed, tampered with or compromised, with scanning on demand or on schedule, alerts and reports and additional protections if tampering has been attempted including the immediate quarantining of the database.
    - encrypted databases mean any theft or improper access of databases by ransomware, other cyberattacks or malicious insiders only obtains encrypted data greatly reducing economic losses and legal exposure and eliminating the need to pay ransoms

  ValidianProtect can secure most databases rapidly including but not limited to:
    - MSFT Access Database Management System (DBMS)
    - MSFT SQL Relational Database Management System (RDBMS)
    - MY SQL RDBMS
    - ProgreSQL RDBMS
    - IBM DB2 SQL RDBMS

- **Validian-Protected Memory**

  ValidianProtect encrypts data in memory, using its policy-driven encryption algorithms and application-controlled keys, so that data cannot be accessed in memory, such as by memory scraping malware, with alerts and reports upon attempts at improper access.

- **Validian-Protected Files (Storage)**

  ValidianProtect encrypts Data in files, using its policy-driven encryption algorithms and application-controlled keys, so that Data cannot be improperly accessed in the file system, such as with malware, with alerts and reports upon attempts at improper access.

- **ValidianProtect Data Drive**

  The ValidianProtect Data Drive encrypts and protects Data on a virtual drive on computers, servers, network servers, shared networks servers and the Cloud
    - better protection than other secured storage including on any Cloud and facilitates recovery from ransomware and other Cyber Attacks

- **Control of Usage of Unencrypted Data**

  ValidianProtect enables the enterprise to protect its Data:
    - by controlling the ability of any end user to access, create, open, read, copy, save, edit, print and manipulate, forward and/or export Data outside of the application network
    - by providing the ability to retract Data immediately from any end user upon demand as well as to set a time limit for automatic deletion and to revoke credentials of and access by any end user immediately upon demand. Retraction of Data without controlling the use of that Data beforehand provides minimal value.
    - with alerts and reports upon any authorized uses and any attempts at any prohibited uses

- **Secure Usage of Unencrypted Data**

  Unencrypted Data in use, or between encrypted transit and encrypted storage, within a Validian-enabled application or solution cannot be improperly accessed, stolen or infected by any malware or spyware that has infected a host device or network or by any unauthorized external or internal party.

- **ValidianProtect Application & Data Intrusion Prevention** (not just intrusion detection)

  Validian creates a virtual closed system (not just a "wrapper"), which Validian calls a "Realm". This Realm ensures that only authorized application endpoints can participate and provides a protective barrier against cyber attacks and improper access, oftentimes even when other cyber security measures that are present (e.g. firewalls, intrusion detection, threat prevention, Zero Trust etc. with or without artificial intelligence) fail, or devices have been hacked, improperly accessed, infected with malware or spyware or otherwise compromised, even through zero-day vulnerabilities.
    - this prevents access of new, existing or legacy Complied Apps or Web Apps and the Data therein by any unauthorized internal personnel (e.g. malicious or careless insiders) or external parties (e.g. hackers, malware, spyware or ransomware)

- **Secure Transport** uses dynamically changing encryption algorithms on demand and dynamically changing symmetrical encryption keys on schedule or for each message, which encrypts Data (messages and attachments) on an "extended end-to-end" basis from within the sending application to within the receiving application
    - that is enhanced with dynamically changing levels of compression on demand and 16 types of addressing
    - this is not just "end-to-end" encryption, which can be bypassed because it is in the network or perimeter not in the application
    - there are no stored cryptographic keys to steal to decrypt encrypted data stolen during transit
    - there is no gap in cyber security protection between Secure Transport, Secure Storage and Secure Usage i.e. the cyber security protection is **seamless**

- **Guardian App**, which can be private labelled, for secure communications and secure rapid, large file transfers for internal or external usage, that includes:
    - IMFA to authenticate the Guardian App sending and receiving endpoints, host device(s) and end user(s) to each other
    - Secure Transport
    - Secure Storage
    - Controls of Usage of Data
    - Secure Usage
    - dynamically changing on-demand credentials for all endpoints makes it more secure than WhatsApp, Signal or Telegram and all email apps whose credentials can be, and often are, stolen and exploited
    - more secure, faster and efficient than SFTP (Secure File Transfer Protocol), SMS or texting

- **Validian-enabled WebApps** comprising
    - IMFA to authenticate the server, client, client host device and end user to each other even if SSL/TLS is already implemented in the WebApp
    - dynamically changing credentials and "extended end-to-end" encryption of messages between the client and server using policy-driven encryption algorithms and application-controlled keys
    - Validian Protected Databases and Memory of the WebApp(s)

- **Validian-enabled Browsers**
    - a session specific, rapidly activated Validian Add-In for any designated browser
    - with Validian Runtime Browser Authentication with unique identifiers and dynamically changing service credentials and policy-driven encryption algorithms and application-controlled keys, on demand and/or on schedule, so that only designated and authenticated browsers can access a designated and authenticated webapp
    - with IMFA to authenticate the designated Browser, accessed by the designated and authenticated end user to access the designated and authenticated WebApp server & client on a designated and authenticated WebApp host device even if SSL/TLS is already implemented in the WebApp and Browser
    - dynamically changing credentials and extended "extended end-to-end" encryption of messages between the designated Browser and the designated WebApp using policy-driven encryption algorithms and application-controlled keys, and even if SSL/TLS is already implemented in the WebApp and Browser

- **Validian-enabled Sandbox**

  A modified ValidianProtect Data Drive for saving, storing, reading and using attachments of any file type that may or may not be infected with ransomware or other malware or viruses
    - with Validian protected Readers so that the user can open and read the attachment inside the Inbox and/or Sandbox and not activate any ransomware or other malware or viruses
    - with the ability to then copy the content of the opened attachment inside the Sandbox and then paste the content outside the Sandbox to then use the content and document without the ransomware or other malware or viruses

- **Validian-enabled Microsoft Outlook**

  Microsoft Outlook is the most used email by enterprises but it is also a major vector of cyber attack for phishing and ransomware. So Validian has created a virtual, transparent Validian Add-In to Microsoft Outlook that prevents phishing, ransomware and other malware from exploiting Microsoft Outlook:
    - with IMFA to authenticate the Outlook app sending and receiving endpoints, designated host device(s) and designated end user(s) to each other
    - with extended end-to-end encryption of messages and attachments between the sender and receiver
    - a Validian protected Reader that enables a user to open the attachment of any file type in the Outlook Inbox and read that attachment, which may or may not be infected, without activating any malware or viruses
    - a Validian-enabled Sandbox for saving the attachments, which may or may not be infected, and which then can be opened in the Sandbox with a Validian-enabled Reader without activating any malware or viruses. The content can be copied and then pasted outside the Sandbox to then use the content and document without the ransomware or other malware or viruses.
    - the ability of the enterprise to force each end user to only sign on to Outlook using IMFA and to only use the Sandbox for saving, opening and using attachments, thereby ensuring that the enterprise is not exposed to phishing, ransomware, other malware and other forms of cyber attacks
    - administrator-controlled policy directing the method of verification to use during login and/or critical application actions such as sending a PIN code to a secure device or reading a protected QR code

- **Validian-enabled Anti-Phishing & Anti-Ransomware Solutions**

  A comprehensive Validian-enabled Anti-Phishing & Anti-Ransomware Solution(s) thereby protecting the Data but also protecting the network(s) and devices against ransomware and other malware, comprising:
    - VP-enabled/encrypted Databases
    - VP-enabled Memory
    - ValidianProtect Data Drive
    - VP-enabled WebApps and therefore any online webapp
    - VP-enabled Browsers
    - IMFA for authentication during log-in and/or critical application action
    - VP-enabled Sandboxes
    - VP-enabled MSFT Outlook

- **Validian Removal & Neutralizing of Existing Malicious Intruders and Malware from Government & Commercial Digital Operations, Critical Infrastructure, Applications, and Data**

  This ValidianProtect Solution is designed to rapidly identify, isolate, and eliminate all forms of **known and unknown** unauthorized access, including existing malicious intruders, rogue insiders, and advanced malware, from government and commercial systems. It also integrates proactive defense mechanisms to prevent future threats from gaining access or causing harm.
    - without the lengthy time of an Incident Response and the recovery implications of wiping everything and then reinstalling