January 2022

Validian

ValidianProtect Features

Validian

Seamless data protection — now.

Validian

ValidianProtect Features List

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 on centralized or decentralized networks, to seal off the application and the data therein from threats posed by malicious parties.

Many different types of applications can be protected or existing applications extended; from legacy client/ server applications, to fully distributed business and industrial applications, to more modern web, mobile and Cloud applications, easily and intuitively.

These applications can then be deployed on either a cloud, on-premises or hosted basis with the level of protection controlled dynamically by administrators.

With its innovative Protection Realms, ValidianProtect encompasses and seamlessly protects the application and the **complete life cycle of data** encrypting data in memory, in databases, in storage, in transit and against the interception of data by untrusted operating systems as well securing data in **all forms of usage, including creation, opening and reading, copying, saving, editing and manipulation, forwarding or exporting**.

Furthermore, ValidianProtect **seamlessly** secures data in use, in memory, in databases, at rest (storage) and in transit on and between all devices, operating systems and technology platforms so that the application and the data are never exposed and cannot be improperly accessed, copied or stolen regardless of any type of cyberattack or vulnerability or if the host device or network has been hacked or improperly accessed, infected with viruses or malware, or otherwise compromised, thereby protecting the confidentiality and integrity of data.

The ValidianProtect product line consists of:

- the **Application & Data Protection Platform** that protects against network-borne vulnerabilities such as intrusion, impersonation and interception
- the **Data Protection Module** that protects against host-borne vulnerabilities such as memory-scanning and file system scanning as well as provides ready-built capabilities such as flexible control over usage and retraction of data and immediate alerts on the permitted usage, and on the attempted prohibited usage, of data
- a **Confidential Application Tool Kit comprising** a **set of programming tools and Software Development Kits (SDKs)** that facilitate integration of the platform and module within the target application

ValidianProtect Application & Data Protection Platform Features

Integrating the **ValidianProtect** **Application & Data Protection Platform into an existing or new application ("App") enables and provides the App with the following features:**

Low Cost, Rapid Integration, Development & Deployment of Consistently High Quality, Secure, Feature Rich, Mobile, Cloud, Web, Local & Network Applications:

- **by any developer**, without any security expertise or experience
- integration ranges from a few days to a few weeks compared to integration of: SSL/TLS (Secure Sockets

Layer/Transport Layer Security) or PGP (Pretty Good Privacy), which can take 6 to 18 months; SSL/TLS & PKI (Public Key Infrastructure), which can take 15 to 24 months; or wrapping, which can take 12 to 18 months; and none of which, and no combination of, have the level of security, functionality and features as ValidianProtect

Enhanced Cyber Security with:

Cyber Security Information Policy Management Platform for Enhanced Information Policy Management & Access Control, which enables Information Technology (IT) or cyber security personnel in a Validian-enabled environment:

- to provide and to reconfigure dynamically standardized cyber security, crypto & information policies governing communication of data and to redeploy these in seconds to all application endpoints. Current policies apply Authentication, 26 Encryption Algorithms, Key Management and Variable Compression, Permissions & Access Control, Advertising, and Information Retraction
- to govern, to enforce and to manage who can and who cannot access specified data or digital information
- to govern, to enforce and to manage who can and who cannot access specified servers, databases, mobile devices and non-mobile devices
- to govern, to enforce and to manage who can and who cannot communicate with whom
- to turn each feature and policy on or off in any combination of features

which enables IT or cyber security personnel and/or end users in a Validian-enabled environment:

- to govern, to enforce and to manage who participates in any of one or more of their groups and who individually or by group can access them or communicate with them
- to govern, to enforce and to manage their data and digital information, including what any recipient can do, or not do, with any particular data or digital information the End User has sent to the recipient such as storing, sharing or forwarding

Application Authentication: using dynamically changing Service Credentials comprising pairs of public and private keys and non-third party certificates that prevent any internal or external access of or communication between mobile, Cloud, web, local and/or network applications and access of the data therein until and unless they are mutually authenticated

- new Service Credentials are issued upon initialization as well as upon manual or automatic replacement and are deployed automatically to every applicable Validian-enabled App endpoint without any recoding or installation
- the Revoke Function takes an existing Service Credential away from one or more Validian-enabled App endpoints/end users, which can then no longer access or use the Validian-enabled App under strict authentication
- the Replace Function takes away an existing Service Credential from, and then reissues a new Service Credential to, one or more Validian-enabled App endpoints/end users
- Manual Revocation and Manual Replacement can be done by the Administrator upon demand at any time
- Automatic Revocation and Replacement can be done by the Administrator upon demand at anytime or on a set schedule such as every hour, # of hours, days or weeks
- ensures secure access to digital information on mobile & non-mobile devices, servers & databases and in memory
- ensures secure access to mobile & non-mobile devices, servers & databases
- prevents internal and external hacking and improper access of, and thereby certain types of cyber attacks against, the application and the data regardless if the network, host device, servers, other devices or other applications have been compromised, including with viruses and malware

Integrated Authentication: integrating authentication of the application with two-factor randomly generated PIN's and/or three-factor biometric end user authentication and/or with the unique identifiers of the host mobile device, non-mobile device, server, database or infrastructure

- an additional control on which end users and which devices can access specified applications, data and digital information

"Dynamically Changing" Encryption Algorithms

- the Administrator selects any one of the standard encryption algorithms provided (e.g. 26 in the standard version, 7 in the FIPs version and/or any others on a plug-and-play basis) upon initialization and then can replace on demand the existing encryption algorithm by selecting a different one and the next encryption algorithm will be deployed each time automatically to each applicable Validian-enabled App endpoint without any recoding or installation
- eliminates the current "Pick One Syndrome" where cyber security developers have to select and install only one encryption algorithm
- enables change of encryption algorithms in seconds at no cost versus current and historical process of change of recoding and re-installation that takes months to years and can cost large organizations and governments in the hundreds of millions of dollars
- enables interoperability between organizations, governments and world regions that prefer particular encryption algorithms
- can create specific Protection Realms of designated groups for communication and data sharing to the exclusion of all other parties by changing that Realm to another encryption algorithm
- immune to the breaking of particular encryption algorithms because the encryption algorithm can just be changed and changed faster than even Quantum Computing can break it

"Dynamically Changing" Symmetrical Keys for Encryption

- Symmetrical Keys for encrypting and decrypting data for transport, which are issued prior to and after each message exchange, are deployed automatically to every applicable Validian-enabled App endpoint without any recoding or installation
- so there are no stored cryptographic keys to steal to decrypt encrypted data stolen during transit
- this is not a form of PGP, which uses Public (asymmetrical) key encryption and Private (symmetrical) key decryption

Extended Encryption & Decryption with Variable Compression of Data in Transit

- compresses data first and then encrypts the same data **inside** the sending application **prior** to commencement of transport of data
- followed by secure transfer of that data in a virtual, session-specific tunnel from inside the sending application to inside the receiving application where the data is then decrypted so that data never travels in the clear including in the OSI stack
- encrypts, transports and decrypts data of any type, format and size
- *also prevents theft or improper access of data by untrusted operating systems and rooted devices*

"Seamless" Security: so that data is always protected and never exposed during usage, in memory, in databases, in storage and in transit as well as between each of these stages

- all other cyber security implementations are a fragmented patchwork of various point solutions: crypto protocols such as SSL/TLS, PKI and PGP for encrypted transport of data, which must be supplemented by separate encryption for storage of data and a range of network filter technologies to protect the network or perimeter like smart firewalls, intrusion and threat prevention systems, and anti-malware, which do not work together seamlessly and have security gaps between them that are readily exploited.

Enhanced Performance and Reduced Costs of Mobile & Non-Mobile Communications With:

Addressing & Roaming Scheme with all 16 possible addressing configurations and 5 roaming aspects that is abstracted from, and independent of, Internet Protocol (IP) addressing

- hides applications from hackers - if they can't be found, then they are more difficult to exploit
- eliminates or greatly facilitates infrastructure reconfigurations due to IP address changes, which are particularly problematic for mobile applications
- enables the immediate location, authentication of and communication with applications, including mobile when they are assigned different IP addresses such as when roaming

Dynamic and Systematic Data Logic that automatically adapts to: form of connection (e.g. wired, wireless, mobile, dial-up); connection speed and bandwidth; and regardless of size, format or type of data.

Variable Compression and Encryption of the Same Data *which increases speed of transmission of data while reducing bandwidth consumption and maintaining security of data in transit*

Secure Peer-to-Peer (P2P) communications and data transfers, critical for decentralized networks as well as secures client/server and server-to-server communications and data transfers of centralized networks

- the use of Validian's secure P2P infrastructure results in significant infrastructure operational cost savings as compared to the traditional client-server infrastructure that burdens enterprise, government, social media and mobile messaging operations
- traditional crypto protocols like SSL/TLS and PGP cannot encrypt P2P communications or data transfers, rather only the traditional client/server communications and data transfers

Secure, Efficient Internet (i.e. IP-based) Advertising, marketing and notification channel that transports and delivers graphic rich advertising content through mobile, web and non-mobile applications viewed by end users

- immune to advertising blockers thereby enhancing delivery and quality of advertising "Impressions" to end users and prevents certain types of cyber attacks that exploit advertising as a means of access

Cross Platform Ready and Multi Platform Interactive by being designed, architected and coded to work on, and between, and/or migrate to, any mobile, non-mobile or server operating system including Android, Windows and Windows Phone OS, Apple O/S and iOS, Blackberry QNX, Tizen and all Unix and Linux platforms.

Designed & Architected to Protect Critical Information on all Platforms and Devices

- Laptop & Desktop Computers, Mainframe Computers, Servers and Databases
- Mobile Devices and Networks
- Cloud Environments
- Browsers and Web Apps
- Internet of Things (iot)
- Software Defined Networking (SDN)
- SCADA (e.g. smart sensors)

ValidianProtect Data Protection Module Features

The ValidianProtect Data Protection Module contains a group of downloadable, re-usable features and capabilities, which make it possible for a programmer to quickly and easily add any combination of a

significant number of pre-built, commonly used functions and first-to-market differentiating features to or from any application, thus saving many man-years of previously extra development time.

Transfer of Formatted Data Packets over TCP/IP (Transmission Control Protocol Over Internet Protocol)

- secure texting and messaging
- secure file transfer
- secure data transfer

A similar set of features will be created when ValidianProtect is migrated to UDP (User Datagram Protocol) for the transfer of unformatted data packets over UDP:

- secure encrypted voice
- secure encrypted audio
- secure encrypted video

Protection of Data in Memory

Data in memory is encrypted, so that unencrypted data cannot be accessed in memory, such as by memory scanning or scraping malware.

Protection of Data in Databases

Data in databases is encrypted, so that it cannot be improperly accessed.

Control: the ability of the sender to control what the recipient can do with the data (text or file) sent:

- urgent or caution notification (see Alerts)
- time limit for remaining in queue on sending device when not sent yet
- time limit for delivery after which the data (text or file) disappears
- time limit for opening/reading after delivered to receiving device after which the data (text or file) disappears
- open and read only (a subset of save or not save to safe)
- keep or disappear (with time limit) after delivery or read
- save or not save to safe
- copy or not copy (to screen buffer)
- forward or not forward from conversation
- forward or not forward from safe
- export or not export from safe

Retract: the ability of the sender to retract the data (text or file) after it has been sent

- when remaining in queue on sending device and not sent yet
- sent but not received by receiving device
- sent and received by receiving device but not opened yet
- received by receiving device and opened but not saved yet, regardless of control feature of "save or

not save to safe"

- after saved by receiving device, and therefore when in the safe
- after forwarded by receiving device from conversation or from safe
- but not after exported from safe by receiving device

Alerts: alerts or confirmations that can be given to the sender regarding what the recipient has done with the data

- when still queued on sending device (not sent yet)
- urgent or caution notification
- when received by receiving device
- when failed to deliver (not received by receiving device)
- when opened or read (i.e. if a text only then clicked on, if a file then opened)
- when saved to safe
- when copied to screen buffer
- when forwarded from conversation or from safe
- when exported from safe
- when attempted to be saved when saving has been prohibited
- when attempted to be copied when copying has been prohibited
- when attempted to be forwarded when forwarding has been prohibited
- when attempted to be exported when exporting has been prohibited

Additional Secure Capabilities/Features

- **Peer-to-Peer (P2P) Group Management**
- **Presence & Presence Visibility**
- **Extended and Varying Presence** to each of different contacts so that the end user can show a different presence (e.g. online, offline, invisible, do not disturb, busy, away, etc) to each or any of the members in his/her group of contacts
- **SAFE: secure**, encrypted storage of messages, files and data on a device and in memory that cannot be improperly accessed if the device, servers, network or Cloud has been otherwise compromised
- **Protection of the usage of data** (e.g. reading, open on screen of host device, creation and editing of some data but potentially can protect usage for creation and editing of all data)
- **Secure Camera**, protected by Validian's virtual closed system, so that pictures are protected seamlessly from the time they are taken onwards, regardless if the mobile phone, other host device or the network is infected by malware, improperly accessed or otherwise compromised
- **PDF Viewer**, protected by Validian's virtual closed system, so that pdf documents are protected seamlessly when being transferred, received, viewed or stored, regardless if the mobile phone, other host device or the network is infected by malware, improperly accessed or otherwise compromised
- **Burn It:** when you need to wipe a conversation from your device and someone else's, you can burn it. With the feature, you forensically remove traces of your history in a conversation or with a contact from your device and their device. (There's a waiting period between burning on your local device and burning remotely. Remote burns require the burnee to log in.)

- **Find Me** lets users synch select phone contacts with the app but protect privacy by blocking others thereby enabling users to grow their contact lists quickly while maintaining control over the people who can connect with them on the platform
- **Large Message Support,** defined as largest messages that the mobile device itself can create, send and/or receive - e.g. greatly increases size of files or videos that can be sent on a mobile device
- **Large Message Support Extension,** defined as largest messages that non-mobile devices can create, send and/or receive but by sector (e.g. for eHealth would require up to 100 megabytes but Entertainment would require up to 500 gigabytes)
- **CheckPoint Restart** uses Validian's Dynamic and Systematic Data Logic that automatically adapts to: form of connection (e.g. wired, wireless, mobile, dial-up); connection speed and bandwidth; regardless of size, format or type of data; and then breaks the data to be transferred into a specific numbers of sequentially numbered data packets, so that when the data is transferred, if the transmission is interrupted, the transfer recommences at the next sequential data packet instead of having to resend all of the data again. When all of the data packets have been transmitted then the receiving App reassembles the data packets in order.