January 2022

ValidianProtect(™)

Our unique Application & Data Protection Software takes seamless data protection, and your business, seriously.

Validian

ValidianProtect (TM)

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 its data from threats posed by malicious parties.

Many different types of applications can be protected and/or extended; from legacy client/server applications, to distributed business and P2P social networking applications, to web, mobile and Cloud applications, easily and intuitively.

These applications can then be deployed on either an on-premises or a hosted basis with the level of protection controlled dynamically by administrators via intelligent policy directives.

Each Validian-enabled, Trusted Application has an unlimited number of virtual closed systems, termed "Realms", which encompass and seamlessly protect the application and the complete life cycle of data encrypting data in memory, in databases, in storage, in transit and against interception by untrusted operating systems, as well as securing data in all forms of usage, including creation, opening and reading, editing and manipulation.

ValidianProtect can protect the confidentiality and integrity of data by seamlessly securing data on and between all devices, operating systems and technology. Data is never exposed and cannot be improperly accessed, copied or stolen regardless of any type of cyber attack or vulnerability or if the host device or network has been hacked, improperly accessed, or infected with viruses or malware.

The ValidianProtect product line

1. The Application & Data Protection Platform that protects against network-borne vulnerabilities such as intrusion, impersonation and interception.

2. 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.

3. 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 Features Overview

ValidianProtect is an Application & Data Protection Platform that integrates into an existing or new application ("App") and provides the following features:

Comprehensive Security

Protection of critical data while in use, in memory, at rest (storage), in transit and against interception by untrusted operating systems.

Validian

Low cost of development & deployment

Easy-to-use programming model & APIs that enable:

- Rapid Integration
- Development & Deployment of Consistently high quality, secure, feature rich:
  - Mobile
  - Cloud
  - Web
  - Local & Network Applications

Policy Driven Cyber Security

Policy Management Platform that allows Information Technology (IT) or cyber security administrators to dynamically control the security parameters of the Validian-enabled environment.

Application Authentication

Dynamically changing service credentials comprising pairs of public and private keys and non-third party certificates that protect communication and access of data until and unless application endpoints are mutually authenticated.

Integrated Authentication

Enhanced user authentication using two-factor randomly generated PIN's, three-factor biometric authentication or with the unique identifiers of the host platform.

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

Dynamically Changing Encryption Algorithms

Rich set of standard encryption algorithms (e.g. 26 in the standard version, 7 in the FIPs version and/or any others on a plug-and-play basis) that can be changed on initialization or on demand and automatically deployed each time to Validian-enabled App endpoints without any recoding or re-installation.

Dynamically Changing Symmetrical Keys for Encryption

Symmetrical Keys for encrypting and decrypting data in memory, in databases, in storage and for transport, which are issued on initialization and changed after each message exchange, and are deployed automatically to every Validian-enabled App endpoint without any recoding or re-installation.

Extended Encryption & Decryption with Variable Compressionof Data in Transit

Compresses data first and then encrypts the same data inside the sending application prior to commencement of transport of data.

Seamless Security

Protection can be seamless from inside the sending App to inside the receiving App with limited exposure.

Validian

Enhanced Performance and Reduced Costs:

- Unique Addressing & Roaming Scheme
- Dynamic and Systematic Data Logic
- Variable Compression and Encryption of the Same Data
- Secure Peer-to-Peer (P2P) communications and data transfers, critical for decentralized networks
- Designed & Architected to Protect Critical Information on all Platforms and Devices:
  - Laptop & Desktop Computers, Servers and Databases
  - Mobile Devices and Networks
  - Cloud Environments
  - Browsers and Web Apps
  - Social Media
  - Internet of Things (iot)
  - Software Defined Networking
  - SCADA (e.g. smart sensors)

In-application Content Provisioning

Secure Internet advertising, marketing and notification channel that allows direct communication to all endpoints.

Professional Grade

Configurable fault-tolerance and load-balanced components for scalable and reliable operation.

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 unique differentiating features to or from any application, thus saving many man-years of previously extra development time.

- Transfer of Formatted Data Packetsover TCP/IP (Transmission Control Protocol Over Internet Protocol)
- Protection of Data in Memory
- Protection of Data in Databases
- Control: the ability of the sender to control what the recipient can do with the data (text or file) sent
- Retract: the ability of the sender to retract the data (text or file) after it hasbeen sent
- Alerts: alerts or confirmations that can be given to the sender regarding what the recipient has done with the data

Additional Secure Capabilities/Features

- Peer-to-Peer (P2P) message transfer
- Presence & Presence Visibility: Controllable display of presence to contacts to allow the end user to show a different presence (e.g. online, offline, invisible, do not disturb, busy, away, etc) to each contact
- 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
- Extended Contact Features

Validian

- 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 and PDF viewer: In-application capture and viewing of content that prevents unauthorized disclosure and assures seamless protection regardless
- 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
- Forensic Burn of Content or Conversation: Wipe messages from sender and receiver devices to remove any traces of conversation or contact history
- Integration with Device Contact: Synch and import select device contacts to grow contact lists quickly while maintaining control over the people with whom to connect
- Large Message Support - Automatic segmentation and re-assembly of messages that are limited only by device storage capacity
- 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 - Automatic adaptation to type of connection (e.g.wired, wireless, mobile, dial-up), connection speed and connection state (error, interrupted, etc.)regardless of size, format or type of data