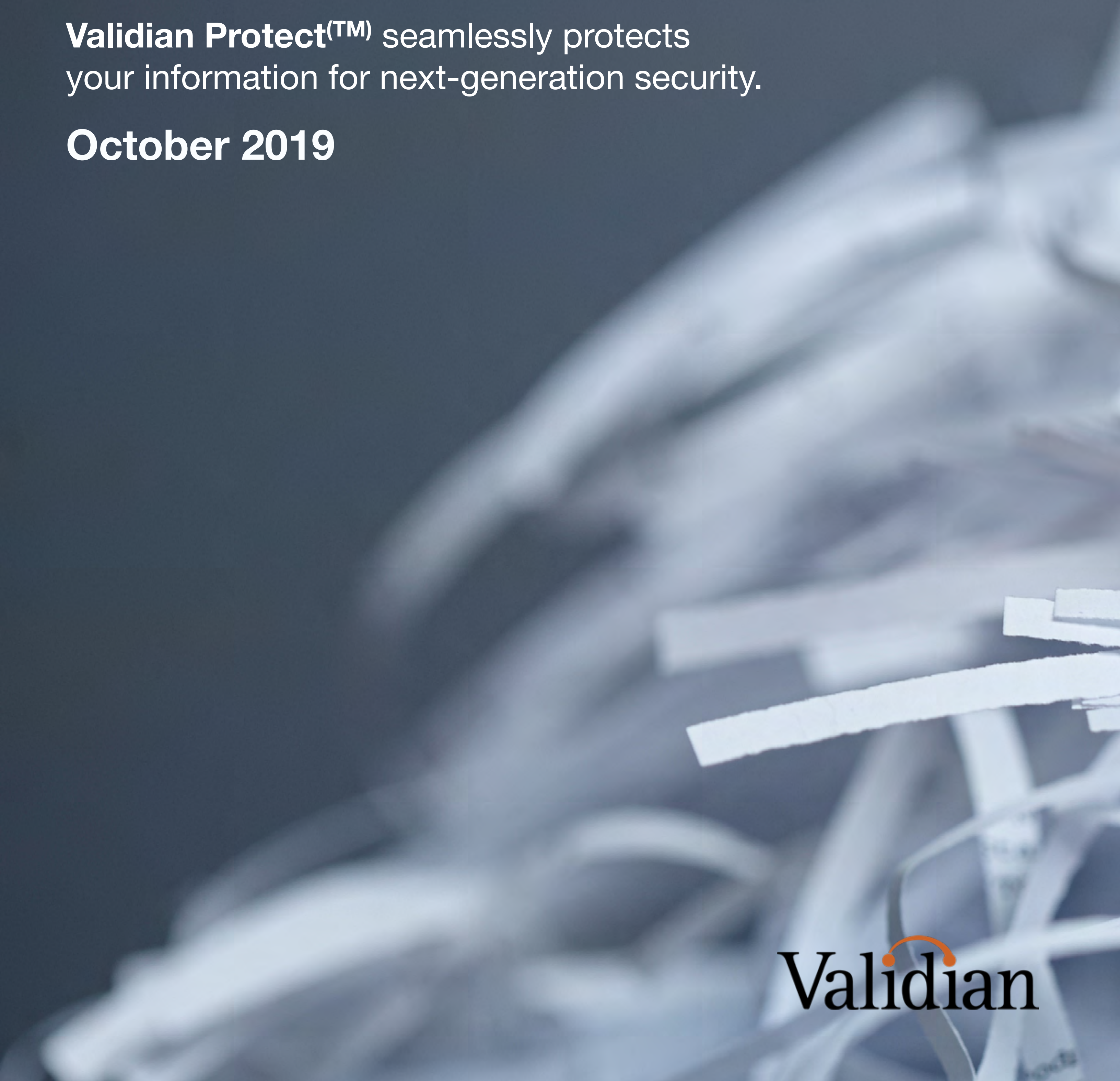
Confidentiality & Integrity of Data

Validian Protect(TM) seamlessly protects your information for next-generation security.

October 2019



Validian

Confidentiality & Integrity of Data

The triad of confidentiality, integrity and availability (CIA) is at the core of information security.

Confidentiality means that data, objects and resources are protected from unauthorized viewing and other access. Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct. Availability means that authorized users have access to the systems and the resources they need from any where at any time.

Validian Solves Critical Problems Affecting Confidentiality & Integrity of Data

There is insufficient and incomplete protection of the confidentiality and integrity of data unless the data is seamlessly secured. Seamless security includes data during usage, in memory, at rest and in transit — and between each of these states. Control on who can view and edit data is also critical. This requires software-enabled-controls on the permitted uses and prohibited uses of data that can be readily implemented, enforced and monitored in real time.

Current approaches in protecting data in all computing predominantly address securing data at rest and in transit. This leaves gaps in protection that Validian can fill.

Securing data in use is considered the third and possibly most challenging step to providing a fully secure lifecycle for sensitive data. Meeting the challenge means addressing the following:

- encrypting data in memory without exposing it to the rest of the system
- controlling permitted and prohibited uses of data.
- securing data seamlessly

ValidianProtect solves the following critical problems that plague confidentiality and integrity of data.

Hacking and Improper Access Protection

In any networked activity performed using public and private facilities (i.e. the Internet, corporate networks, etc.) there are always vulnerabilities. With the level of ingenuity and resources demonstrated by parties with malicious intentions, it is difficult to know all vulnerabilities or to know or to anticipate what future vulnerabilities are going to be.

As well, almost any device such as mobile phones, desktop computers, cloud servers, data bases, network applications, and IOT devices like sensors in power grids and automobiles can be hacked, attacked, or otherwise compromised.

Therefore it is assumed that even best practices can fail to fully protect data on any device, regardless of robust security posturing.

Application Authentication

ValidianProtect provides added protection by authenticating applications using dynamically changing service credentials. Each service credential consists 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

With Validian, access to apps, data and devices can be mutually authenticated and enhanced by integrating authentication of the application with two-factor randomly generated PINs 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.

Non-Stored Crypto Keys

Unlike other solutions which store encryption keys, ValidianProtect dynamically changes the symmetrical keys for encrypting and decrypting data for transport, upon initialization and after each message exchange.ValidianProtect deploys these keys automatically to every applicable Validian-enabled application endpoint without any recoding or installation. There are no stored crypto keys.

Data in Use

Data for almost all uses cannot be used if encrypted. So data in use is in the clear (i.e. unencrypted) and can be accessed readily by viruses and malware, as well as hackers and unauthorized parties, that have penetrated host devices and networks.

ValidianProtect can secure data in various forms of usage, including:

- creation
- opening and reading
- copying
- saving
- editing and manipulation
- forwarding or exporting

Data in Memory

During normal course of operation, data is unencrypted in memory leaving it vulnerable to malicious actors that may have infiltrated the computing device.

ValidianProtect can encrypt application data in memory so that it cannot be improperly accessed, including by memory scanning and scrubbing malware.

Malicious Insiders

Malicious insiders are a threat to all sensitive data. Insiders are ones that already have access to sensitive data so access controls are often irrelevant and standard permission controls insufficient. Insiders can either steal the data or improperly modify or share it.

Edward Snowden is one of the most famous. Other examples include movies stolen during post-production by film editors, movies stolen during pre-screening and reviews by critics, nominators for awards and studio executives as well as movies stolen during the distribution process, which events of piracy continue to populate the news. However, all organizations face this risk to their IP and other sensitive data.

ValidianProtect provides controls for the permitted uses and prohibited uses of data, allowing owners to grant or disallow various types of usage by counterparties. Permitted or prohibited use can include:

- creation
- opening and reading
- saving
- copying
- editing and manipulation
- sharing
- forwarding (which can be easily done without thinking)
- and publishing

ValidianProtect enables enforcement and monitoring in real time with tracking and alerts when a permitted use occurs and when an attempt at a prohibited use occurs, with the ability to remotely, on-demand or automatically, immediately retract data and revoke access.

Rooted Devices

Rooted devices and untrusted operating systems can improperly access data before it is encrypted by standard crypto protocols and encryption algorithms. Rooting is a process that attains privileges to modify the software code on the device or to install other software that the manufacturer wouldn’t normally allow.

ValidianProtect encrypts data inside the application prior to triggering the OS for network communication. Additionally, ValidianProtect can prevent a Validian-enabled application from working and prevent any access to data therein if there is a rooted device or if the operating system is not trusted.

Careless Insiders or Insufficient Security?

The news constantly reports on theft of money from e-transfers and online banking, with banks blaming clients for weak or careless handling of passwords. Billions of dollars of economic damage have been attributed to data breaches caused by phishing, spoofing and ransomware attacks blamed on employees unsuspectingly clicking on malicious emails or infected websites.

However, this is not just due to careless insiders with weak passwords or poor training - it's due to insufficient security.

Best practices of access control using end user authentication, comprising strong passwords, two factor (PIN's & fobs) and bio-metric (finger print or eye scans) with filters such as smart firewalls, intrusion detection and prevention, and anti-malware, supplemented with proper training are necessary measures. But they are not sufficient and will not stop sophisticated hackers.

This has become obvious.

ValidianProtect's seamless data security protects the application and the sensitive data therein, including digital money, if the password, host device or network has been hacked or improperly accessed, infected with viruses or malware, or otherwise compromised.

Blockchain

Blockchains, such as Bitcoin and Ethereum, are growing in usage as underlying decentralized records of transactions. However, a chain is only as strong as its weakest link and the apps built on top of them, and the data in those apps still have major cyber security exposures that are being exploited.

The news has been rife with stories of the breaches of apps built on blockchain resulting in the theft of hundreds of millions of dollars of cryptocurrencies from the exchanges and vaults and of digital currency from digital wallets, which are effectively theft of the data in those apps.

.

As more apps in more markets are put on top of blockchain, economic losses are going to continue to grow due to these cyber exposures.

ValidianProtect, including its P2P security, is integrated easily into the apps built on top of blockchains thereby greatly reducing if not eliminating the cyber risks to these apps and the data therein.

Seamless Security

Other cyber security implementations are not seamless — they 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. These do not work together seamlessly and have security gaps between them that are readily exploited to improperly access and steal data.

ValidianProtect can secure data in and
between all states including:

- in use
- in memory
- at rest
- in transit
- on all devices,
- operating systems
- and technology platforms

This means that the application and the data are 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 or improperly accessed, infected with viruses or malware, or otherwise compromised - there are no security gaps in between that can be exploited.

Validian Also Enhances Availability

Reduced Time To Market & Costs

It generally takes 1 to 2 years to develop each and every application depending on the level of sophistication — despite sales pitches by developers that they can do so in a matter of weeks to a few months.

It generally takes an additional 9 to 15 months for each and every application to insert standard crypto protocols, such as TLS or a wrapper, for encrypted data transport and a separate encryption algorithm for encrypted data storage — also despite sales pitches by security experts that they can do so in a matter of 3 to 6 months.

Building a new app, or enhancing an existing app, with ValidianProtect's pre-built seamless data security, functionalities, features and capabilities generally takes two weeks to two months by any developer, with or without security expertise, depending on the sophistication of the Graphic User Interface.

Enhanced Mobile Availability

Mobility has become essential to personal and business life yet is still plagued with problematic usage, particularly when roaming or traveling, and costly consumption of bandwidth as more computing and internet usage is migrated to mobile.

ValidianProtect's mobile-enhancing features include:

- unique addressing & roaming scheme enhances mobile availability particularly when roaming or traveling by facilitating reconfigurations due to IP address changes, which are particularly problematic for mobile applications

- dynamic and systematic data logic that automatically adapts to:

1. form of connection (e.g. wired, wireless, mobile, dial-up);
2. connection speed and bandwidth, regardless of size, format or type of data.

- variable compression and encryption of the same data increases speed of transmission of data while reducing bandwidth consumption and maintaining security of data in transit, regardless of file type or size.

Enhanced Encrypted Interaction

Encrypted communications and data transfers require communicating endpoints to use the same encryption algorithm.

ValidianProtect uses the same standard encryption algorithms available in other crypto protocols such as SSL/TLS. However, with SSL/TLS and other approaches the cyber security developers have to select and integrate just one of these encryption algorithms and cannot change and redeploy these rapidly.

It can take almost a year and millions of dollars for a large organization to change their encryption algorithms once.

ValidianProtect dynamically changes the encryption algorithms on demand. These changes are very fast (a matter of seconds) and automatically deployed to each applicable endpoint without any recoding or installation. So the administrator can change the encryption algorithm rapidly and often for enhanced security.