Validian is first-to-market with the next generation of Information Policy Management technology that provides the next generation of Intrusion Prevention, which fully secures existing and/or new mobile, non-mobile and web applications on, and the storage, access and transfer of digital information on or between, mobile and/or non-mobile devices over wired, wireless and mobile networks for peer-to-peer, client-server and server-to-server transmissions.

Mobile is a Juggernaut with over 2 billion smartphones and tablets accessing mobile applications, web applications and compiled applications on other mobile devices and on non- mobile devices (servers, desktop and laptop computers). Validian has completed development of its core technology and is now launching the Validian-enabling of mobile, social media, web and non-mobile applications, many with tens of millions of endpoints where potential M&A acquisition valuations increase exponentially with the growth in the number of Validian-enabled endpoints.

The Problem: Digital Information is where the value is: sensitive Government and business information, confidential personal financial and medical records, movies and music. EVEN MONEY IS NOW DIGITAL. Where there is value, hackers, thieves, governments and competitors want to gain unauthorized access to and/or steal this valuable Digital Information.

All Digital Information is stored, accessed, retrieved, transferred, received and then stored again by applications. Valuable Digital Information should do so securely because currently, greater than 90% of successful cyber attacks start by hacking the applications that store, access and/or transfer Digital Information, resulting in billions of dollars in losses and exposure. The reason is because existing cyber security technologies and products protect the networks and authenticate end users and hardware but do not prevent hacking or unauthorized access of the applications nor protect sufficiently against the unauthorized access of or theft of Digital Information.

The most visible problem is that all larger businesses, organizations and every level of Government have state of the art cyber security implementations that encompass all of the solutions and products outlined in the Cyber Security Landscape described below. While all of them are necessary, none are sufficient to stop the onslaught of cyber attacks. The result is that there is an estimated range of $300 Billion to more than $1 Trillion in annual economic losses due to security breaches and data theft (McAfee, July 2013). **Accordingly, "companies & government need to take a radically different approach to cybersecurity". (U.S. Secret Service, May/14) Another generation of Firewalls, Antivirus and Intrusion Detection Systems applying security to the network is insufficient. What is required is software only, asynchronous technology that applies security directly to the data because that is where the value is (Yahoo, Aug/14). This is Validian!**

The less visible but significant problem is how to manage the mobile and non-mobile devices and particularly the integration and management of the information and crypto policies that manage the Digital Information. This problem is causing enormous and ever increasing operational and administrative problems and costs and causes some key vulnerabilities to cyber attacks.

The Cyber Security Landscape: Virtually all existing cyber security technologies, products, solutions and approaches fall within one of the following categories. None of them do what Validian does and none of them are designed to ever do what Validian does. Validian does not replace these rather works seamlessly to "seal the gaps" that cyber attacks currently exploit.

Filters monitor and inspect the traffic of data packets over IP based networks to detect "known" suspicious, unwanted or malicious content or activity. First generation Filters inspect data packets transferred over IP based networks between the first 3 layers of the OSI model, i.e. between the Physical Layer and the Network Layer. Second generation Filters perform the work of their first-generation predecessors but operate up to layer 4 (Transport Layer) of the OSI model. Third generation Filters inspect the transfer of data packets up to the Application Layer (layer 7) and to the application endpoints. If the inspection of the data packet results in detecting malicious content or activity then the data packet is dropped, rejected or blocked. Depending on what the Filter is detecting dictates where the Filter falls into one or more of the following product categories:

Anti-Spam inspects email and its attachments for spam**. Firewalls** inspect data packets to compare against a set of rules as to whether access to the network or application endpoint is permitted. **Antivirus & Anti-malware** inspect data packets for viruses and malware. **Intrusion Detection** and its next generation **Intrusion Prevention Systems** inspect data packets for cyber attacks and other malicious activity that have breached networks or are in transit to application endpoints. As these various types of Filters have evolved in a series of generations, all of them are now evolving to incorporate Virtualization. To date, Filters cannot risk exposing the network by opening attachments and data packets to accurately determine exactly what they contain, which is why all types of Filters have less than a 100% rate of detection of "known" malicious packets, a significantly less and even minimal detection rate of "unknown" malicious packets and also have false positives, thereby dropping, rejecting or blocking valid data packets that are not malicious.

Virtualization is now being used by the latest generation of Filters to test unverified programs, data packets and attachments, which may contain a virus, other malignant code or malicious content, particularly those that are "unknown", without allowing the software to harm the host network or device by directing it to, opening and testing it in a safe, virtual environment or container within a network or on a device.

Application Code Scanning solutions identify weaknesses in the coding of applications, which can be exploited by hackers who gain access to those applications to insert malicious code.

Crypto Policy technologies and solutions, primarily comprised of SSL/TLS, PKI, PGP/GPG & VPN's, integrate crypto policies regarding certificates, encryption algorithms, public & private cryptographic key exchanges, keys and key length at the Network Layer to apply these policies for end user authentication to the Network and to encrypt, transfer and decrypt data packets outside the application between the application endpoints. These suffer from the "Pick One" Syndrome of hard coding one set of encryption algorithms and sometimes symmetrical keys, limited policy management, "end-to-end" encryption and an inability to secure Peer-To-Peer communications. Management and operations are tedious, costly and unsuited for mobile.

Mobile Device Management (MDM) software monitors and manages mobile devices deployed across mobile operators, service providers and enterprises. They do not manage information or crypto policies. Any security, which is not their core competency, tends to be limited to standard 2 factor end user authentication and SSL based "end-to-end" encryption.

The Validian Approach: Validian's Information Policy Management Platform (IPMP) is integrated rapidly into the source code of the application to apply the Information & Crypto Policies to the data packets inside the application and ABOVE the Application Layer (layer 7) of the OSI model. **This obtains radically innovative results.**

- **Next Generation of Policy Management,** the **Validian Information Policy Management Platform**, which enables IT managers to provide and to reconfigure dynamically policies governing communication of data, including changing encryption algorithms, keys, key life time and level of compression, and to distribute these automatically, immediately and transparently to all end points without having to re-develop or re-install the software. No other technology or solution can do this - Mobile Device Managers cannot dynamically change policies. Furthermore, SSL is stuck with the "PICK ONE" syndrome of coding only one encryption algorithm and symmetrical key, which takes several months and significant cost to change even once. Current Validian policies apply Authentication, Encryption, Key Management and Variable Compression, but other policies, such as Permissions & Access Control, Information Redaction and Billing can be added.

- **Next Generation of Intrusion Prevention Platform** that PREVENTS, not just detects, hacking and unauthorized access of critical applications and of sensitive Digital Information, including impersonation, spoofing, phishing, Man-In-The-Middle and Man-In-The-Browser attacks. Validian has the only technology that PREVENTS more than 90% of the successful cyber attacks in the world today because these cyber attacks are initiated or targeted at the application.

- encryption of the data inside the sending application followed by secure transfer of that data in a virtual tunnel from inside the sending application to inside the receiving application where it is decrypted, so that the data cannot be stolen before the encryption process or after the decryption process. All other technologies use industry standard "end-to-end" encryption, including SSL, PKI, PGP and VPN's, where data can be stolen just before "end-to-end" encryption encrypts the data or just after it decrypts the data.

- encryption & decryption using "dynamically changing", instead of "stored", symmetrical keys to encrypt and decrypt data or Digital Information of any size, type and format, including: sensitive Government, business and personal information; confidential medical records; texting; pictures; and music, videos and movies. Unlike SSL, PKI and VPN's, with Validian the symmetrical keys cannot be stolen to decrypt stolen encrypted data.

- Variable compression and encryption of the same data at the same time inside the sending application. SSL cannot compress and encrypt the same data rather only compress or encrypt, so that data must be encrypted by SSL then compressed by another technology, which is the wrong order for effective compression.

- **Secure peer-to-peer communications as well as client/server and server-to-server.** SSL cannot secure peer-to-peer.

- **Rapid, Consistently High Quality Development of Secure Applications**, wherein Validian's technology can be integrated into an existing or new application **by any developer**, without any security expertise or experience, in an average of a few days, whereas SSL requires a developer with security expertise and can take from 4 to 24 months per application.

The Opportunity: Mobile is a Juggernaut. There are now more than 2 Billion smart mobile devices: smartphones, tablets and phablets with more than 100 Billion application endpoints. This means that each 1% of this market at $0.25 per endpoint per year is worth more than $250 million in annual revenue to Validian **plus** any advertising revenue received by Validian.

Today's valuations for M&A of emerging technology companies initially are based on the underlying technology and then increase with the # of installed application endpoints on mobile, web and non-mobile, which generate both license fee and advertising revenue.

Non-cyber security technology companies are being bought for over $40 per endpoint.

- Facebook bought Instagram for $1 Billion with 25 million endpoints in Apr 2012
- Facebook bought WhatsApp for $19 Billion with 450 million endpoints in Jan 2014
- Blackberry's BBM with 82 million endpoints added $3.5 B to its market cap after the WhatsApp acquisition

But cyber security and mobile management companies are being bought at even higher premiums

- Palo Alto acquired Cyvera for its technology (intrusion prevention), in Apr/14 for $200 million
- FireEye bought Mandient (intrusion prevention), which had only 2 million endpoints, in Dec/13 for $1 Billion
- VMware bought AirWatch (mobile device management), which only had 30 customers & less than 2 million endpoints, in Jan/14 for $1.54 Billion.

Validian is now deploying its technology to numerous sectors generating increasing numbers of Validian-secured endpoints.