



DATA SHEET



KEY FEATURES

Rapid and Flexible Deployment

- Works out of the box with no integration required
- Rollout requires no changes to applications and does not impact user behaviour
- Capable of running in both zero-integration and real-time intervention modes, for a choice of monitoring and intervention strategies

Superior Fraud Detection

- Analyses user behaviour and spots anomalies to prevent fraud including zero-day attacks
- Profiles and self-adjusts for each user for fewer false positives
- Leverages intelligence from VeriSign, a critical Internet infrastructure operator and high-assurance SSL certificate provider

Comprehensive Solution

- One platform for monitoring and authentication
- One vendor—VeriSign, your partner in consumer authentication
- Unlimited opportunities for enterprises to define parameters and configurations for a system specific to their unique requirements

VeriSign® Identity Protection (VIP) Fraud Detection Service

Financial institutions, e-commerce sites, and other business organisations are becoming more sensitive to attacks against their infrastructure and how these attacks affect consumer confidence, their brand, and their bottom line. Consequently, they are increasingly interested in mitigating losses due to fraud, avoiding the bad press associated with consumer data breaches, and making their internal fraud analysts more effective. As an example, financial institutions in the United States are implementing measures to follow the Federal Financial Institutions Examination Council (FFIEC) guidance to use multi-factor authentication alongside user names and passwords for their online services.

VeriSign is addressing these consumer authentication challenges with VeriSign® Identity Protection (VIP)—one of the most comprehensive suites of identity protection and authentication services available, designed to help strengthen and protect consumers' digital identities. Delivered across a trusted, shared network, VIP helps manage reputational risk for financial services, e-commerce, and other enterprises that digitally interact with consumers' personal data.

At the core of VIP is the VeriSign® Identity Protection Fraud Detection Service. This solutions takes a proactive approach to fraud detection, using policies and pattern recognition technology to help detect both known and unknown attacks (zero-hour fraud) and adapt to each customer's usage habits. The system uses advanced anomaly detection technology, detecting fraudulent logins and transactions in real time without affecting a legitimate user's Web experience. Because the service actively learns about each user, it can adapt to both changes in legitimate behaviour and fraud attacks without manual intervention. This nonintrusive approach requires no change to a Web site and remains invisible to the consumer until anomalous activity is detected.

The many benefits of the VIP Fraud Detection Service include:

- Rapid deployment—works out of the box—with no integration required
- Little or no impact on users, unless fraud is detected
- Superior fraud detection through the use of both rules- and anomaly-based engines to prevent new fraud attacks and yield fewer false positives
- Automatically and quickly “learns” new user behaviour, minimising inconvenience to users
- The flexibility of unlimited parameters and configurations that permits customers to define systems specific to their unique requirements
- A comprehensive solution on one platform from one vendor—VeriSign, your partner in consumer authentication





+ VIP Fraud Detection Service: How It Works

The VIP Fraud Detection Service uses a unique behavioural engine in combination with a powerful business rules engine. Its servers and application components are deployed within an enterprise to use data that is readily available in that environment, and it can be installed in both passive and active configurations.

Passive Integration Mode

Because it comes preconfigured with the ability to read industry-standard Web and application server log files, the VIP Fraud Detection Service allows for a true zero-integration implementation. It automatically detects new entries to log files and reads only incremental changes, thereby allowing for high performance when reading from large transaction repositories. All VIP Fraud Detection Service functionality is available, including complete protection by both the behaviour and rules engines. Fraudulent transactions can generate real-time internal alerts—via email or SMS—that are available for instant viewing over the VIP Fraud Detection Service Web portal and online reports. This mode allows for a no-risk implementation while providing industry-leading fraud protection and aiding in regulatory compliance.

Active Integration Mode

The VIP Fraud Detection Service can also be implemented in an active mode, with enhanced bidirectional functionality. In this mode, transactions are sent in real time and the details of any suspicious transactions are immediately available to fraud analysts and customer service teams through the VIP Fraud Detection Service case management system. Support personnel can access that information when customers call about suspicious activity on their accounts, and analysts can use the information to proactively investigate instances of suspected fraud. Active integration also allows real-time intervention, so that users can be asked to provide additional information to validate their identities or transactions.

+ VIP Fraud Detection Service: Key Components

The VIP Fraud Detection Service uses a powerful rules engine in combination with a unique behavioural engine to help maximise fraud detection and minimise impact on users. The rules engine provides a blanket of protection and policy enforcement to all users, helping enterprises address known fraud risks and support business policies. The behavioural engine adds a final layer of protection that is automatically fine-tuned for each user, addressing unknown fraud attacks and eliminating unnecessary intervention. Any intervention that is necessary is provided in real time either with methods that are built into the service or with your own custom method.

Rules Engine

This powerful component of the VIP Fraud Detection Service comes preloaded with rules created by VeriSign experts to quickly identify many common patterns of fraudulent transactions. It allows companies to select from the predefined rules and create their own rules using an intuitive user interface. Additionally, VeriSign professional services can help businesses identify suspicious patterns unique to their environments and implement automated rules to find these patterns.



Behavioural Engine

The VIP Fraud Detection Service behavioural engine builds a model for each user that accurately scores whether or not new transactions fit that user's unique behaviour. While traditional solutions try to impose a one-size-fits-all approach, the VeriSign solution automatically generates a custom model for each user. This capability is crucial for applications with heterogeneous user bases, where there is no standardised user behaviour.

In order to lower false positives and still capture fraud, VIP Fraud Detection Service automatically adjusts the weight associated with each transaction parameter according to how important that parameter is for that specific user (e.g., a geolocation parameter will have much more weight for a user who does not travel than for a user who travels frequently). In essence, VIP Fraud Detection Service is capable of painting an accurate profile of each individual, focussing on the behaviour elements that define a user without getting distracted by other uncharacteristic traits.

The VIP Fraud Detection Service behavioural engine helps spot any anomalous activity, including new fraud attacks from non-blacklisted IP addresses (zero-hour fraud), without having to rely on invasive techniques, such as cookies, JavaScript, or ActiveX controls. Leveraging state-of-the-art clustering algorithms, VIP Fraud Detection Service uses the characteristics of user logins—Web browser type, IP address, time and date, account owner information, and other parameters—to build a profile of normal user behavior. When a login attempt doesn't match that user's normal patterns, perhaps because it is from a different computer, on a different day, or in a different country, the VIP Fraud Detection Service system flags the transaction as suspicious, even if the attempt does not trip any rules and comes from a non-blacklisted machine. Likewise, the VIP Fraud Detection Service can be used to monitor transactions like money transfers, payments, and anything else to determine if a specific transaction is anomalous when compared to that user's normal behaviour. The VIP Fraud Detection Service can even be used to monitor suspicious behaviour for other variables. For example, the VeriSign stock trading policy module analyses trades to see if they are normal for that particular stock.

Built-In Real-Time Intervention

The service bundles a choice of built-in and easy-to-deploy authentication methods to automatically challenge the user when a suspicious transaction is detected. This standard service allows for both in-band challenge/response questions as well as out-of-band verification via email, SMS text messages, and automated phone calls (fixed or mobile). The results of such challenges are then used by the system to eliminate future false positives for each user and to learn what fraudulent transaction patterns look like for sharing across the enterprise.



DATA SHEET

+ VIP Fraud Intelligence Network

This set of shared services in the VIP network builds on the VIP Fraud Detection Service and helps businesses obtain intelligence about online identity fraud events happening outside of their enterprise.

Criminals on the Internet use many different mechanisms to capture personal information—including phishing Web sites, using key loggers and false storefronts, and database theft. Often, criminals will try to use the same information on multiple Web sites, testing login information by trial and error, establishing multiple fraudulent accounts, and other malicious activities. In the offline world, because banks and credit card companies know that attackers will often reuse stolen identity information, they have established data-sharing consortia to identify fraudulent applications and account usage. The same approach can be used to stop identity theft and account fraud on the Internet.

The VeriSign® Identity Protection Fraud Intelligence Network leverages the unique knowledge of Internet threats that is gleaned from the global operation of core Internet technologies, as well as information gathered from other VeriSign partners. The VIP Fraud Intelligence Network will also leverage the emerging standards being developed in the Initiative for Open Authentication (OATH) to share transaction fraud or “thraud” information.

Why is VeriSign able to deliver this best-of-breed identity protection solution? With a proven track record operating the critical infrastructure for the Internet, VeriSign provides authentication services to more than 900,000 Web sites, over 93% of the Fortune 500, the world’s 40 largest banks, and 43 of the 50 biggest e-commerce sites.

+ Learn More

For more information about VeriSign Identity Protection, please call +61 3 9674 5500 or email: sales@verisign.com.au

+ About VeriSign

VeriSign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

Visit us at www.Verisign.com.au for more information.

