

## Verdasys sets out to reshape DLP as enterprise information protection

**Analyst:** Steve Coplan

**Verdasys** has seen the future for securing the flow of data, and it's called enterprise information protection (EIP). The company views EIP as the logical evolution of data loss prevention (DLP), to the extent that it builds on the technology components of data discovery, control and authorization. However, the concept entails a holistic approach focused on business process that extends beyond product or technology to iteratively align risk-based security management (with data the atomic component) and business performance.

### The 451 Take

The EIP push as both a defining security trend and vendor category is probably not unrelated to Verdasys' IPO aspirations. However, we see the concept as consistent with both emerging market requirements and a shift in security models, driven by risk management and the integration of functional silos – not least identity management and data protection. We also like the explicit statement of security as a process (and being the sum of technology, policy and operational practices). But this notion is intrinsically tied to business process modeling, a more flexible enforcement model (which Verdasys has begun to address through interaction with the user on specific actions) and interaction with multiple policy stores, which is still largely uncharted territory.

### Context

Verdasys was founded in 2003, and started out using the agent-based Digital Guardian product to provide rules-based encryption of enterprise data. A constellation of changes have ensued over the past year at the company, not least its stated intention to work toward an IPO in 2010, and the coalescence of product development, strategy and marketing around the concept of EIP.

The growth in absolute customer numbers, from 130 a year ago to 220 currently, is solid – particularly in the context of a market that has witnessed incumbent security management vendors entering via acquisition. But what is notable is that Verdasys' claimed annualized revenue growth of 200% is more than double that of the increase in customer numbers. This disparity suggests revenue is weighted toward business from existing customers, as opposed to new customer acquisition. Verdasys reports that repeat business follows a consistent pattern. The initial average sales price is in the region of \$350,000. But as enterprises either

increase the number of users and hosts or add modules, the scale of the commercial relationship grows in a step function, to about \$5m over the life of the account, Verdasys tells us.

On the management side, former international sales VP Omri Dotan has been appointed chief business officer, and Verdasys has bulked up sales and marketing. Headcount is currently at 150.

## Technology

While technology is clearly a foundational element of Verdasys' EIP, its approach integrates a set of methodologies and best practices to achieve two objectives. The first is to engineer a synthesis of enforcement and process, or, as Verdasys frames it, to enable a focus on business-value creation rather than on the threat posed by untrammelled data movement. The second objective is to build an extensible platform that can adequately address the current set of requirements driven primarily by compliance needs, and over time support a scalable, proactive security model centered on governance (and based on the data object as the foundational building block). This second objective is intimately tied to the notion that compliance, risk management and transactional security are iterative processes, as opposed to a single, monolithic technology implementation.

The strategic argument for this path is obvious – Verdasys is hoping to define an entirely new technology category that becomes central to security management (more below). But we believe that does reflect a sea change building in security models, precipitated by changes at the infrastructure tier and an associated higher rate of data movement to enable business processes.

The functional components of EIP consist of four elements: data discovery, classification and inventory; data-level access management; information usage management or authorization; and forensics and reporting (for compliance and risk management). The outcome of the application of the functional components is the ability to gain visibility into the characteristics of the data, define controls, authorize its use based on both context and classification results, and capture events for analysis, reporting and forensics. Verdasys harvests data from identity management infrastructure (**Microsoft** Active Directory and LDAP directories) to derive access control and entitlement logic.

The Verdasys' Digital Guardian product architecture is agent-based, but the company contends the distinction between agent-based and network-based is misleading. Instead, it believes that to encapsulate the components of the flow of data through discovery, activity characterization and acceptable destination-localized control and visibility is required. This is achieved through a library of agents – segmented broadly between corporate and remote agents. Corporate agents are in turn broken down into endpoint and server entities, providing authentication, discovery, classification and content inspection. Remote agents are broken down between endpoint and application agents, and provide authentication, anti-malware and session security.

## Strategy

The convergence of identity and access management and DLP – or, more prosaically speaking, data protection and access controls – is a significant trend framing our research agenda. This convergence is driven by the need for a unified policy statement or control construct that specifies who can touch what data when. In its most technically elegant construction, the two control mechanisms would be governed by an abstracted policy management layer that incorporates risk modeling. But what we are seeing in actual, commercial deployments could be described as policy concatenation, with DLP policies incorporating contingencies derived from identity management logic.

But the trend also throws a spotlight on some of the structural challenges that DLP still faces. Since a large chunk of enterprise data is unstructured or semi-structured, an automated mechanism is required to infer whether a data-access request is within policy. On the other hand, DLP products need some way to communicate with identity management directories to determine what access entitlements are associated with a set of credentials. This creates the need for a common (or shared) way to describe data that becomes more acute when it has to be classified on the fly and in real time.

Also, the quality of the controls directly correlates to the effectiveness of the enforcement. One approach to this challenge is to proliferate agents at both ends of the transaction and harvest as much access control and authorization logic from identity management infrastructure – as Verdasys has done. Over time, we expect to see several alternative models emerge across a broad spectrum from distributed policy decision points to centralized and colocated policy decision points and policy enforcement points.

The push to respond to these technical challenges comes not only from the crushing operational overhead entailed with compliance, the evolution of the threat environment and application devolving to the effective network perimeter. The push also emanates from the need to balance process and enforcement, and discover ways of architecting 'transactional security' that is independent of the infrastructure tier in order to facilitate continuous governance. As Verdasys appropriately points out, the need exists for a framework to manage risk to operations – as opposed to securing the transfer of data.

That's not to say security is a secondary consideration. Instead, the first phase of EIP in Verdasys' formulation is a profusion of use cases – from restricting data use based on ITAR and HIPAA regulations, to USB encryption, to secure, differentiated access to fileshares and collaboration platforms – that eventually coalesce around a set of organizing principles to manage the flow of data based on user identity, their role, the nature of the resource and the context of the transaction.

But there are also some pragmatic considerations. The DLP market, as broadly categorized, has undergone a period of consolidation that saw Verdasys' direct competitors being absorbed by larger security vendors, including **Symantec**, **McAfee**, **RSA** and **Trend Micro**. Daylight remains for independent vendors – either because they can better address a specific market segment or because their development resources are dedicated to a specific functionality set – but can they thrive? Verdasys reports impressive revenue growth, and penetration within enterprise accounts, but still needs net new customer acquisition to scale its revenue base. Partnerships are one option to expand sales channels and engage with

enterprises on security strategy, as opposed to tactical deployments driven by way of competing directly against vendors. Granted, **Vontu** is still sold by a dedicated sales force, and McAfee is still engaged with integrating multiple acquisitions.

Will the EIP pitch resonate? That depends largely on the quality of the relationships Verdasys builds in technology alliances (specifically identity management, content management and increasingly transaction and systems management), implementation and professional services. Ultimately, controls are ineffective if they are not data-specific and focused on a user and their role.

And while there are still challenges to securing data at rest, data in motion – particularly as the infrastructure itself is transformed via virtualization and cloud computing – presents operational challenges that impinge on efficiency. 'Encrypt everything and decrypt only when needed' addresses immediate compliance requirements, but is only peripherally related to business process modeling. However, to effectively map controls and discovery to business process, Verdasys will need some help. Some of those relationships are in place, including **Hewlett-Packard** and **IBM**, but relationships with systems integrators and professional services firms with expertise in change management will need to be more assiduously cultivated.

## Competition

In broad strokes, Verdasys' competitors can be lumped into three buckets: DLP products sold as part of a broader security management product portfolio; independent DLP vendors that are increasingly articulating similar marketing messages of context and content; and vendors focused on a specific functionality subset, such as encryption, data governance or port-based controls based on finger-printing.

**CA Inc**, via its acquisition of **Orchestria**, is probably in a category of its own. Although CA's security management portfolio is not as extensive as those of Symantec and McAfee, the company does have a significant enterprise presence and an extensive identity and access management installed base to leverage with its 'content and context' pitch for the integration of the Orchestria technology. We believe **Oracle** will also be moving in this direction, and specifically, mapping access control and authorization to business process modeling.

The DLP market (in its various permutations) experienced a period of consolidation over the last 18 months, with Symantec's acquisition of Vontu for \$340m in November probably the most significant transaction. Our understanding is that Symantec has retained a dedicated Vontu sales team, and remains a highly visible and successful competitor. RSA's DLP products primarily result from the late 2007 acquisition of **Tablus** with its network- and agent-based approach. McAfee has assembled its DLP product set from the acquisitions of **Onigma**, **Reconnex** and **SafeBoot**. **Websense**'s ability to classify content is derived from its **PortAuthority Technologies** acquisition, while **Provilla** provided Trend Micro with fingerprinting and DLP agents.

Although independent DLP vendors like **Code Green Networks** and **GTB Technologies** are still focused on improving their core functionality, vendors like **BitArmor Systems**,

**nexTier Networks** and **NextLabs** are articulating a similar marketing message to Verdasys. We expect the chorus will grow over time, and see RSA acting as an arms supplier through a DLP partnering strategy (with Microsoft only the first).

More pragmatically in the area of what Verdasys is calling enterprise adaptive encryption – which can also be described as intelligent or granular data encryption that can automatically make decisions about encrypting individual fields, records or entire databases – the company goes up against **GuardianEdge**, **Utimaco**, **PointSec** and RSA. In the area of email encryption, Verdasys goes up against **PGP Corp**, **Zix Corp**, **CA-Orchestria** and **Voltage Security**. We imagine that the full disk encryption beta that Verdasys has just completed is in part spurred by competitive dynamics.

### SWOT analysis

Strengths	Weaknesses
Verdasys has managed to entrench itself in a large number of high-end accounts and gained a reputation as a flexible, effective product.	Even as Verdasys articulates a high-level message, it is competing on the basis of tactical use cases. It may find its marketing is ahead of the market.
Opportunities	Threats
What is the addressable market for EIP? If Verdasys can get the strategy right, and manages to provide the framework for a security heartbeat for business processes, it is feasible to postulate that both the extent of the market and the depth of the relationship with enterprises will be exponentially larger.	While Verdasys may be setting the pace in the DLP arena, the idea that a single policy governing who gets access to what data, and how they can use it, is driving strategic deliberations at larger vendors. If these vendors can knit together the constituent parts more elegantly, and strengthen relationships with implementation partners, Verdasys will have a steeper hill to climb.

Reproduced by permission of The 451 Group; copyright 2009. This report was originally published within The 451 Group's Market Insight Service.

For additional information on The 451 Group or to apply for trial access, go to: [www.the451group.com](http://www.the451group.com)