



GUARDING AGAINST THE FUTURE

In the hunt for a comprehensive security solution that is capable of protecting valuable corporate information now and into the future, Verdasys has looked to an idea that has roots in the past in developing its Digital Guardian platform. Digital Guardian prevents data leakage or loss at the point of use across applications, devices, as well as channels of communication.

“It is literally the decades old idea of the reference monitor that is the conceptual model for Digital Guardian”, says Dan Geer, VP and Chief Scientist at software developer Verdasys. The basic idea is that wherever there is an interaction between humans and computers that changes a piece of data that is ‘at rest’ and places it ‘in motion’, that’s where you have to be prepared to intervene to protect it. CXO talked to Geer to find out more.

CXO. What kind of threats are companies now facing when trying to protect corporate data?

DG. Internal threats to information are increasing rapidly and are becoming more serious in nature. It’s also becoming much harder to define precisely what ‘inside’ is because it’s harder to tell what your information perimeter is. That means it’s now more difficult to determine where all your data is and how safe it is. Companies know they are exposed, for example when data is being shared and outsourced, but they don’t tend to have good mechanisms in place for keeping track of what that exposure is. What is becoming clear, however, is that the financial and reputation exposure of a company created by losing data are greater than they ever used to be.

CXO. Cryptography has become more popular to secure sensitive information but as technology advances, is this too becoming more flawed?

DG. Encryption has, and will always have, a place in information security. The real test, however, is whether cryptography solutions can ever be

made flexible enough to permit you to have cost effective collaboration among co-workers or with your supply chain and not adversely affect your existing business processes. Encryption key management is hard to control, particularly in cases where a person leaves a firm and you have to get rid of the keys, or if you want to share information with others but don’t want to share keys. Crypto is fabulous for the loss of a physical device. For example, if a laptop has a crypto file system as its core functionality and is stolen, the device effectively becomes a brick that might only have resale value for its hardware. As with most things, you have to look at what problem you are trying to solve. Don’t imagine cryptography as a panacea.

CXO. What are the most common mistakes companies make when trying to protect data at point of use?

DG. The wonderful thing about the computers, operating systems and applications you can buy these days is how easy it is to share and find data. But the fact that there are so many ways to move data – and this changes frequently – means that when there is a new threat it’s hard to close all the vectors at once, or protect data flow via all the possible combinations of

devices, channels and applications. However, you have to cover them all if you want your data to remain truly safe. For every identified problem there probably is a solution, but you should not confuse having a large menu of solutions with having a coherent overall data security strategy or you'll always be behind. Digital Guardian protects against threats to data across devices, channels and applications using a single product that gives you total visibility and the ability to audit data usage.

CXO. When collaborating on a global basis, what are the risks associated with being able to transfer sensitive and proprietary data outside the corporate network?

DG. With global collaboration involving the exchange of high value intellectual property, you have to consider the present value of losing it, the future value you might obtain for keeping control of it, and what it will expose you to if it disappears. If you contractually transfer IP to other global firms, it can travel through multiple hands over different jurisdictions that don't have fully harmonized data security laws. The key here is to maintain control over information you share with your supply chain partners, without slowing down the processes that collaboration was meant to accelerate. Using Digital Guardian means you can define which specific activities involving the use of intellectual property are permitted and which are not, without having to physically be there – copying a document, burning a CD, opening the application, cutting and pasting, etc. For example, if you want to stop people from sending out information such as a new product design specification by e-mail, or burning it onto a CD, you can just configure Digital Guardian to prevent this. Digital Guardian will stop the action from taking place even when it occurs in a foreign country and will send you an electronic alert and notification when it occurs.

CXO. Some companies are particularly uneasy about security when outsourcing. How do your solutions maximize security in this field?

DG. Many outsourcing operations handle significant volumes of extremely sensitive information. These could include insurance companies outsourcing their client health records, and financial institutions processing credit card applications, etc. With our solutions, you're in a position to stipulate exactly who can see sensitive information and what they can then do with it. We can, in effect, draw a virtual perimeter around the data by providing Digital Guardian oversight of this activity. You know exactly who has looked at that data and we can make sure it stays where you put it, even in a foreign country.

CXO. Compliance is a major issue. Is this requiring tougher security measures?

DG. Most of the regulations that people care about most these days relate to financial or health information. For example, one of our clients was told by their auditors that because of Sarbanes-Oxley they had to

have auditable separation of duties in place – the systems administrators must be prevented from being able to modify the financial data and vice versa to prevent fraud. With our solutions, you can see who has logged into the computer and prevent them from having access to certain parts of the file system without changing anything on the machine

(this includes a user with system administrator privileges). We can provide a complete audit trail of all activity which greatly enhances an organization's ability to answer questions during an audit. Another more complex example is a health insurance firm we work with. They have a call center in a foreign country that is operated by large systems integrator on a contract basis, but the database that supports this operation resides in the US, and the data centre there is owned by yet another third party. Given all the 'cooks in this kitchen', regulatory compliance (such as HIPAA regulations) threatens you with real penalties without a good security solution in place. Digital Guardian is one of the few solutions that can deal with this level of complexity without significant custom application development.



Dan Geer

"The cost effectiveness of most security solutions you can acquire today is limited because they aren't future proof"

CXO. Is it easy to integrate your data security solutions?

DG. From the very beginning, we built Digital Guardian with integration in mind. All of the software is written using Unicode, making it easy to modify language for localization purposes. The transport mechanisms we use to move data around are based on standards, such as http. The databases that contain the records we keep are based on industry standard products (Oracle and SQL Server). Our central console is accessible via a standard web browser. Our agents can be deployed centrally using Digital Guardian console (based on your network configuration employing AD or LDAP as standards), or using common provisioning products such as SMS, or Marimba. Our report format is provided to our customers so that they can access the information they contain to create custom reports, and for purposes such as integration into their other enterprise, or management applications. And our rules language is based on industry standard XML. We take standards very seriously at Verdasys, and we are committed to creating all of our products with standards in mind.

CXO. As technology advances, how do you see the emphasis on point of use data security changing in the future?

DG. The cost effectiveness of most security solutions you can acquire today is limited because they aren't future proof. The future will be vastly more data rich, and while the amount of data being handled continues to grow spectacularly, it is also becoming more mobile. The rate of advance of storage capacity and bandwidth for your money is growing extremely fast. It is impossible to buy a laptop these days with less than 10GB of storage and at a consumer level you can buy 300GB disk drives for less than a dollar per gigabyte (remember, one gigabyte is equal to roughly the equivalent of a pickup truck full of paper). The diseconomies will come from thinking 'every day there is a new threat so everyday I have to buy a new solution'. Digital Guardian is future-proof because it protects data at the point where humans and computers interact to solve the problem – at the point of use. It's the wisdom of our elders. ■