

The true meaning of global data security

■ By **Dan Geer**, VP and Chief Scientist, Verdasys

At Verdasys, we are staking our reputations on the idea that global data security is where the action is. By 'global' I mean location independent. By 'data' I mean any set of bits that have value. By 'security' I mean the absence of surprises.

A tool which location independently ensures zero surprises for any set of bits that have value will have important requirements and constraints. To meet a 'no surprises' constraint, your tool has to deal with malicious insiders and

malicious outsiders alike. With respect to insiders, your tool must be able to deal with human creativity without disrupting productivity. With respect to outsiders, your tool has to be future proof.

The digital world is a steady stream of nasty surprises: new pathogens, new weapons, new insights from some evil genius, new business models for crime. A tool that provides global data security has to be future-proof – it has to work in many possible futures and do so without inventor-grade skill on the part of the users. It cannot require repeated mid-course corrections or perpetual subscription.

Because human attackers are resourceful and digital pathogens mutate, recognizing on sight all the bad stuff anyone can think up is an unwinnable strategy, a strategy of hope; the dimensionality of attack is too great. Were this medicine, I'd be telling you that there may be 5000 diseases and a new one every few hours but all those diseases share the same half dozen symptoms, so you must focus on symptomatic relief and not try making antibiotics as fast as new diseases arise. Give up on causes and entry points. Give up on detecting pathogens. Give up on closing every hole in programs you didn't write. Give up on separating incompetence from

“We can all agree that the value of data is real and that the percentage of total corporate wealth that is data is rising. As such, the word data in global data security is about wealth preservation”



treachery. Focus instead on data security and a small number of effects from a large number of causes – if the effects can be blocked independently of their cause then you have an abstraction that works whether or not the user has a disease or just a mean streak therapeutically indistinguishable from a disease. The insider problem is severe enough. The outsider attack automation problem is severe enough. You are better off if you don't have to mount separate defenses for each.

Data

The second part of global data security is data. The unit cost of storage falls by half every 12 months, total stored information doubles every 30 months, and consumer devices from USB dongles to iPods to telephones, automobiles and cameras may differ in their IO but all are data-rich. As fast as data volume grows, data mobility grows faster still – doubling perhaps every nine months, not every 12. Though data grows in volume very fast, in the aggregate it will be more mobile tomorrow than it is today. A 1GB USB token needs no power of its own, is small enough to swallow and contains as much information as a full-size pickup truck filled with paper. As this is easy to explain, the market is full of purpose-built security tools for that particular risk vector.

“The data that matters is, of course, the data that has value. Echoing former Supreme Court Justice, Potter Stewart, I may have a hard time defining the value of data, but I know it when I see it. To precisely value data we have to choose between the cost of production, the present value of future revenue streams based upon it,

Losers are those whose data is either not in motion enough or in motion too much. If I walk out onto my hotel balcony I will walk right up to the rail and look over. If the balcony has no rail, I won't go near the edge though the facts are otherwise unchanged: the gravitational constant, how tall/sober I am, the altitude. With the railing, I use the whole of my balcony. Without the railing, I use less. With my eyes shut, I use my balcony once. The difference is the railing. Similarly with

some internet-age axiom, or even that their own information wants to be free. It is because they don't understand what a perimeter is in a world that has given up on physical borders. Your firm has a perimeter: it is exactly the reach of your control, no more, no less.

Call it entitlements, call it accountability, call it what you must, but if XYZ is not in your control then XYZ does not belong to you and it is not inside your perimeter. If you want to say that you control nothing, then feel

“Our data is always a few milliseconds away from being global and, in fact, we want our data to be global, but none too much”

data and security, without security you cannot put your data in motion or, if you do, pretty soon you'll be dead. With security, your data can be in much more motion and creating much more wealth. Our Digital Guardian solution, which prevents data leakage or loss at the point of use, is that balcony railing.

Global

The last consideration in the phrase global data security is global. Walk the floor of any trade show or leaf through any business journal and the word global will appear all the time. We live in globalized business, if not in globalized liberty. You and I can travel the entire globe at approximately the speed of sound and anyone older than our grandparents would find that astonishing enough. Our data moves faster and farther. When programmer Alan Cox said “In the new world order, Bombay is

free to say you have no perimeter. Otherwise, stop dodging. Global data security means deciding whether you want control or you don't. Saying ‘we have no perimeter’ is making a virtue out of failure. As the US Army Ranger Handbook says: ‘Two of the gravest general dangers to survival are the desire for comfort and a passive outlook’. I see that in almost every company I look at, though to be fair and gentle there are good people who say they have no perimeter because their desire to do better has been beaten out of them.

Here, then, is the punchline: global data security is not an option in exactly that sense that NASA's Gene Kranz said: “Failure is not an option”. More data more in motion is creating a Darwinian moment. Your strategy has to be global data security – global in the location irrelevant extension of your control, data as the wealth of nations and enterprises alike, and security in the avoidance of surprises as under Darwinian conditions death tends towards sudden surprise. Your company is virtualizing. It will soon be nothing so much as your global data security enables it to be. There is too much coming at you from too many directions to have a solution matched to every problem. I think that a reference monitor – a distributed, recording, non-tamper, host-based data surveillance agent – is just about the only economically viable answer to surprise-free, future-proof, data protection that does not get in the way of getting your job done. I'm wedded to this idea and for this reason my firm offers the embodiment of that idea in Digital Guardian. This is a competition of ideas that I believe is over. The competition of implementers can now proceed. We're ready. Bring it on. ■

“In an electronic world where data is both asset and coin, the winners are those who make the most use of their data, the ones whose data is most in motion”

the simple cost of replacement, the downside potential to which you would be exposed should that data be mislaid, and others. We can all agree that the value of data is real and that the percentage of total corporate wealth that is data is rising. As such, the word data in global data security is about wealth preservation.

Yet, it is not just wealth preservation, it is also wealth creation. In an electronic world where data is both asset and coin, the winners are those who make the most use of their data, the ones whose data is most in motion.

250ms from New York”, he was talking about bits not atoms, about data not you. Our data is always a few milliseconds away from being global and, in fact, we want our data to be global, but none too much.

As a long time consultant, I've had the privilege to help any number of firms in any number of fields to learn from them and to contrast them. When people say that their corporation has no perimeter they are half right. It is not because they have universal connectivity without universal access control or they have absorbed