100 percent catch rate for data leakage? You bet!

E

very now and then, I see an old work-
horse — and “old” could mean last
year in this business — dressed up in
fancy new clothes. When I see that old horse
looking better than its newer contemporaries
I really get enthusiastic. That’s the case with
the latest release of the Inspector from GTB.
It may be in its 12th release, but this baby, as
they say, sure can cook.

The GTB Inspector v.12, which I had the
privilege of reviewing as a late beta, claims a
100 percent catch rate for data leakage from
the enterprise, and it delivers. One caveat, of
course, is that a perfect catch rate depends
on having a blacklist of things to look for.
That list could be words, numbers, phrases
or protocols.

However, when I thought about having a
blacklist of, for example, key personal identi-
fiable information sitting in clear text on a
gateway in IT, it gave me the shivers. This is
not where you want to put the most sensitive
data in the organization. Not to worry, it
turns out. When you fingerprint that infor-
mation, all that the device saves is an MD5
hash of the data. Nothing else is on the
Inspector.

The GTB Inspector has several ways of
identifying sensitive data leaving your enter-
prise. Some are far more accurate than oth-
ers, but all are extremely competent. In addi-
tion to the fingerprinting, for example, the
device can spot data — such as credit card
numbers — and calculate whether the num-
ber is a genuine credit card or just a number
that looks like one.

The Inspector also can block certain types of
protocols, such as FTP or peer-to-peer. It can
catch email content, whether the user is using
a standard email program, such as MS
Exchange, or a web mail program, such as
Yahoo, Google (Gmail), etc. It comes with a
wealth of pre-written rules for various types of
data — such as the credit card calculator or
the social security number identifier. You can,
however, write your own, and all rules can be
refined as you use the product to reduce false
positives for non-fingerprinted data.

The amount of information available in the
reports is prodigious as well. There are full
details of sender and receivers (including
blind carbon copies), the type of content, and
the rule or policy that has been violated.
Time and date, of course, are there, too,
along with full email headers.

The device is able to decrypt SSL on the fly
and inspect the contents of data leaving
through an SSL tunnel or VPN. The security
event logs provide all of the data you ever
will need, and you can drill down to the
specifics of an alert.

The product is easy to set up and configure
and is well documented. Because the GTB
Inspector is an appliance, virtually all of the
basics are done for you. It took Mike
Stephenson, our lab manager, about 15 min-
utes to get the Inspector up and running and
ready for me to start poking around.

I took about an hour and a half virtual tour
with the folks from GTB — support for this
product is first rate — and by the end of that
time, I could set up, install, configure and
tune the product myself. They pointed out
that they had offered me nothing that isn’t in
the manuals and they were right.

However, if getting some support help to
implement your new Inspector is your cup of
teas, GTB will accommodate you with remote
installation, set-up and configuration at no
cost. If you want a GTB engineer on site, you
can have that too, but, predictably, there is a
cost involved.

At $30,000, plus $49.95 per computer over
200 computers, the product may seem pricey.
However, compared to other products of its
type with less capability, the Inspector is a
bargain. Consider the consequences of
extremely sensitive data being removed from
your network. The potential costs of that sort
of breach are sobering.

Administration, once the appliance is con-
figured and deployed is straightforward. The
logs and notifications can be sent to anyone
you wish which may include a security team,
the CISO, security analysts, IT staff, or
whomever. You can chose to send a notice
to the offender and his or her boss if you
wish. Actions include blocking, quarantining
and simply notifying. You can build your
own policies or use existing ones with or
without refinement.

The GTB Inspector v.12 is a hot device.
Protecting your organization from data
leaked from your enterprise is easy to do
and easy to manage. The accuracy and log-
ging will likely stand up in any related legal
action as “best evidence.” If you have sensi-
tive information on your enterprise, you need
this device — if for no other reason than that
you’ll sleep much better knowing your data
is protected.

We give this product our SC LabApproved
rating, the highest recognition we offer.

— Peter Stephenson, with Mike Stephenson