

# Real Test Plans for Real Results

By Mark S. Kadrach

---

**It's not good enough just to know when something works. You also need to know when, and under what conditions, will the product you've selected cease to function as the intended solution, and begin working against you?**

**I**t's not good enough just to know when something works. You also need to know when, and under what conditions, will the product you've selected cease to function as the intended solution, and begin working against you?

This is a great question that is usually only answered after the product has failed. The problem is that the failure mode isn't always obvious. It may be a deployment issue or it may be a usability issue. The problem isn't with the product. It's with the way the product was selected. If you make the assumption that smart people will make good decisions when presented with the right information, then the problem becomes one of supplying the right information. So why don't we get the right information? The following anecdote may help.

## Digging deep for information

Until very recently, I was part of a team that was responsible for security at a very large security product company. During the course of one of our status meetings, the fact that users wanted to use their smartphones to access corporate email came to light. Being the helpful group of security practitioners that we were, we naturally told them, no way. Actually, we told them *not right now*, but it sounded to them like no way. We tried to explain that before we said yes, we needed to have an answer on how to do what they wanted to do securely. After all, there were people out there who would dearly love to see what we were up to, and we weren't going to make it easy.

Realizing that we needed more information, our fearless leader pointed at one of the team members and said: "You must find a product that allows us to use our smartphones securely."

I saw real fear. Why? Because that person knew he was going to have to research the possible solutions, get candidate products in a lab, test them, and make a recommendation. A mistake in the recommendation, and he could be in worse shape than a congressional buddy of Jack Abramoff – in other words, professional toast.

---

**Realizing that we needed more information, our fearless leader pointed at one of the team members and said: "You must find a product that allows us to use our smartphones securely."**

---

He had a reason to be worried. The group was already gun-shy because they had made a recommendation on a database replication product that had been intended to address a security issue associated with direct access to the system. As it turned out, the solution was worse than the problem. The decision was made using very little real knowledge about the product or the company that produced it. The reason for this hasty decision: too much work to do, and not enough time to do it in.

My colleague realized that he and the group were once again facing a dreaded situation: They needed an accurate answer, but they lacked the resources to learn the truth of what ripple effects their decisions would create in their security infrastructures, as those plug

into the larger security system. They needed to know as much as they could about mobile security products in order to address the customer's need. And this meant more than knowing how a given product meets the authentication and privacy requirements. My colleague needed to dig to a whole new level of detail and answer a fundamental question: Is the product itself secure and stable in his environment? And does the company providing the solution understand how its product influences the overall security posture of his enterprise?

## Taking the time to test

I'm sure that if you ask a vendor those questions, they're going to say yes to both. In reality, they speak in generalizations and assumptions – testing and certifications and Evaluation Assurance Levels (EAL), the result of general assumptions that may cover some of the gross reliability evaluations. But as we all know from experience, the real test is in proving out the technologies in the lab.

---

**A test plan will sniff out where a new product can compromise your network, even if it's seemingly benign and not a security tool.**

---

A well designed and implemented test plan is a crucible for truth. It will tell you if the vendor's representatives were being truthful when they told you they had a documented systems development life cycle (SDLC), and that they have an active software assurance program. A test plan will sniff out where a new product can compromise your network, even if it's seemingly benign and not a security tool. It will tell you if the product is going to be a deployment nightmare and subsequently the best shelfware you've ever bought.

A well designed and implemented test plan will tell you when your candidate solutions are going to break. But the test plan can only do that if you have the resources to accurately implement it. Most organizations treat product testing as a side job that's done only when the day-to-day tasks are completed. This creates a lack of continuity. Not to mention that it takes forever to get the test done – if you tested again, would you even get the same results?

If you're like every other risk management professional, thinking about the answer to that question probably left you in some doubt. And these questions are only the beginning. Each set of questions peels back the layers of the onion to reveal another set of questions. And therein lies the problem. Getting the answers to these questions implies that you have the time and resources to devote to the process of hierarchical discovery and point-of-failure mapping.

## Producing the hard evidence

For this reason, we've put together a group of professionals dedicated to keeping the vendors honest. We'll do so through what we call military-grade destructive product testing. We examine the selected products in our lab and test them until they break. This is not a feature shootout, but an in-depth study of selected products and the vendors that provide them, not to exclude market viability or capability for product support.

Our knowledge base will allow us help our customers spend their security dollars more effectively. We will be able to do apples-to-oranges comparisons in a meaningful way. We do the heavy lifting and arm the decision-makers with relevant information.

Our program isn't an effort to tell vendors, "Ha, your product broke when we tested it!" It's an effort to understand the best product for a particular environment, and build an actionable library of reliable information that can be put to use to answer these questions. Our effort serves to foster the understanding that it is important to have a documented SDLC and a working software assurance program, as well as a functional product. In other words, just because the product works doesn't mean that it's the right product for the task at hand. And it definitely doesn't mean it's secure.

Over the next few issues of the *The ISSA Journal*, we will be sharing some of our findings distilled from our lab testing, threat environment and market intelligence. While we can't say what products we'll be examining, we will be asking some tough questions, and I'm sure we're going to get some interesting answers.

## About the Author

*Mark S. Kadrich is the President and CEO of The Security Consortium, a security product knowledge development company. The professionals he speaks of in the article are Rodney Thayer, VP Engineering, and Deb Radcliff, VP Research. Mark can be reached at markkadrich@thesecurityconsortium.net.*