

Bp.IPTM Checklist

The Out-of-the-Box Examination

Usage

This checklist is for use by anyone evaluating physical security system software or hardware products, especially a product intended for use on an Ethernet network. It can also be used by manufacturers to ensure that their products pass rather than fail an out-of-the-box examination.

Description

Enterprise IT departments need to have systems and equipment that can be deployed quickly and accurately, with minimal effort, and that can be operated at low cost and low risk of trouble. IT groups have personnel who are assigned the task of evaluating candidate technology to see how they comply with these general requirements.

The evaluation step is commonly referred to as the “out-of-the-box experience” or “out-of-the-box examination.” What does it take to unpack, connect and “fire up” the system or device? What kind of problems can be anticipated? What are the general characteristics of its network traffic? How accurate and complete is the documentation? The key question is: Will the product PASS or FAIL the *out-of-the-box examination*?

Background

Most security industry manufacturers, integrators and consultants are surprised to learn what can be validly concluded from the out-of-the-box experience. This checklist contains some basic evaluation points for networked appliances and devices. Physical security vendors and integrators, and their physical security practitioner customers, are generally not aware of the importance of these evaluation steps.

Such evaluations are typically performed against the background of the evaluator’s experience. The more experienced an evaluator is, the less forgiving the evaluator will be. The evaluator knows from hard experience that forgiveness is likely to result in pain and regret somewhere down the line.

Checklist: The Out-of-the-Box Examination

Some security vendors have said that it would be unfair to judge their products on the out-of-the-box experience, because they have thousands of products successfully deployed. But are they defining “success” in the same way that enterprise customers do? Seen through the customers’ eyes, the out-of-the-box examination plays an important and effective roll in high-production, low-cost IT departments.

Is it fair to judge the likely product deployment costs and efforts in large part on the out-of-the-box experience? We assert that it is fair, because it is not just the product that is being evaluated — it is the vendor as well, based on how well the vendor enables its customers to be successful with *low-effort deployments* and *cost-effective customer internal support*, starting from the point where the product is taken out of the box.

Checklist

The *Out-of-the-Box Examination* checklist starts with opening the box and ends with a brief evaluation. Many physical security technologists and security managers are surprised to learn what can be discerned from these steps. Most don’t have an extensive IT background and thus don’t have the insights that come from high-volume non-stop technology deployments.

For this reason the checklist is more than just a list of bullet items to consider. It contains descriptions of each step, along with possible results and conclusions. None of this material is intended to limit examinations or their findings and conclusions. It is intended to provide examples of forward-looking examination: based upon what you see or don’t see, what kind of deployment outcomes could result?

PASS or FAIL

There are two distinctly different situations in which the *Out-of-the-Box Examination* is done: competitive product evaluations, and single product evaluations. Obviously if there seems to be only one product that fits a particular need, not using the product is not an acceptable outcome for a FAIL EVALUATION finding. In a competitive evaluation, it is still possible for all products to have a FAIL EVALUATION finding, and of course deploying nothing is not the desired outcome.

In such cases the product wouldn’t be disqualified on the basis of the *Out-of-the-Box Examination* alone. After all, some considerations of worthiness put the product or products on the candidate list in the first place.

So instead of being immediately disqualified in such cases, a conditional qualification is appropriate: the product *MAY be acceptable based on the results of further testing*.

Checklist: The Out-of-the-Box Examination

In this circumstance, rather than ending the checklist work at the first FAIL point, the full checklist should be applied as much as possible, with findings noted.

The failure points would then serve as the basis of a request for additional information from the vendor, and if necessary could also be used in the engagement of an in-house or external specialist to help with Proof of Concept testing or Pilot testing.

The failure points will help you gauge the level of effort that will have to be applied to additional product evaluation steps. The failure points identify aspects of the product and of the vendor's support services that will require specific attention during those steps and possibly also during deployment if the vendor remains weak or poorly responsive on any points.

If in any evaluation you do fully disqualify a product, then for the sake of the vendor and its current and future customers please report the evaluation details to the vendor, so that the company can become aware of the issues it needs to address.

Submitting a Rant or Rave

In the case of a FAIL EVALUATION conclusion, do consider submitting a **Rant** to the Bp.IP Initiative, as that also sends a message to both the company and to existing and prospective customers about the situation.

When a vendor achieves a PASS EVALUATION according to your *Out-of-the-Box Examination* review, and you are very happy about the results of the examination, please consider submitting a **Rave** as the company deserves some public credit for doing things right.

This link is the starting point for submitting a Rant or Rave:

www.bpforip.com/read-rants-and-raves.html.

Checklist: The Out-of-the-Box Examination

EXAMINATION CHECKLIST (v1.0)		SOME FAVORABLE POSSIBILITIES		SOME UNFAVORABLE POSSIBILITIES	
Action	Steps	Results	Conclusions	Results	Conclusions
Open Box	<ul style="list-style-type: none"> Take out contents. 	<ul style="list-style-type: none"> Looks like the right stuff. 	<ul style="list-style-type: none"> PASS – continue evaluation Good so far. 	<ul style="list-style-type: none"> Wrong product. 	<ul style="list-style-type: none"> FAIL EVALUATION
Find Documentation	<ul style="list-style-type: none"> Is there a list of parts (separate or in installation guide) and pieces against which the contents can be checked? 	<ul style="list-style-type: none"> Identify all parts and verify contents complete. 	<ul style="list-style-type: none"> PASS – continue evaluation Contents complete. 	<ul style="list-style-type: none"> Can't verify contents as complete. 	<ul style="list-style-type: none"> Continue evaluation until a question can't be answered or another shortcoming is encountered. Then FAIL for poor product and packaging, due to high likelihood of excessive time required for support.
Identify Documentation	Look for paper and/or CD: <ul style="list-style-type: none"> installation guide user manual release notes disclosures data sheets application notes network hardening guidance tech support contact info 	<ul style="list-style-type: none"> All items are found and are a match for the product that has been provided for evaluation. 	<ul style="list-style-type: none"> PASS – continue evaluation All documentation is found and is correct for the product. 	<ul style="list-style-type: none"> Documentation is incomplete. 	<ul style="list-style-type: none"> Documentation is incomplete. If no tech support, no contact info – FAIL because there is no way to determine whether or not the evaluation can be completed. If tech support cannot be reached in reasonable time – FAIL EVALUATION as the evaluation will probably take too long, and support will probably be too troublesome.
Examine release notes	Check release notes for: <ul style="list-style-type: none"> sufficient history bug fixes known issues incompatibilities 	<ul style="list-style-type: none"> Able to identify 	<ul style="list-style-type: none"> PASS – continue evaluation Vendor has active maintenance processes and will be able to support a deployment. 	<ul style="list-style-type: none"> No release information available, old releases, mention of lock-in to legacy technology. 	<ul style="list-style-type: none"> FAIL EVALUATION Vendor shows insufficient evidence of maintenance processes and/or investment in the product

Checklist: The Out-of-the-Box Examination

EXAMINATION CHECKLIST (v1.0)		SOME FAVORABLE POSSIBILITIES		SOME UNFAVORABLE POSSIBILITIES	
Action	Steps	Results	Conclusions	Results	Conclusions
Check release note history	<p>Check for:</p> <ul style="list-style-type: none"> • things being fixed • things being upgraded and/or enhanced • notifications of compatibility with new devices • new features released (as opposed to all engineering efforts being captured by bug fixing, which would be a bad thing) 	<ul style="list-style-type: none"> • Able to confirm that technologies are being given appropriate attention • Buggy features are being corrected in a reasonable time frame. (Having a product WITH A SOLID BUG REPAIR HISTORY is a GOOD THING rather than a bad thing.) 	<ul style="list-style-type: none"> • PASS – continue evaluation • When bugs are found the vendor is likely to make a good effort to correct them. • The product keeps advancing with beneficial new features, regardless of how many or few bugs are found. • Workarounds are quickly provided for newly-discovered product security vulnerabilities • Vulnerabilities are fixed in a reasonable time frame. 	<ul style="list-style-type: none"> • Lack of release history or other technical data indicates poor support habits on the part of the vendor supply chain. • Releases once or twice a year only, timed just before major trade shows, and which contain <u>mostly</u> new product features and <u>few if any</u> but corrections, indicates a lower level of true product support than is desirable. 	<ul style="list-style-type: none"> • “BAD MARKS” go to this vendor - can’t trust the vendor to “be there” if we had to call with a problem; can’t expect a timely resolution. • FAIL if any more “bad marks” accumulate.
Check release note bug fixes	<ul style="list-style-type: none"> • Check the bug fix lists for each release against online discussion forums, as a means of verifying that fixes are done in a timely manner, and that no serious unhandled bugs are known. 	<ul style="list-style-type: none"> • Bug fixes match complaints in forums and discussions, and look to be fixed in a timely manner. • Details are available on the vendor’s website. 	<ul style="list-style-type: none"> • PASS – continue evaluation • Vendor seems to be responsive and responsible in addressing and reporting bug fixes. 	<ul style="list-style-type: none"> • Few or no bug fixes reported, and forums contain serious complaints that span multiple releases. • Track record on the web of vendor belligerence towards bug reporters generally indicates a lack of commitment to delivering technically solid products. 	<ul style="list-style-type: none"> • FAIL EVALUATION • Vendor releases products without sufficient testing (i.e. uses customers as guinea pigs), and is not responsive enough in addressing problems. • Product will be troublesome to utilize and may fail critically at some point in time.

Checklist: The Out-of-the-Box Examination

EXAMINATION CHECKLIST (v1.0)		SOME FAVORABLE POSSIBILITIES		SOME UNFAVORABLE POSSIBILITIES	
Action	Steps	Results	Conclusions	Results	Conclusions
<p>Check release note known issues</p>	<ul style="list-style-type: none"> Check the documentation and vendor website for workarounds for the known issues. 	<ul style="list-style-type: none"> Workarounds are published at least for critical issues. Forums report that the workarounds are satisfactory. Workarounds seem feasible for those vulnerabilities that apply to your deployment. 	<ul style="list-style-type: none"> PASS – continue evaluation Vendor seems to be responsibly reporting issues and actively providing workarounds. A track record of dialog on resolving issues shows it's worth working with the vendor if there are limitations, or if compensating controls or workflow modifications are required. 	<ul style="list-style-type: none"> Critical known issues have no workarounds in vendor documentation or in online forums. YouTube has videos of how to compromise product and there are no published workarounds. 	<ul style="list-style-type: none"> FAIL EVALUATION Vendor releases products without sufficient testing (i.e. uses customers as guinea pigs), and is not responsive enough in addressing problems. Product will be troublesome to utilize and may fail critically at some point.
<p>Check release note incompatibilities or for vendor-supplied documentation on known compatible products (in sufficient detail)</p>	<ul style="list-style-type: none"> Check the list of incompatible items against the security department's technology roadmap, IT and security department standards, and the lists of installed products in that category. If such information doesn't exist, provide the security technologists with the list of incompatible products and have them respond as to whether or not there is a conflict with existing or planned equipment deployments. 	<p>(A) Incompatible items ARE NOT FOUND in existing or planned deployments</p> <p>—OR—</p> <p>(B) Incompatible items ARE FOUND in existing deployments but can easily be replaced per cost/benefit analysis.</p>	<ul style="list-style-type: none"> PASS – continue evaluation for either condition below (A) Give vendor "GOOD MARKS" for listing incompatibilities. (B) If no Incompatibilities are listed, check online forums for incompatibilities, and check with vendor tech support. If no incompatibilities with existing deployed technology are known to exist, Give vendor "GOOD MARKS" for high compatibility. 	<ul style="list-style-type: none"> Known incompatible products are found in existing or planned deployments, and cannot or will not be changed out. <p>—OR—</p> <ul style="list-style-type: none"> Major incompatibilities with existing deployed technology are found to exist and are not documented by Vendor. 	<ul style="list-style-type: none"> FAIL EVALUATION Incompatibilities cannot be feasibly dealt with and are not acceptable.

Checklist: The Out-of-the-Box Examination

EXAMINATION CHECKLIST (v1.0)		SOME FAVORABLE POSSIBILITIES		SOME UNFAVORABLE POSSIBILITIES	
Action	Steps	Results	Conclusions	Results	Conclusions
Check documentation	<ul style="list-style-type: none"> • Confirm the documentation for the specific product configuration as specified is identifiable and check it for usability and validity. 	<p>Able to find necessary information:</p> <ul style="list-style-type: none"> • How to set up • How to harden • How to reset to factory defaults • How to enable/confirm use of required features • How to integrate with an enterprise network infrastructure 	<ul style="list-style-type: none"> • Documentation appears sufficient to support evaluation/confirmation of vendor delivered features, deployment, and integration with ongoing operations 	<ul style="list-style-type: none"> • Multiple gaps in documentation when compared with state of the art enterprise infrastructure deployments; • Explicit feedback from vendor support contains undocumented items • Clearly visible error messages that are totally undocumented 	<ul style="list-style-type: none"> • FAIL EVALUATION • Insufficient or no documentation will make deployment risky, difficult and/or expensive, and will make operations difficult and/or unreliable.
Check “getting started” guidance	<ul style="list-style-type: none"> • Check to confirm information is sufficient to perform a brief evaluation to evaluate the product. 	<ul style="list-style-type: none"> • Information provided through some appropriate channel (might be text file, might be online website, might be a YouTube video, might be tech sales rep explaining how they’ll install it in front of you with narration...) 	<ul style="list-style-type: none"> • Product is likely to meet requirements, so that is sufficient to merit technical validation exercise • Sufficient information is present to develop a sound evaluation plan 	<ul style="list-style-type: none"> • Vendor has never heard of a ‘getting started’ guide; no demo is available; no online information can be found; additional vendor-proprietary equipment (connectors, power supplies, special cables, etc. not provided) required to perform an evaluation. 	<ul style="list-style-type: none"> • FAIL EVALUATION • Vendor sales process limits or prevents customer access to known technical limitations in order to close the deal • Support is likely to be poor • Engineering is likely to be underfunded/shoddy and unresponsive to customer needs. • Deploying this product would likely be a significant technical risk.

Checklist: The Out-of-the-Box Examination

EXAMINATION CHECKLIST (v1.0)		SOME FAVORABLE POSSIBILITIES		SOME UNFAVORABLE POSSIBILITIES	
Action	Steps	Results	Conclusions	Results	Conclusions
Evaluate Product	<ul style="list-style-type: none"> • Perform brief (one week, in an office lab environment) set-up and exercising of product • Evaluate product itself • Evaluate and document (for later reference during deployment) its impact on the network 	<ul style="list-style-type: none"> • The product can be deployed without excessive vendor support being required • The demonstration provides sufficient technical detail to assure deployment and operations teams of the product's viability • Substantial technical validation via live exercises produces data to back up customer management buying decision process 	<ul style="list-style-type: none"> • PASS EVALUATION • Usable technical results support the project team's product selection process. • No serious issues with network traffic or behavior on the network. 	<ul style="list-style-type: none"> • Product does not work, product has bugs, product hard to use, and evidence contra-indicating the product fits the desired use cases. Causes unacceptable network problems. 	<ul style="list-style-type: none"> • FAIL - Product not appropriate for deployment in the intended use cases.