



ICSA Labs Product Assurance Report

A study conducted by the Verizon RISK Team

Table of Contents

Introduction	2
Methodology	2
• Testing and Certification	
• Data Collection	
Looking Back: 20 Years in the Security Industry	4
Product Testing Results	6
• Frequency of Criteria Violations	
• Common Types of Violations	
• Factors Contributing to Violations	
Conclusions and Recommendations	18
• Recommendations to Vendors	
• Recommendations to Users	

Authors

- Wade Baker
- George Japak
- Charles D Hylender

Contributors

- Peter Tippett, MD, Ph.D.
- Jon McCown
- Dave Archer
- Brian Monkman
- Kevin Brown
- Thang Phan
- David DeSanto
- Leo Pluswick
- Sam Glesner
- Al Potter
- Darren Hartmen
- Guy Snyder
- Andy Hayter
- Jack Walsh
- David Koconis
- Greg Wasson

Introduction

Are the security products your organization depends upon every day reliable? Do they consistently meet expectations and live up to their billing? Chances are they do not. This experience has resulted in the not-so-tongue-and-cheek postulation that new security products are created to compensate for the shortcomings and side effects of the existing ones. That's not to say there is never a legitimate need for new security solutions; new business models, new technologies, new threats, and new levels of global interconnectedness require us to continually adapt the products and practices we employ to protect information assets.

Unfortunately, the market's solutions to all this newness are not always as legitimate as the need. Product quality is often left behind in the rush to be latest and greatest. New is distorted with innovative bigger touted as better, and promises frequently exceed performance. Thus, the work of helping to distinguish fact from fiction is critical.

In response to this challenge, ICSA Labs formed in 1989 with the goal of providing credible, independent, third-party assurance for computer and network security products. Since then, ICSA Labs has worked with hundreds of the world's top developers and industry experts to create and apply objective testing criteria for measuring product performance and reliability. We believe we have contributed to the improvement and maturity of the industry over the last two decades by facilitating collaboration, fostering accountability, and increasing user confidence.

Two decades of certification testing has afforded ICSA Labs a great deal of experience and knowledge about common weaknesses in security products. Testing products before they hit the shelves provides insight into what is prone to happen once they leave them. We've learned what improves reliability and what tends to detract from it. We've seen first hand how often problems occur, what types occur most often, and why they occur. We've also seen how vendors respond to these issues and how their actions can affect consumers for better or for worse.

This report is an effort to distill observations from the ICSA testing labs along with others from the security product industry over the last 20 years. It is the first step in a larger agenda at ICSA Labs to expand information sharing and collaboration with the security community. Future work will provide additional product-specific findings as well as more detailed analysis. We hope readers find these efforts helpful in their mission to protect information assets and useful to the decisions and deployments made in support of that mission.

Methodology

There are three key components to ICSA Labs' core business: consortia operations, research and intelligence, and product testing and certification. This report is most directly related to the latter but is very much a product of the first two as well. As such, this methodology section covers ICSA Labs' testing and certification model and the data collection process used for this report. Information on consortia operations and other research activities can be found on our website (www.icsalabs.com).

Testing and Certification

ICSA Labs is probably best known for providing vendor-neutral testing and certification for hundreds of security products. While certification cannot eliminate risk and is not a guarantee of product performance, it can substantially reduce risk by ensuring that products meet objective criteria, thereby increasing security, trust, and usability.

Certification Criteria

The ICSA Labs certification is based on public, objective criteria that yield a pass-fail result. The criteria—drawn from expertise across the industry—are clearly defined and address common threats and vulnerabilities for each product. Meeting the criteria is possible with current technology and typical “know-how” so that the certified product can be truly effective within the community of users. Furthermore, the criteria are applicable among products of like kind and can therefore be used for better understanding, comparing, and assessing security products.

When developing certification criteria, ICSA Labs queries numerous experts, specialists, organizations, user enterprises, developers, academia and other industry groups. In addition, ICSA Labs reviews various regulatory requirements (HIPAA, PCI DSS, etc), and where applicable, includes these requirements within the established testing criteria. Once accepted, criteria do not remain stagnant. A continuous process of updating criteria and test cases is a fundamental aspect of ICSA Labs certification. This effectively “raises the bar” to drive product quality up over the long term.

Testing and Certification Process

After a contract is signed, the product is delivered to ICSA Labs where it is deployed in the lab and tested against the current criteria. Great care is taken to ensure that the testing environment and procedures model the real world. Once a testing phase is complete, the vendor is notified of any criteria violations or issues. A criteria violation indicates that the product did not pass one or more test cases defined in the criteria. Certification requires that all test cases be successfully met. The analyst identifies all violations and explains the test cases in sufficient detail for the vendor to reproduce the results. Vendors then work to address violations and resubmit the product to ICSA Labs for testing. This process continues until certification is attained (or retained), until the vendor withdraws the product from testing, or until the boundaries of the testing contract are exceeded.

The product remains continuously deployed in the testing lab throughout the length of the contract. Each testing program re-tests certified products at different frequencies, but for the most part, products are tested at least annually. In the Anti-Virus and Anti-Spam testing programs, products are tested much more frequently (monthly and daily respectively). In addition to the regular test schedule, products are available for on-demand testing on a 24/7 basis.

Stakeholders

There are two primary stakeholders with respect to ICSA Labs certification: vendors and users. Vendors are the developers and/or owners of a product in the certification program. They are ICSA Labs’ customers. Users include both home consumers and enterprises that purchase and deploy ICSA Labs certified products. This report speaks to both groups.

Data Collection

The scope and span of time represented by this data set are daunting. Collecting nearly two decades of testing results across hundreds of products is non-trivial. Products and vendors emerge and disappear, split and merge, evolve and even devolve. Testing criteria undergo numerous iterations and transformations.

Even the technology used to store and access test data has seen substantial change. We certainly cannot make the claim that a single, consistent data collection method was employed across all products throughout the timeframe of this study. In the case of some of the newer programs, a simple database query would provide the desired data. Data records for some of the earliest programs are available only on paper forms. In addition to going through these records, we conducted multiple rounds of interviews with program managers and testing leads over a period of several months.

We also examined documents, service contracts, and e-mail messages about testing programs and the history of ICSA Labs. Collectively, these diverse data sources form the basis for the results discussed in this report.

In the end, we identified seven certification programs for which data could be reasonably collected in sufficient quantity and quality to allow for valid conclusions. These programs are listed in Table 1. For those desiring more information, ICSA Labs publishes descriptions, certification criteria, and testing results for these (and other) programs on our website (www.icsalabs.com) along with other relevant information.

Program	Established
Anti-Virus (AV)	1991
Network Firewall	1995
Web Application Firewall (WAF)	2006
Intrusion Prevention System (IPS)	2005
Internet Protocol Security (IPSec)	1998
Secure Sockets Layer (SSL)	2003
Custom Testing Services	2004

Table 1. ICSA Labs certification programs included in this report

In the sections that follow, we report quantitative statistics whenever possible. For many points of interest, however, hard data are not available; in such instances, we provide observations and commentary that we hope are insightful and useful.

Looking Back: 20 Years in the Security Industry

The last two decades in the information security industry have been a relentless process of change. Twenty years ago, antivirus software, now a fundamental technology in any corporate security program, was still in its infancy. Network firewalls hadn't been born yet; large-scale corporate networks were still far from common. With no HTML¹ there was no WWW², and without that, of course, no need for SSL or WAFs. One can imagine how much lighter the official security lexicon of the time was before its pages were filled with all the other terms and acronyms from the last 20 years. Back then, many of the industry heavyweights so familiar to us now weren't even a gleam of hope in a venture capitalist's eye.

Through this period, ICSA Labs has helped to define, test, and certify many of the major security products you use and rely upon every day. This vantage point has enabled ICSA Labs to observe overarching industry trends as well as developments on the ground with specific products. Although we've witnessed countless changes, a few stand out as particularly relevant to the security market and the products that comprise it. These broader trends are presented below, while more detailed findings based upon certification testing in our labs over the last 20 years follow in the remaining sections.

Information security emerged as a distinct industry

Information security is not a new concept. Nor is the field of information security as it applies to computers and IT. The notion that information is a valuable asset and the desire to secure it have been around for as long as mankind has had information worth protecting.

However, the security industry as we know it today, with strong ties to the Web, e-commerce, and elaborate corporate networks, is a rather new development. Amid escalating concerns over privacy and the protection of information

¹Hypertext Markup Language

²World Wide Web

assets, the field outgrew its origins as a niche of IT and developed into an industry of its own. As this budding industry emerged, so too did the number of dedicated security companies and products in the marketplace. Universities followed suit to fill the need and began offering specialized degree programs in information security. Though far from a reversal of this trend, there has been movement in the opposite direction of late with the acquisition of several security firms by broader IT companies.

Products evolved toward greater complexity and functionality

Twenty years ago, the few dedicated security products that existed were point solutions with a singular goal and function. Then things started to change. Computing devices became faster, smaller, and more mobile. The use, users, and users of IT grew exponentially. Networks interlaced the planet. Business became ever more techno-dependent. Threats evolved rapidly to exploit this new climate and security vendors were forced to keep up or shut down. Keeping up often meant pushing new features into the marketplace as quickly as possible.

In the late 1980s, for instance, anti-virus (AV) needed only concern itself with a few viruses. As viruses transitioned to malcode and then to malware, and as their prevalence and virulence skyrocketed, AV products necessarily broadened in scope. AV spread from the desktop to servers to gateways to clouds and were required to monitor media, networks, e-mail, browsing habits, and more. Recently, even this broadened species of AV is seen as too narrow in function. Holistic security suites that bundle AV with personal firewalls, anti-spyware, anti-phishing, browsing control, and other functionality are ever more common.

This evolutionary swelling exhibited by AV and other security products isn't necessarily a bad thing; if multiple functions can be performed as well as one, most IT administrators would consider that a benefit. On the other hand, the relationship between security and complexity has a dubious past and will undoubtedly present challenges into the future.

Maturity was born of greater standardization and accountability

When ICSA Labs set up shop in 1989, it soon realized that the security industry bore more than a passing resemblance to the Wild West. It was (and still is, in many ways) largely unregulated. Few laws or standards existed and it was difficult to distinguish between snake oil and legitimate solutions. One vendor's definition of what a product was supposed to do did not always match another vendor's interpretation of the same type of product. Furthermore, performance claims often went untested. The user was lost, uncertain if a product could really deliver on its claims and was largely on their own when trying to determine how best to use the hardware or software.

This created an obvious need for greater standardization and accountability. Various working groups, standards bodies, third-party testing entities, and regulatory agencies rose to the call. Though not perfect, the situation has improved over time and the industry has matured. Users have certainly benefited from this maturation process but so has everyone involved—and the Information Security field is better for it.

The industry exhibits both convergent and emergent tendencies

History has shown that consolidation is the natural progression of a maturing industry. What begins with rapid growth and the emergence of many players vying for advantage eventually gives way to a fewer number of large players in it for the long haul. Where is the security industry along this sequence of events? It is difficult to tell. Established and dominant veterans are present yet new players take the field with regularity. Mergers and acquisitions seem ever more commonplace, yet innovation is still in the air and new technologies continue to emerge. Competition within certain product lines is high and profits margins tight yet regulation remains fairly loose and the door for entrepreneurship is open. This is perhaps to be expected as the security product market is still—when seen holistically—if not in its infancy, then certainly in its youth.

Lest the reader think that AV developers have had an easy time of it, a bit of perspective might be in order. When the Anti-Virus testing program was first launched there were only about a half dozen vendors who desired to participate. At the time, (the early 90's) there were no more than a few hundred known viruses that were actually impacting systems. To get started, ICSA Labs requested that each of the participating vendors send in the top 50 viruses that they saw in the wild, in order that those viruses could then be aggregated with ones submitted by the other vendors as a means to develop a test set.

The goal for the successful completion of round one was simple: the vendors were required to detect 80% of the viruses on the aggregated list. The almost unanimous vendor response was that this test would be much too easy to be of value. No problem, ICSA Labs stated that they would increase the detection rate to 90% of all listed viruses. The vendors agreed with this scenario, but many felt that the test still lacked teeth and was simply a hurdle to jump through. Once the first round of testing was complete the results were a dose of reality—100% of the AV products failed the testing.

The criteria had to be scaled back in order for any of the vendors to attain certification. Over time, the program again increased the frequency of the testing along with the number of samples. Today there are thousands of samples used in the test sets and the numbers increase almost daily. In addition, vendors must now attain 100% detection for malware in the wild³ and are tested monthly. This story perfectly illustrates a common theme that has emerged over the years of ICSA Labs history. Namely, vendors are often overconfident. They believe their products will fly through testing, and then are dismayed to learn how many issues are left to fix. That so many eventually do pass points to the effectiveness of established criteria, accountability and testing.

Independent security products are a dying breed

The last century has seen a shift from isolated, “vertical” enterprises to highly collaborative “horizontal” networks of partners, suppliers, vendors, and customers. There is good reason for this: A well-run supply chain benefits all members and results in a superior product at a lower price to the consumer.

Not surprisingly, the security industry has mirrored this trend and it is increasingly rare that a single vendor is responsible for all aspects of a product from design to post-implementation support. Whether this is a problem is often unclear and largely depends on those involved and the collaboration between them. What is clear is that when there is a problem, it is often “someone else’s problem.” Understanding the ramifications of these trends and learning to manage them effectively will confront practitioners and policy-makers in the industry for years to come.

Product Testing Results

While the previous section highlighted some of the overarching trends in the security product market, this section provides results and insights directly from our testing labs. These results are presented under three main headings:

1. Frequency of Criteria Violations
2. Common Types of Violations
3. Factors Contributing to Violations

Although the focus here is on failures encountered during product testing, it is not the purpose or desire of ICSA Labs to fail products. We want them to pass, because we want them to work. It’s our purpose to continuously improve the quality of security products used by organizations around the world. We believe that problems discovered in the Labs are problems that won’t be discovered in an operational environment (or worse, by a malicious entity). In this sense, the failures we identify under testing conditions should be viewed as successes for both the product vendor and the user.

Frequency of Criteria Violations

No one ever said creating quality products was easy. Of course, that doesn’t mean they can’t be substantially improved either. So, how often do violations occur during ICSA Labs certification testing? In short: almost always.

It is unlikely that anyone’s worldview will be radically altered if we claim that years of product testing at ICSA Labs upholds the old adage that “Nothing is perfect.”

³“In the wild” refers to malware that has spread in the real world as opposed to, for example, proof-of-concept code that never actually infected systems.

As Table 2 plainly shows, it is extremely rare that a product attains certification in its first round of testing with no criteria violations. This was true in the early days of ICSA Labs and it is true today. With the exception of Anti-Virus, there is no substantive difference with regard to this finding across the testing programs. Some products exhibit major criteria violations, others relatively minor. Some have numerous deficiencies, others only a few.

After the almost invariable first failure, most vendors attempt to make corrections and resubmit products for further testing. On average, 82% of products deployed eventually achieve ICSA Labs certification. While it might be obvious, it is worth making a distinction here. 82% does not refer to all products in existence; it refers only to those submitted to ICSA Labs for testing. For some programs this includes nearly all products in that market, but for others it represents the minority.

It should not be assumed from this seemingly high success rate that faulty products are given a free pass or that the bar is progressively lowered until everyone easily steps over and attains certification. In fact, the bar is routinely and systematically raised. Some vendors spend significant amounts of time, effort, and resources to improve their products in pursuit of the ICSA Labs certification. Some attempt to negotiate their way around difficult requirements or even fight back against them. It is not unusual that meeting all criteria requires numerous attempts over several years but products typically attain certification within 2 to 4 testing cycles.

The results in Table 2 are remarkably consistent across programs except for a few outliers that are worth explanation. First, while only 27% of Anti-Virus products achieve certification on the first attempt, this program is still considerably higher than the others listed. This is largely due to the comparably mature state of the AV industry and the age of the certification program. Some AV vendors have developed ICSA Labs-certified products for quite some time. The effect of this experience is evident when the first-cycle certification rate is split according to how long vendors have been in an ICSA Labs program. For products submitted by veteran AV vendors, this figure grows to roughly 35% while new vendors hover around the 5% mark. As in life, age and experience clearly make a difference in the world of product assurance.

	All Programs	Anti-Virus	Network Firewall	Web App Firewall	Network IPS	IPSec VPN	SSL VPN	Custom Testing
Percentage of products that attain certification in the first cycle of testing	4%	27%	2%	0%	0%	0%	0%	0%
Percentage of products that eventually attain certification	82%	92%	86%	100%	29%	90%	91%	87%
Number of testing cycles typically required before products attain certification	Typically 2-4 cycles							

Table 2. ICSA labs certification programs included in this report (percentage of products)

Second, that only 29% of Network IPS products ever attain certification is attributable to several factors. Unlike AV, IPS is one of the newer programs at ICSA Labs and a more recent technology as well. It is also a complex technology with difficult testing requirements, making certification a challenging process. When the program began, the majority of IPS vendors participated but many soon dropped out (although some continued to try without success for two years) because they were unable to meet the rigorous set of test cases. Typically they left with the promise of returning when their product was better prepared to pass the criteria. Unfortunately for users, these products continued to be sold (sans ICSA Labs certification) in the interim. Although some kept their promise, most of these vendors never returned and the market share of the IPS program has fluctuated around the 30% mark over the last few years.

Once a product passes, it's common for the vendor to have difficulty maintaining the certification. A few data points relevant to this topic can be found in Table 3. As explained previously, ongoing testing after a product attains certification is foundational to the ICSA Labs testing methodology. Inevitably, such testing results in a currently certified product exhibiting criteria violations. If not resolved, this will result in the product losing its certified status. There are several reasons for this including: changes in threats, changes in the criteria and/or test cases, changes in the product itself, or even changes in the vendor's desire for certification. These are discussed throughout the remainder of this section.

	All Programs	Anti-Virus	Network Firewall	Web App Firewall	Network IPS	IPSec VPN	SSL VPN	Custom Testing
Percentage of products that exhibit violations during post-certification testing	36%	30%	18%	50%	93%	24%	27%	11%
Percentage of products that lose certification	13%	13%	3%	20%	43%	6%	9%	0%

Table 3. Results for post-certification testing (percentage of products)

Changes in Threats

A constantly evolving threatscape is a frustrating but enduring characteristic of the information security field and it certainly affects the products and tools used in that profession. At ICSA Labs, test cases are updated to more accurately reflect current threats over time. For some programs this occurs almost continually and for others on a more as-needed or periodic basis. This is especially challenging for products like AV and IPS that are required to recognize current attack signatures or patterns. After struggling unsuccessfully and in danger of losing certification, some vendors have admitted they were unprepared to update their products so frequently and thus dropped out of the program. Interestingly, we have observed regional factors in play here as well. For instance, Asian AV vendors historically have difficulty obtaining a complete "wildlist" of malware for development and testing purposes and also struggle with polymorphic analysis.

ICSA Labs frequently conducts what are internally referred to as fire drills. If an exploit or weakness is discovered with one product that may affect other similar products, tests are conducted to determine the extent of the problem. Because so many products utilize the same core code base, it is not at all unusual to find a number of them affected by the same issue. When these situations arise, all affected products enter the remediation cycle described above. Though fire drills are not necessarily initiated by new threats or exploits (i.e., could be a general functionality problem), such is often the case.

Changes in Criteria

In addition to keeping pace with current threats, products must also handle periodic changes to ICSA Labs' testing criteria. Criteria changes occur less often than updates to test cases (the latter have more to do with current threats) but are by no means static. The intent is to drive the quality and rigor of testing up over time as well as to improve or extend the capabilities of the product. Therefore, a product that meets criteria version 1.0 may not pass the next scheduled test, regression test, or spot check using version 2.0—even if the product itself did not change at all in the interim. Many vendors find this moving target difficult to hit and, as a result, criteria violations usually spike immediately after criteria changes.

In the mid 1990s, a small IT vendor approached ICSA Labs to certify their new firewall product. After the usual rounds of attempt, fail, and try again they eventually attained certification. They remained certified for several years, but eventually withdrew from the program stating budgetary concerns as the primary reason. Approximately two years later they contacted ICSA Labs and expressed a desire to re-enter the program. They would soon release a new version of their firewall and felt that the ICSA Labs logo would help lend it credibility in the marketplace.

By policy, vendors (or products) returning to an ICSA Labs program receive no special treatment; they enter the standard testing process as if they had never been previously certified. In this case, both the product version and the criteria changed during its absence from the certification program.

The vendor signed the new contract and submitted their firewall with full confidence that their new (very similar) product would breeze through testing with little effort this time around. This confidence proved unfounded as testing yielded dozens of criteria violations. Company executives were astounded by this outcome but, to their credit, made the decision to address all outstanding issues and eventually regained certification (which, as a side note, required more cycles than the initial submission).

Changes in the Product

Anyone familiar with technology products of any kind knows that they do not remain static. Old features are improved, new features added, and the product changes from version to version over its lifetime. Security products are no different. Because these iterative changes can affect performance against certification criteria, ICSA Labs retests certified products at specified intervals. In addition, regression tests and spot checks are often conducted following significant product changes or fixes.

In some cases, criteria violations following product changes are almost predictable based on historical precedents. For instance, when new functionality is added to a product, it is very likely that it will exhibit at least a few violations. Another, perhaps less expected but well-substantiated trend is that previously addressed criteria violations are prone to resurface during later testing cycles. In other words, the fixes applied to version 1.0 of a product are not carried forward to version 2.0. Reasons for this are many but may include a rewrite of code not involved in the first fix, the loss of key personnel, interdepartmental miscommunication within the vendor, or simply an oversight in the versioning or updating process. Whatever the reason, it occurs with surprising regularity in products across the board.

Changes in the Vendor

On occasion, a vendor will voluntarily choose to pull their product from an ICSA Labs certification program. This may occur before certification is attained but also happens afterward, during which time the vendor must continue to work to maintain certification. We've heard many justifications for this over the last 20 years but reasons typically relate to either the outright difficulty of maintaining certification or resource constraints (or a mixture of both).

The first reason is simple; maintaining certification over the long run proves too difficult for some products. This may be due to challenges inherent to the technology itself or inadequate development and quality assurance capabilities within the vendor. The IPS program provides examples of both. No more than 4 vendors have been certified at any one time and there is a lot of rollover (one will be decertified and another certified and so forth). Some IPS vendors passed the rigors of certification but later decided to leave the program when unable to keep their products performing at levels required to pass subsequent testing.

The other group of reasons offered by vendors choosing to exit an ICSA Labs program is business related in nature. Some vendors run out of budget while some have the money but feel it could be spent better elsewhere. Others want the ICSA Labs logo for the initial product launch but do not want to allocate the resources required to maintain it. In one rather amusing example, a vendor used the portion of their marketing budget tagged for certification to instead hire “booth babes” at conferences throughout the year. They probably succeeded in giving away a lot of swag but in the process gave up product quality and their certification as well (the vendor re-entered the program a year later after losing market share to competitors but could not pass certification).

One common example where both technological and financial priorities are in play involves products nearing end of life. Vendors often desire to pull them from certification and concentrate on developing, certifying, and maintaining new and more current products. From the vendor’s viewpoint, this is understandable. As discussed above, maintaining a single product through changes in threat, criteria, and product versions is challenging—even more so for multiple products in varying stages of their lifecycle. From the user’s viewpoint, however, this is not as attractive a proposal. Products are typically serviced beyond their shelf life and remain in use long after that. Ensuring quality (whether accomplished via ICSA Labs certification or some other means) should have an eye toward the end user.

Based on our experience, it is not a question of whether a product will have a problem attaining and maintaining certification, but how the vendor responds to issues that arise. While criteria violations are virtually inevitable, failure is certainly not. Whether with difficulty or with ease, vendors that persevere and make full use of the ICSA Labs testing program have a demonstrably more reliable product in the end.

Common Types of Violations

Having discussed how often criteria violations occur during product testing at ICSA Labs, we now turn attention to the various types of violations observed by our analysts. Every certification program has its own testing criteria and procedures (and thus its own violations), but certain classes of deficiencies are endemic regardless of product category. These are listed briefly in Table 4 and expounded throughout the rest of this section.

	All Programs	Anti-Malware	Network Firewall	Web App Firewall	Network IPS	IPSec VPN	SSL VPN	Custom Testing
Core functionality	78%	85%	98%	100%	100%	64%	36%	60%
Logging	58%	11%	97%	80%	57%	8%	82%	73%
Product security	44%	3%	65%	50%	93%	12%	64%	20%
Documentation	41%	NT ⁴	24%	30%	14%	5%	91%	83%
Default Setup	30%	21%	9%	60%	NT ⁴	NT ⁴	NT ⁴	NT ⁴
Interoperability & Compatibility	23%	NT ⁴	3%	NT ⁴	14%	64%	9%	NT ⁴
Revisions & patching	21%	43%	17%	10%	21%	16%	18%	NT ⁴
Administration	16%	4%	20%	40%	7%	NT ⁴	NT ⁴	7%
Persistence	8%	NT ⁴	9%	10%	NT ⁴	NT ⁴	0%	5%

Table 4. Common types of criteria violations (percentage of products)

⁴NT stand for not tested.

Core Functionality

According to our results, a product is more likely to be deficient in performing its primary security function than any other class of criteria violation. Core functionality, of course, represents something different for each type of product. For Anti-Virus, it means preventing infection. For firewalls and IPS, it's filtering malicious traffic. Though the context differs, the conclusion is the same: many products don't (adequately) do whatever it is they were made to do.

This finding admittedly has much to do with the focus of testing. While certification criteria address functionality, they are largely defined around functions central to the product's purpose. It makes sense, therefore, that testing would often uncover these core deficiencies. That it occurs so often among products that have already passed in-house QA and are considered by the vendor to be ready for release is a bit more unexpected—and perhaps even unsettling. Surely most users would like to think they can rely on a security product to adequately perform its basic purpose.

With regard to core functionality, the results in Table 4 warrant a little more explanation. While we do come across products that are wholly unable to perform functions basic to their kind, it is more often the case that products cannot perform them under certain conditions and/or handle even small variations from "normal." For instance, we commonly see firewalls brought to their knees by malformed packets or very trivial single-source denial of service attacks at less than T1 speeds. Firewalls, IPS, and AV products are prone to pass packets (or files) that violate security policy when under increased load. Many products perform admirably in certain network traffic conditions but degrade sharply with mixed or real traffic.

Another class of problems related to core functionality can only be described as unexpected consequences from seemingly normal actions, conditions, or settings. Every product in an ICSA Labs certification program undergoes standard testing as defined by the criteria, but non-standard tests are also performed when possible—especially for ways the product is likely to be used. For instance, we found that when http scanning was turned off in one AV product, it quit scanning other protocols as well though they were still active. Malcode passed through completely undetected. An all-in-one printer/scanner/copier/fax machine tested as part of a Custom Testing engagement was not supposed to process documents labeled confidential. It worked fine if documents were oriented properly on the scanner bed but, on a whim, the analyst turned the document 90 degrees and tried again. The document was scanned and faxed as though nothing was amiss. Similar things happen quite often and, of course, are reported to the vendor along with any other standard criteria violations. Vendors aren't excited about these unexpected problems but they are relieved because they represent vectors that would almost certainly be discovered and exploited through normal use after release.

Logging

Logging receives a greater share of testing in some programs than others but it is addressed to at least some extent within the criteria of each program. Most of these tests check to make sure the device consistently and correctly records some variation of "who did what and when?". As seen in Table 4, logging capabilities are often found to be deficient across most programs.

The logging problems observed in our labs mostly fall within three categories: the product does not log at all, it logs but incompletely, or it logs inaccurately. Incompletely can refer to a failure to log all relevant events (i.e., only 8 of 10 events are logged) or logging only part of the data elements required on a single event (i.e., capturing the "what" but not the "when"). As the name implies, a device that logs inaccurately may capture all the right entries and elements but these records cannot be used because the information they contain is wrong. Incorrect date and time stamps are a particularly common example of this.

In 1998, ICSA Labs began researching and soon launched a program to test Intrusion Detection Systems (IDS). The program ran for several years until a shift occurred within the industry away from detection alone to real-time prevention (the reasons behind this shift are a story unto themselves). Previous IDS vendors began promoting IPS instead and ICSA Labs discontinued IDS testing and began incorporating lessons learned into a new program to certify IPS.

Based on input from enterprise users and product developers, ICSA Labs built the network IPS testing program to reflect real world conditions as much as possible. While some testing labs settled for artificial network traffic from commercial traffic generation tools, ICSA Labs was researching what a suitable mix of legitimate business traffic ought to be. The answer was simple in theory but less so in application. Why not use actual traffic from a typical enterprise network? After modifying over 40% of the code from an open source tool, ICSA Labs was soon able to replay once live traffic through devices at rates up to at least 10Gbps. While building the infrastructure to replay realistic traffic in the background, ICSA Labs also conducted extensive research to determine which exploits should be run in the foreground. Here again, analysts opted for real, working exploits to test the effectiveness of IPS.

One of the unexpected, initial dilemmas for the new IPS program involved throughput. At issue was the fact that tested devices were performing at 40-60% less than what they advertised in their marketing material. Many IPS posted dramatically different numbers in relatively homogenous simulated network traffic than in our mixed traffic taken from actual networks. Though ICSA Labs provided members with histograms of the legitimate network traffic that included detailed protocol breakdowns, most could not significantly

- Continued on next page -

Historically, logging is a weakness of any kind of firewall product; almost every network or web application firewall tested at ICSA Labs has at least one logging violation. Logging is relatively new to the certification criteria for IPSec (and so not much historical data exist) but is a frequent cause of violations within the SSL VPN program. This mostly involves not logging the right information. Within the IPS program, logging issues usually manifest themselves in the form of reporting deficiencies.

Another interesting observation with respect to logging violations is that they can be particularly difficult to fix. Quite often, an adequate solution requires a total reengineering of the product. This has a lot to do with the product architecture (i.e., whether logging is handled by the firewall engine or not) and seems to be getting worse as hardware sophistication, throughput requirements, and reliance on third-party software increase.

The widespread nature of logging violations is made more distressing when overlaid with findings from the Verizon Business Data Breach Investigations Report. The report makes it plain that the only time many organizations learn they lack the right information is after something has gone wrong. Though logs usually contain some evidence of an incident, investigators often find critical information to be missing or incomplete. The view held by many (vendors and users) that logging is a nuisance and something merely done to “put a check in the box” surely contributes to the inability of organizations to detect and respond to incidents in a timely manner.

Product Security

Do security products have security problems? According to our test results, over 40% of them do indeed. Security issues exposed in testing range from vulnerabilities that compromise the confidentiality or integrity of the system to seemingly random behavior that affects availability.

One of the more ironic examples we’ve ever come across was a web application firewall that turned up numerous vulnerabilities within its web administration interface. Cross-site scripting, SQL injection, and buffer overflow vulnerabilities and unencrypted admin interfaces are some of the common security issues identified within the Custom Testing engagements, Web Application Firewalls, and Network Firewalls programs. Vulnerability testing is not a major component of the AV program but they are sometimes found nonetheless. AV products, especially the all-in-one varieties, do struggle with performance and stability problems that negatively impact the integrity and/or availability

improve their performance numbers. This finding exposed several important things about IPS devices at the time.

First, there is no standard set of network traffic to use when determining IPS throughput and no standard method to create that mix. As a result, developers often test differently when they produce throughput numbers for their marketing materials. Second, there are a number of factors that strongly affect achieved throughput including the policy being enforced on the device and the properties of the traffic used in testing (e.g., the mix of protocols, the average frame size, etc.). Finally, because of this disparity, users should be cautious when comparing published throughput values and evaluating how IPS products will affect their networks.

of the system on which they're running. Many of the security troubles for SSL VPNs can be traced to the OpenSSL toolkit (which roughly 80% of them use). In these instances, codefixes are hard, usually requiring a major release. By comparison, IPSec VPNs tested have significantly fewer security violations.

Documentation

It may seem odd that certification criteria address documentation but its importance has plenty of historical precedent. Plato, for instance, recognized this and called for anyone leaving behind a written manual to make sure it was accurate and understandable⁵. Unfortunately, many vendors today give little import to product documentation. Sometimes the problem is with quantity (too little documentation), other times it's quality (unhelpful and/or misleading), or even currency (doesn't match the current product version). Either way, poor documentation is at best unhelpful and at times, dangerously misleading.

Because ICSA Labs configures and tests so many products, our analysts spend more time trying to figure out instructions than the average IT staffer. It would be difficult to tally the number of late nights, frustrated outbursts, and grey hairs attributed to documentation over the last 20 years but Table 4 can at least attest to its frequent occurrence. Though frustrating in the lab, the real danger from poor documentation is when it results in deployment mistakes and misconfigurations that erode enterprise security.

Documentation violations arise more often in newer products (regrettably a period of time in which accuracy would be most helpful). This accounts for the high percentage in Table 4 for the Custom Testing program, which regularly tests newer technologies. As products mature and features stabilize, so too does the accompanying documentation. We also see documentation problems vary based on product type. For instance, though prevailing opinion holds that SSL VPNs are easier to implement than IPSec, we find that SSL products consistently fail documentation quality tests, while IPSec VPNs have few issues.

The main issue behind documentation problems seems to be one of prioritization. Documentation is sometimes written in a rush at the last minute by people who know little about the product. We find that the writers and product designers often work in different locations and never talk. Sometimes the documentation was obviously written by someone in marketing who was more concerned with declaring the wonders of the product than imparting technical know-how.

⁵"...Then anyone who leaves behind him a written manual, and likewise anyone who receives it, in the belief that such writing will be clear and certain, must be exceedingly simple-minded..." – Plato, Phaedrus.

Default Setup

This class of violations is somewhat hard to define. In all cases, it relates to certain expectations that must be met regarding a product's "out of the box" state to satisfy testing requirements. From Table 4 it is apparent that many programs do not test for default setup violations but in those that do there is a decent chance that a product's default state is problematic for one reason or another.

A product may enable features by default that it should not or omit those it should. For instance, firewalls are expected to prevent the traversal of traffic during startup and disable unwanted remote administrative services by default but not all do. Though not part of an ICSA Labs certification program, the experience of Verizon Business' Investigative Response team with wireless LAN products highlights the effect default setups can have. Over the last five years WLAN intrusions have fallen substantially due in part to security settings like encryption and password change requests being enabled out of the box. The importance of such initial settings should not be overlooked; it is better for a product to be overly restrictive initially than come pre-loaded with security holes of which the user is unaware.

Interoperability & Compatibility

Interoperability and compatibility refers to a product's ability to work (without major conflict) with other devices in a system. For firewalls, ICSA Labs testing in this area makes sure the device handles traffic without disrupting the network and that it can communicate properly with other devices. An example of compatibility issues observed in IPS products occurs between the sensor and the management device. In the SSL VPN program, tests focus mainly on web browser issues since there is no interoperability between different vendors' products. For IPsec VPNs, however, interoperability testing is absolutely essential and virtually synonymous with their core functionality.

Interoperability, or the lack thereof, was the primary motivation for developing an IPsec certification program at ICSA Labs. With the complexity and ambiguity of the standards, accomplishing interoperability among different products was extremely difficult for developers. Over the years, the technology matured and the situation improved somewhat. However, true interoperability continues to be problematic, requiring extensive testing beyond just session establishment and re-keying to uncover deficiencies.

Revisions & Patching

In a previous section, we touched on the product versioning difficulties observed in our labs. This class of criteria violation is certainly related but focuses more on minor updates and patches deployed between major versions while the product remains operational. Approximately 20% of products across all programs struggle to consistently fold in revisions of one kind or another.

For some products, the ability to do this effectively is as important as its core functionality. Imagine AV software that could not adequately incorporate new virus definitions; it would soon become almost useless. IPS are equally dependent on a steady flow of new vulnerabilities and attack signatures. All products require occasional firmware updates, software patches, etc. These revisions and patches are critical to the long-term viability of the product and ensuring they are handled properly is an important aspect of certification testing at ICSA Labs.

Administration

Security products can be hard enough to properly configure without faulty administrative controls. Oddly enough, many programs do not have specific criteria regarding product administration but deficiencies usually become obvious during the setup and testing process. At times, it's a very rough and non-intuitive user interface. Sometimes irritating compatibility issues arise such as a web panel that works with Internet Explorer but not Firefox. It really

It is often said that ‘necessity is the mother of invention’, and this adage certainly holds true in the development of new technology. In many instances, a new invention owes its birth to a combination of seemingly unrelated factors that come together at a given point in time. Such was the case when a complex set of circumstances, inter-related needs, and burgeoning technology resulted in the creation of our IPSec certification program.

In early 1997, the Automotive Industry Action Group (AIAG), which then consisted of a number of major car manufacturers, was trying to establish a network of VPNs that would work among their trading partners, suppliers, and car dealers. The network needed to ensure identity authentication, data integrity, non-repudiation, and confidentiality. At the same time, the IETF (Internet Engineering Task Force) through cooperation with ICSA Labs and other consortia members, was attempting to nail down a new protocol called IPSec, which was concerned with those very same characteristics. As a consequence, the AIAG and its partners installed IPSec gateways based on this protocol to make up their VPN network. However, because the protocol was new and because suppliers all bought products from different vendors, they were overwhelmed with interoperability problems. While searching for a solution to their problems, the AIAG approached ICSA Labs and invited employees to participate in the brainstorming sessions. The result of these meetings was the IPSec testing program.

The IPSec program worked closely with the AIAG to develop a set of testing criteria based on the IETF protocols that would deliver an ever-changing list of interoperable products to the AIAG members. The AIAG members required their VPN product suppliers to have ICSA Labs certification so they could be assured that their VPN product would work with those

- Continued on next page -

becomes a problem when changes are made but do not actually take effect or are reset once the administrative session is terminated.

Administrative capabilities are interrelated with product documentation. Sometimes it is difficult to tell whether the documentation is right and the configuration interface wrong or vice versa. As with documentation, administration-related violations peak early in a product’s lifecycle and settle out as it matures. For instance, when web application firewalls first came on the market, no one really knew how to configure them properly and the user interfaces were awkward and hard to understand. As people became proficient with the technology (and companies worked on the UI), the configuration became more intuitive and reliance on documentation decreased.

Persistence

There are many things in the security world we take for granted that we probably shouldn’t. Conversely, there are some things for which we should simply be able to “set it and forget it.” The ability of a product to preserve settings through unexpected events is one of those things.

Persistence problems can be serious in operational conditions. We know of several real-world instances in which a device lost power and allowed intruders into corporate networks after rebooting without security settings. Of course, not all persistence violations are so dire. In addition to lost configurations, lab testing finds unintended password resets, time stamp inaccuracies, lost data, and a myriad of other issues.

Factors Contributing to Violations

To now, we have covered the frequency and types of criteria violations but only indirectly touched on the reasons why they exist. Such is the purpose of this brief section. It is different from the previous two sections in that statistical results are not presented. We simply cannot measure how often or strongly any given factor contributes to deficiencies but we can be relatively certain about the factors themselves. Several factors identified over the years as significantly contributing to the tendency of a product to exhibit problems during certification testing are highlighted below.

of their networking partners. These partners also required the products they bought to be ICSA Labs' certified. Ultimately, the ANX (automotive network exchange) was born, and quickly became the world's largest extranet connecting 40,000 trading partners with IPsec VPNs. Although the ANX continues and the IPsec program still flourishes, the project with ICSA Labs proved to be only an initial success.

Due to the fragile nature of interoperability, it was crucial to test and certify products on a version-by-version basis regardless of the vendor. In other words, just because Vendor A has a certified version of a product on the list it doesn't mean that all Vendor A's products will interoperate. Only the version tested against the criteria and proven to work is a viable option. Unfortunately, the ANX was constantly pressured to grant waivers of certification when a member wanted a certain brand of product for some other business reason. When partners and suppliers purchased newer untested versions of a product or purchased from non-certified vendors, the control broke down. Over time the in-flux of non-certified (and therefore non-interoperable) products caused the partnership to erode. Nevertheless, the exercise proved that large-scale interoperability by the extended enterprise was not only possible, but fiscally feasible.

Product Maturity

We've already mentioned the profound effect a product's age or level of maturity can have on many variables related to its performance and reliability. In our experience, the rule of thumb is that newer products—especially newer technologies—have more problems than established ones. Over time, the kinks are worked out and the difference fades. We realize this is intuitive but it is worth confirming nonetheless.

Product Functionality

Another major reason behind criteria violations is the inherent technological difficulty of the product's functions. While some products are over-engineered and introduce unnecessary complexity, oftentimes the mission requires it. Not everything has a simple solution. Here the rule of thumb is that quality-related problems increase with product difficulty and complexity. This too is intuitive.

Vendor Experience

The longer a vendor participates in an ICSA Labs certification program, the better they fare. It's tempting to chalk this up as a self-fulfilling prophecy but that is not the truth of it. While it is true that veteran vendors come to know the process and better understand what's necessary to meet requirements, there's more to it than that. Many also make greater use of the program by working closely with analysts, leveraging criteria for development, accessing research, and participating in consortia—and their products are better off for it.

Vendor Resources

As you can imagine, developing a technology product and bringing it to market requires a substantial investment of time, people, money, and other assets. No organization has unlimited resources, and so choices must be made about how best to allocate them. At times, it is apparent that a product is severely hampered by resource constraints. It may be empty coffers, inadequate knowledge, or staff shortage. Perhaps it's a decision to divert resources to a new product. We've seen it all and more. The simple lesson is that vendors with sufficient resources make more successful products.

Vendor Backroom

Related to but distinct from the resources factor are a vendor's backroom product development and quality assurance operations. Even unlimited resources are no guarantee that a vendor is ready, able, and willing to support a product throughout its lifecycle. Vendors possessing robust and mature backroom capabilities attain certification more quickly and maintain it with far less difficulty. Needless to say, this is a distinct advantage.

Vendor Size

Company size appears influential but is not a one-sided factor. Larger vendors tend to have more resources and experience, both pluses for products in a certification program. They also have the advantage of greater stability through turbulent times and can exert more influence within the industry. On the other hand, smaller vendors are usually more cohesive and responsive. It's often much easier to find the right person(s) when something needs fixing and they are free and motivated to get it done quickly. On the whole though, both large and small organizations have successful histories with ICSA Labs.

Vendor Politics

We at ICSA Labs are not unrealistic; we know that product certification is not the single, all-important vision that unites the organization around a common purpose. Of course, that's a far cry from the corporate infighting, conflicting agendas, red tape, and communication problems we commonly see negatively affecting a product's performance in our testing programs. It's a hard factor to diagnose, but when vendor politics (in their negative sense) are less outwardly visible, products boast a better track record.

Vendor Champion

We've seen far more long-term success when the development side of the house drives a company's certification program participation. The technical staff is generally more interested in doing it right than in acquiring a logo sticker to slap on the outside of the box. On the other hand, many companies pay for the testing via their marketing budgets. When marketing groups and front offices are in charge, they sometimes aren't as focused on dealing with issues that arise inevitably in testing. In either case, the certification process moves more quickly and smoothly when there is a highly motivated champion inside the vendor organization.

Standards participation

Working with standards bodies and other industry organizations is another positive factor for product quality. Those who participate in such groups typically enjoy a higher level of performance in testing. That's no surprise: Technology held to an industry standard improves in both feature set and in reliability. Participation in standards bodies such as IETF typically means that the product is ahead of the curve.

3rd Party Dependencies

The effect 3rd parties can have on product quality is profound. At times, a product benefits greatly from 3rd party components, development, services, etc. However, it is often clear that a product is so fragmented by 3rd party dependencies that it is severely crippled. We have identified deficiencies in a product and reported them to the vendor only to find out that nobody there knows how fix it. If the developer is aware of which 3rd party is responsible for that piece (honestly—sometimes they don't), they may find that the 3rd party has gone out of business,

may no longer offer support, may have lost key staff, or any number of other circumstances that delay or preclude the fix. These issues are widespread and the effects are always evident.

Conclusions and Recommendations

Why does product certification matter? How does it affect my organization? ICSA Labs has heard these questions repeatedly over the years and we expect to hear them for years to come. We hope such questions are, in part, answered by the findings presented throughout this report. At the very least, we hope to have left the impression that certification is not an unthinking, meaningless, purchased, or guaranteed stamp of approval. Vendors bearing the ICSA Labs logo have earned their stripes.

To conclude this report, we would like to make some recommendations to our stakeholders, product vendors and product users. To the suspicious reader, they might sound self-serving, and perhaps they are. But there is a difference between disingenuous self-promotion and relaying credible evidence that supports one's position. What follows are observations and inferences drawn without duplicity from the data collected in our labs and discussed within this report.

Recommendations to Vendors

Most of this report deals with vendor-related issues. Therefore, our recommendations to vendors here are fairly succinct and straightforward: pursue certification as a means of verifying and improving product quality and make use of the findings contained in this report. The information presented herein is a distillation of lessons learned through countless hours testing products, identifying problems, and chasing down solutions. We've discussed common pitfalls to avoid, recurring types of deficiencies of which to be wary, and factors that contribute to success. We hope this information is a help to your product development and management activities. In our experience, most vendors who attain ICSA Labs certification and make use of the associated benefits find it to be well worth the effort.

Recommendations to Users

We have established that all is not as it seems in the world of security products. However, enterprise buyers are not totally without direction when navigating their way through purchase and deployment decisions. Certification not only provides assurance to users of a product but to evaluators as well. Product testing results on our website (www.icsalabs.com), this report, and other ICSA Labs research can serve as trustworthy guides in the decision-making process. We offer the following recommendations as well.

- Use certified products. We say this without apology; products consistently held to a standard are shown to be more reliable. You know what you're getting. Untested products are more likely to have problems "under the hood" which can cause problems that will become evident down the road.
- The market typically demands features over quality. Quality might be expected but that's not the same as demanded. When the market demands quality, vendors will supply it (and features too). You can help drive the demand.
- When selecting products, start with a list of those certified and compare based on features, price, and whatever else matters to you after that.
- The certification criteria are a further means of evaluating products. We frequently field calls from users asking about certified products, the criteria, how we test against them, etc. We don't mind.

- Be suspicious of performance claims and numbers. Vet them as much as possible. If critical to your decision, ask about the conditions and circumstances in which they were measured. Do they match your environment? If not, your mileage may vary.
- New products are likely to have more problems. Unless the need is justified, it might be best to let it mature for a time. If you must buy early, certification is even more critical.
- When functionality is similar among products that suit your needs, opt for simplicity over complexity.
- Prefer vendors that participate in ICSA Labs consortia, standards bodies, and other industry organizations. Our results show participation pays good dividends.
- Research a vendor's backroom operations and quality assurance processes. Excellence here bodes well for the lasting reliability of their products.
- Prefer vendors with a history of products certified in an ICSA Labs program. A lengthy and good track record is a positive sign.
- Vendor size does not appear to be—in and of itself—a decisive factor for product selection. It may be important in combination with other criteria. For instance, if you want maximum assurance that a vendor that will be around in ten years to support a product, then you may prefer a larger, more established vendor.
- When using a certified product, check periodically to make sure certification is current. If a product loses certification, ask the vendor why. The answer may significantly affect the security of your organization.
- Push vendors to maintain product certification even after end-of-life. If you still use it, quality assurance is important.
- Expect the unexpected. Products sometimes exhibit problems that seem unrelated to their function. Try to anticipate them and account for them.
- If security products don't always work as billed and deficiencies commonly arise, it suggests the familiar concept of defense in depth is important. Overlapping controls can cover a multitude of sins.

At the end of the day, certification is not a guarantee of perfect security or flawless functionality. It means a product has been systematically tested against a set of objective, pre-defined criteria. One may find fault with the criteria but one should consider the alternative of having none. Based on our experience, the record on that is not good...and 20 years is quite a long record.



About ICSA Labs

ICSA Labs offers vendor-neutral testing and certification of security products. Many of the world's top security vendors submit their products for testing and certification at ICSA Labs. Businesses rely on ICSA Labs to authoritatively set and apply objective testing and certification criteria for measuring product compliance and reliability. The organization tests products in key technology categories such as anti-virus, anti-spyware, firewall, IPSec VPN, cryptography, network intrusion prevention, PC firewall, SSL-VPN, web application firewall, anti-spam and Wireless LAN. For more information about ICSA Labs, please visit: <http://www.icsalabs.com>.

Copyright

© 2009 Verizon. All Rights Reserved. WP14117 11/09. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information or storage retrieval system, without the express written permission of Verizon.

