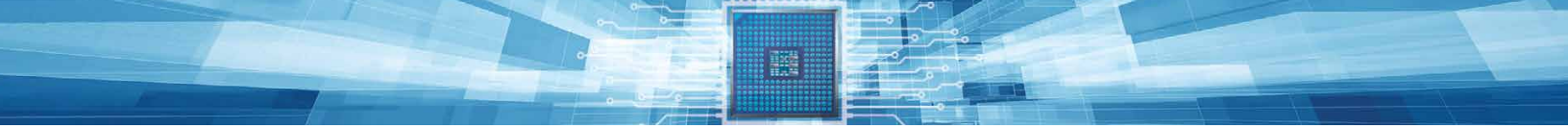
Balancing Cost, Efficiency and Risk for Security Operations

Model for calculating the overlap, effectiveness and ROI of multilayered security

White Paper



Introduction

Anyone who has tried to make a significant corporate purchase knows that you should estimate the total cost of ownership (TCO) and return on investment (ROI). Presenting convincing models with tangible cost benefits is usually the fastest way to get your CFO's approval.

But demonstrating ROI for an IT security purchase has always been challenging. For example:

- How do you calculate the risk of a small chance of having a huge breach?
- How can you gauge the effectiveness of solutions against constantly changing threats?
- How do you measure the overlap and inefficiency inherent in having multiple layers of security with diminishing returns?
- With today's overload of warnings, alerts, and false positives, how can you manage what's always the biggest part of a TCO model—the precious time of your thinly stretched IT staff?

The difficulty is that it's hard to simplify a complex range of challenges into a single monetary measure. You need models that cover a range of very different apples-and-oranges metrics. You also need a model that is sophisticated and nuanced, but not so complex that the results seem like voodoo.

This paper also lets you compare your current TCO with the significant benefits we believe you will realize by implementing the Virsec® Security Platform. You can do this by trying out our ROI Calculator where you can enter the specifics of your own environment and compare your current security situation to how things would look with Virsec. Virsec's Trusted ExecutionTM technology changes the equation for security by detecting the widest range of threats in real-time, and protecting organizations from today's advanced cyberattacks that fly under the radar of conventional security tools.

1. Solution Overlap: Estimating the overlap of various layers of security such as antivirus, web application firewalls, and server endpoint security. While multiple layers may improve security, too many separate solutions deliver diminishing returns and inflate your management costs.
2. Alerts and False Positives: calculating the staffing costs of responding to alerts and false positives, and the exposure if all alerts are not investigated—typical for most organizations.
3. Security Effectiveness: estimating the cumulative effectiveness of multiple security layers across different types of threats, and using risk models to calculate potential breach exposure.

As with any complex model, there are a range of assumptions that may vary by organization. Numbers used for assumptions in the paper are based on publicly available and third-party estimates of effectiveness, false positive rates, and percentage overlap between solutions. This paper includes an example of ROI calculations and includes a worksheet to estimate your own numbers. A dynamic tool to calculate custom ROI is available, allowing you to experiment with any of the variables.

This paper also lets you compare your current TCO with the significant benefits we believe you will realize by implementing the Virsec® Security Platform. You can do this by trying out our ROI Calculator where you can enter the specifics of your own environment and compare your current security situation to how things would look with Virsec. Virsec's Trusted ExecutionTM technology changes the equation for security by detecting the widest range of threats in real-time, and protecting organizations from today's advanced cyberattacks that fly under the radar of conventional security tools.

1 Solution Overlap

The most common complaint from security analysts is that there are too many layers of security and too many point solutions, each requiring management, tuning, and response to frequent alerts.

The security space continues to evolve rapidly and some amount of overlap between solutions is inevitable. As certain types of attacks become well understood, features that protect from those attacks become commoditized and available in multiple products. For example, many security products deliver protection from well known viruses.

But covering the latest threats often requires advanced technology to close urgent security gaps, including against threats that are unknown. The challenge is that the newer solutions may replace some of the legacy layers, but there are often tradeoffs. Frankly, it's always easier to add new layers than to eliminate old ones, but the accumulation of solutions over time can become unmanageable.

For the purposes of this paper we have identified eight layers of security defense that have evolved in recent years including:

- Antivirus: signature-based solutions protect against known malware
- Firewall: traditional networks gateways segment traffic to establish basic security
- Intrusion Prevention System (IPS): monitor network traffic for anomalies and threats
- Next-Generation Firewall (NGFW): add packet filtering, NAT and other capabilities
- Web Application Firewall (WAF): monitor HTTP traffic, filter content specific to web apps
- Host Firewall, IDS (HIDS): monitor traffic for specific systems or applications
- Next-Generation Antivirus (NGAV): apply behavioral models and pattern matching for detection
- Whitelisting: solutions that limit access to known good files or processes
- Runtime Application Self Protection (RASP): block exploitation of vulnerabilities, applications during the software development life cycle (SDLC)

Example

For this study, we use an example of a mid-sized regional bank, Indenture Credit Union. They have a staff of 2,500 employees and manage sensitive and regulated financial data for customers. Their IT organization has a wide range of security tools and manages them in a security operations center (SOC) with a full-time IT security team of 23. This security team faces challenges typical of the industry—too many overlapping security products, too many alerts and false positives to act upon, and broad concerns about the effectiveness of their solutions against today's advanced cyberattacks.

While some products may check boxes in multiple categories, they generally do not offer best-of-breed coverage across multiple categories.

Many enterprises have deployed multiple solutions on this list, and the overhead of managing overlapping solutions can be significant. The fact that there is overlap is clear, but the amount of overlap is somewhat subjective and often depends on the level of expertise and fine tuning at each layer.

This paper and our online calculator provide a model for estimating the cumulative coverage overlap between solutions. Whenever possible, the values used in this example are estimates based on third-party analysis or reports.

In our sidebar example case on page 2, Indenture Credit Union uses each of these security layers and has estimated the annual costs for CAPEX (license/subscription and support) and OPEX (full-time employees—FTEs—required to manage each layer). For these calculations, the average IT salary used is $120,000 per year. The total annual cost for all layers and salaries is $3.055 million.

The next step is to estimate the overlap between each of these security layers and calculate the total amount of redundancy and related costs.

Combining this with the number of servers and cost for each solution level provides an estimate for the cost to organizations of redundant security layers.

Table 1 lists the estimated overlap between each layer of security. These numbers are based on best available industry averages but can be changed in the live tool. For example, the overlap between a typical NGFW and WAF is estimated at 20%.

	CAPEX	FTEs	OPEX	Total
Antivirus	25,000	1	120,000	145,000
Firewall	30,000	2	240,000	270,000
IPS	20,000	3	360,000	380,000
NGFW	35,000	3	360,000	395,000
WAF	50,000	6	720,000	777,000
Host FW	40,000	4	480,000	520,000
NGAV	30,000	2	240,000	270,000
Whitelist	25,000	1	120,000	145,000
RASP	40,000	1	120,000	160,000
	$295,000	**23**	**$2,760,000**	**$3,055,000**

Table 1: *CAPEX and OPEX cost estimates*

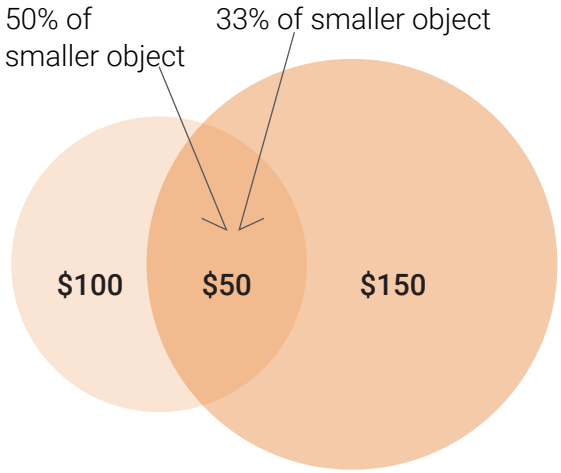
	Firewall	IPS	NGFW	WAF	Host FW	NGAV	Whitelist	RASP
Antivirus	5%	10%	20%	30%	20%	30%	15%	5%
Firewall		20%	20%	20%	25%	40%	10%	15%
IPS			10%	10%	15%	10%	15%	5%
NGFW				20%	20%	20%	20%	22%
WAF					30%	25%	15%	20%
Host FW						20%	20%	20%
NGAV							30%	25%
Whitelist								15%
RASP								

Table 2: *Estimated overlap across security layers*

Note on Methodology

The overlap percentage between two objects will be different unless they are the same size. For example, if two layers cost $100 and $150 and they overlap by $50, this will be 50% of the smaller object and 33% of the larger one. For consistency, all overlaps are shown as a percentage of the smaller object.

Finally, Table 3 shows the overlap in dollars between each layer of security based on the total expenses and overlap percentages from Table 1.



	Firewall	IPS	NGFW	WAF	Host FW	NGAV	Whitelist	RASP
Antivirus	7,250	7,250	29,000	43,500	29,00	43,500	21,750	7,250
Firewall		54,000	54,000	54,000	67,500	108,000	14,500	24,000
IPS			38,000	38,000	57,000	27,000	21,750	8,000
NGFW				79,000	79,000	40,500	29,000	35,200
WAF					130,000	67,500	21,750	32,000
Host FW						54,000	29,000	32,000
NGAV							43,500	40,000
Whitelist								21,750
RASP								
	$7,250	**$61,250**	**$121,000**	**$214,500**	**$362,500**	**$340,500**	**$181,250**	**$200,200**
						Total Redundancy		**$1,488,450**

Table 3: Overlap costs by security layer

Take Away

Based on this model we've estimated total overlapping redundant costs to be **$1,488,450** per year. This represents **49%** of the total costs for owning and operating these security layers. While these numbers will vary by specific organizations, in most cases there is clear redundancy and a compelling case for updating and consolidating security layers.

2 Alerts and False Positives

For most security solutions, the cost of purchasing a product is a small fraction of the labor costs required to keep it tuned and effective, plus follow up on both real and false alerts. In fact, false positives have become the bane of most security practitioners' lives, and the cumulative cost of managing alerts across multiple security solutions can be overwhelming.

Most security products present inherent dilemmas. If you run them in the most restrictive modes you will balloon the number of false positives and user complaints. But if you dial down security with fewer alerts, you are likely to be dumbing down your coverage and inviting a breach disaster.

Alert fatigue for IT teams is also a major source of frustration and inefficiency. The more frequent the alerts, the more likely you are to miss the real threats. The dirty secret of many security teams is that they can't afford the time to follow up with every alert and end up ignoring or suppressing a sizable percentage of them. Remember that with the massive Target breach, security products did provide many alerts that something was wrong, but these were ignored because of alert fatigue and the pressing business imperatives of the holiday shopping season.

To calculate the total cost of managing and responding to security alerts, this model considers several factors:

- Total number of alerts per week across security products
- The false positive rate based on industry averages
- The average time for IT staff to follow-up on alerts, investigate and resolve any problems
- The capacity of a team to follow-up on alerts and percent covered
- The number of true positives and percent not acted upon
- The threat exposure for an organization because of bandwidth limitations

The following example uses data from the sample bank—Indenture Credit Union.

	Alerts Per Week	False Positive Rate	FPs Per Week
Antivirus	200	20%	40
Firewall	100	5%	5
IPS	200	30%	60
NGFW	160	25%	40
WAF	400	40%	160
Host FW	250	30%	75
NGAV	250	26%	65
Whitelist	300	30%	90
RASP	50	10%	5
Total	**1910**	**28%**	**540**

Weekly	
Total Alerts	1,910
False Positives	540
FP Rate	28%
FTEs	23
Alert Follow Up	1.50 hrs.
Alert Capacity	613
Alert Coverage	32%
Missed Alerts	1,297
Missed TPs	930
Missed TP Rate	**49%**

Table 4: Alerts, False and Capacity

Table 4 lists the average number of alerts per week received by the SOC team by type of security. From this we calculate the average number of false positives based on industry averages for each technology.

The total staffing costs are fixed based on the current number of employees of 23 (see Table 1). With an average salary of $120,000, the labor costs are $2.76 million per year.

However, if the average security alert requires 1.5 hours to investigate and resolve, (assuming a 40-hour work week) the team only has capacity to follow up on 613 alerts—only 32% of the total.

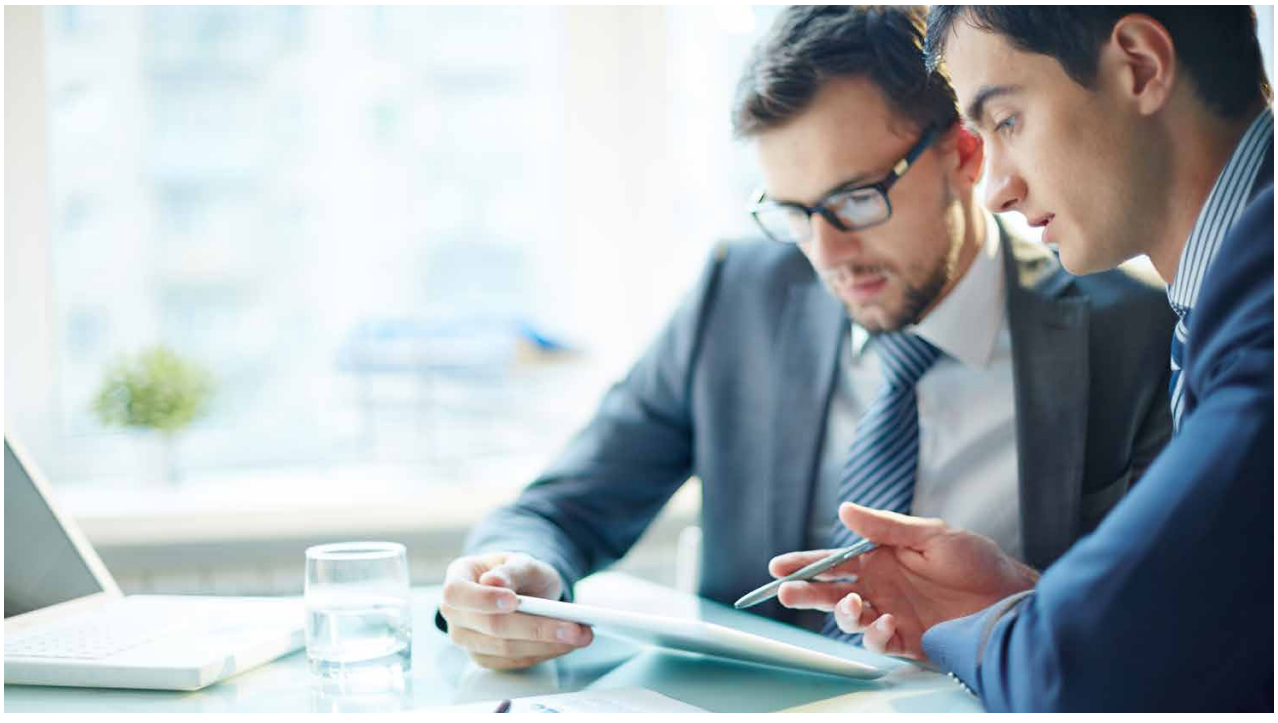
Of the alerts not acted upon, we assume that 28% would have been false positives. This leaves a total of **930 alerts—49%** of the total, that represent actual threats that have not been acted upon. This is a significant gap in security and risk that is not easily addressed. This forces IT organizations typically to make difficult choices, none of which are satisfactory:

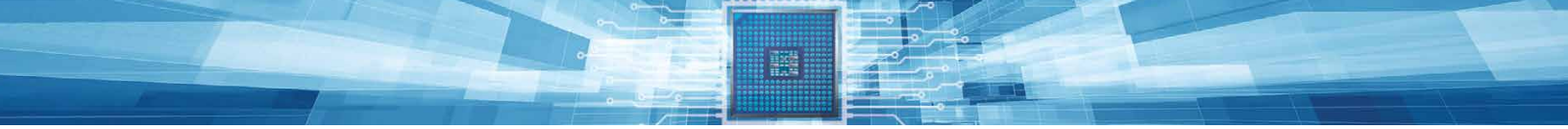
- Enforce more restrictive security policies that inevitably increase the total number of alerts and false positives, increasing the number of alerts not acted upon
- Lower security policies to be more permissive, which lowers the response burden of the IT team, but inevitably reduces the effectiveness of each security layer
- Accept the status quo and cross your fingers that missed alerts don't turn into breach disasters like Target

The online version of the calculator tool enables you to adjust the security level for each technology and see the impact on false positives and effectiveness.

Take Away

Many security teams cannot follow up on all alerts, leaving significant exposure. For this example, almost half of the alerts represent real threats that are not acted upon because the IT security team is too busy with other alerts.





3 Security Effectiveness

At the end of the day, all organizations want effective security, but having multiple layers of security does not always deliver more effective results. Conventional wisdom is that organizations should apply defense in depth, deploying multiple technologies to try to close the gaps of each specific layer.

As discussed above, overlapping layers raises costs, and increases the number of alerts, potentially overburdening your team with alerts and false positives. Redundant layers also deliver diminishing returns, and reduce your overall ROI.

More importantly, effectiveness of each security technology varies greatly based on the type of threats. For example, most products have a high capture rate of known threats, using signature databases. However, unknown threats, fileless attacks and memory exploits are not detected by most security layers—and so, they are becoming much more frequent.

The NIST National Vulnerability Database (NVD) tracks threats by type and frequency over time. For this study, we have categorized the NVD vulnerabilities, and then assessed the effectiveness of each security layer across these categories:

- **Network-based threats:** attacks targeting data at the network layer
- **Known file-based threats:** executable malware files that are found in most signature databases
- **Unknown file-based threats:** new executable malware without existing signatures
- **Malicious scripts:** an increasing threat vector as scripts are largely customized and not found in signature databases
- **Memory & process threats:** advanced attacks designed to corrupt memory and/or manipulate application processes

The effectiveness of any specific security technology changes over time as threats evolve and become more sophisticated. For example, as any type of malware gets identified, it is added to threat signature databases and can be blocked by multiple types of security. However, the hackers know this, and the advanced ones rapidly move to new attack vectors that have not been identified or cataloged.

We have also seen several generations of cyberattacks that find ways to sneak under the radar of existing security tools. The latest wave of attacks target unprotected areas of applications at the process and memory level using fileless techniques to evade databases of known malware.

Deploying multiple layers of security is an inherently good practice—if one security layer misses something, there is a good chance another technique will catch it. But as we've seen, overlap in technologies, and the overwhelming number of redundant alerts can make this unmanageable. While it's important to fill as many security gaps as possible, most legacy security technology redundantly covers a narrow band of attacks, while leaving other areas wide open.

Table 5 shows the average coverage across security technologies and threat types. The net coverage calculates the total coverage going through all relevant layers. Each layer is calculated against the uncovered remainder of the previous layers. This table is color coded—red representing the least coverage, and green representing the high levels of protection.

	Network	Files (Known)	Files (Unknown)	Scripts	Process/ Memory	Average
Antivirus	0%	75%	0%	0%	0%	**15%**
Firewall	80%	0%	0%	0%	0%	**16%**
IPS	30%	10%	0%	0%	0%	**8%**
NGFW	70%	70%	0%	5%	0%	**29%**
WAF	0%	40%	0%	25%	0%	**13%**
Host FW	0%	50%	0%	0%	0%	**10%**
NGAV	0%	60%	10%	10%	5%	**17%**
Whitelist	0%	60%	30%	0%	0%	**18%**
RASP	0%	0%	0%	0%	20%	**4%**
Net Coverage	95.8%	99.7%	37.0%	35.9%	24.0%	**58%**

Table 5: Heat map of coverage across technologies and threat types

As you can see, legacy solutions such as antivirus, firewalls, and IPS are well established in protecting against traditional network exploits and known file-based malware. In fact, with two or three layers of security, these threats can be covered more than 95%. You can also see significant overlap in solutions coverage for detecting known file-based attacks, with diminishing returns.

This table also shows that coverage for advanced threats that involved unknown files, scripts, process or memory exploits across existing security layers is very weak. While some newer solutions such as next-gen AV and whitelisting, are touted as addressing unknown files, and scripts, they are all based on external patterns of past behavior—not on the actual execution within applications.

Only runtime application self-protection (RASP) technology offers some protection against advanced memory-based attacks, but this coverage is limited to only interpreted code at the web application layer. RASP technologies are also typically limited in usage to software development, and not applied in real-time with existing applications.

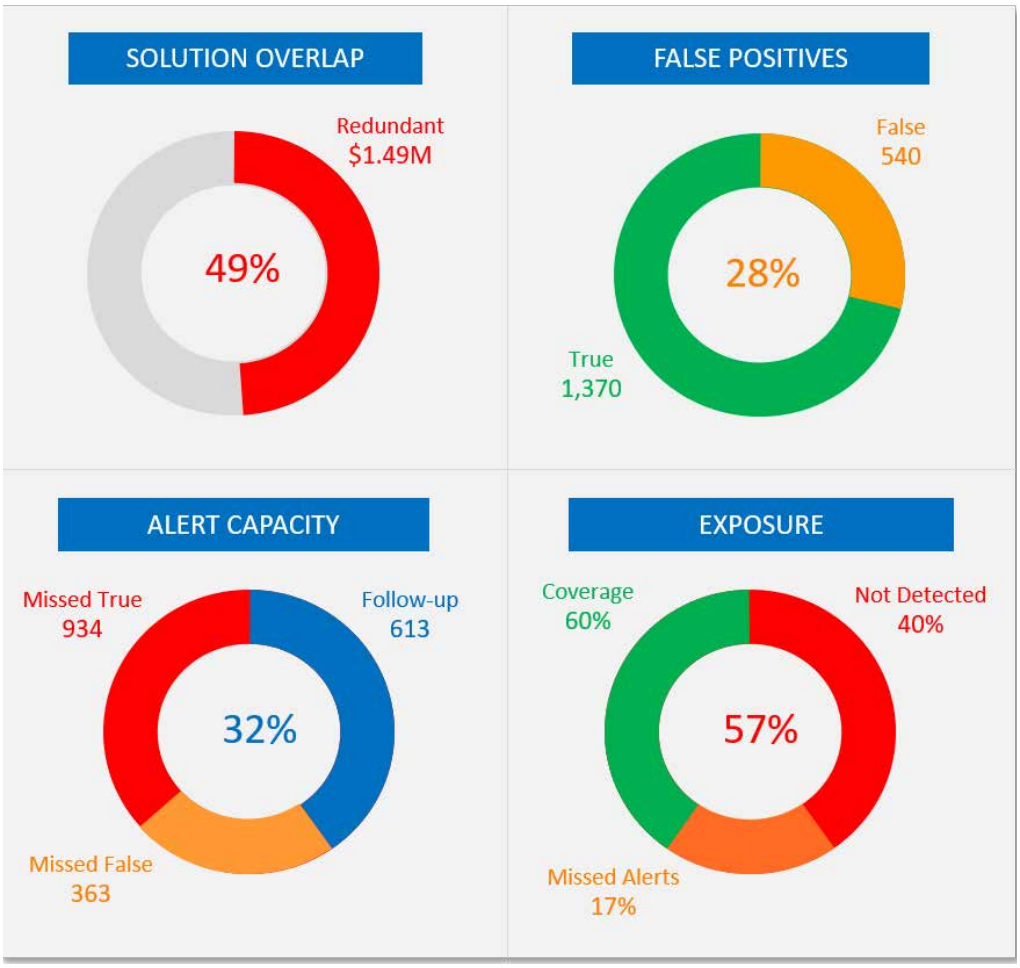
Based on this data, our example bank—Indenture Credit Union, has a total overage coverage of **58%** across the range of today's threats. This not only leaves more than **40%** exposure, but as discussed in the previous section, **29%** of the detected threats are not acted upon because of bandwidth limitations of the IT security team. Combined, this means that on average only **42%** of all true threats get detected and acted upon.

4. Overall Results

Overall, the results from this study show many problems with conventional, cumulative security models. There is considerable overlap between existing technologies, yet the total coverage is woefully inadequate, and IT security organizations are struggling to keep up with a barrage of false alarms.

No wonder the bad guys seem to be winning the cyber security war.

Here is a summary of the key results from our example with Indenture Credit Union:



5. The VIRSEC Alternative

Virsec directly tackles the significant exposure that organizations face from today's advanced cyberattacks with a fundamentally different approach to security. Most legacy technology is locked into an outdated security paradigm—protecting the perimeter and looking for patterns of known attacks.

Protecting networks at the perimeter seems logical but this model is inherently limited in effectiveness. Even the best security guard outside a building has little knowledge or context of what really goes on inside. A guard can look for obvious threats, but most attackers are stealthy and may even be malicious insiders. Without inside knowledge of the workings of businesses, the guard is mostly for show.

Security based on pattern matching is always backwards-looking and only protects against threats that have been previously identified, analyzed and cataloged. Today's innovative hackers know not to repeat themselves and therefore intentionally use new hacks or vulnerabilities that have not been previously identified and patched.

Security from the inside

Virsec Security Platform takes a radically different approach. Rather than trying to detect threats with a perimeter gateway, Virsec lives side-by-side with your applications, detecting and stopping threats where they are aimed. With its patented Trusted Execution technology, Security Platform dynamically maps what your applications are allowed or not allowed to do. Your applications should be predictable and are designed to follow predefined paths. If they don't, something is seriously amiss, and this is a definitive indicator of hacking or tampering.

Virsec also operates at a layer well below any other security technologies, monitoring application processes and memory usage in real-time. The recent wave of advanced attacks, such as WannaCry, Not-Petya, and Equifax, all used fileless techniques to break in and memory buffer overflow errors or corruption techniques to manipulate applications into going off the rails and exposing data.

Virsec Security Platform is unique in its ability to precisely detect and block advanced attacks at the lowest levels. Because Virsec's approach is deterministic, not reactive, it is extremely precise, largely eliminating the overhead of false positives.

Significant improvements in coverage

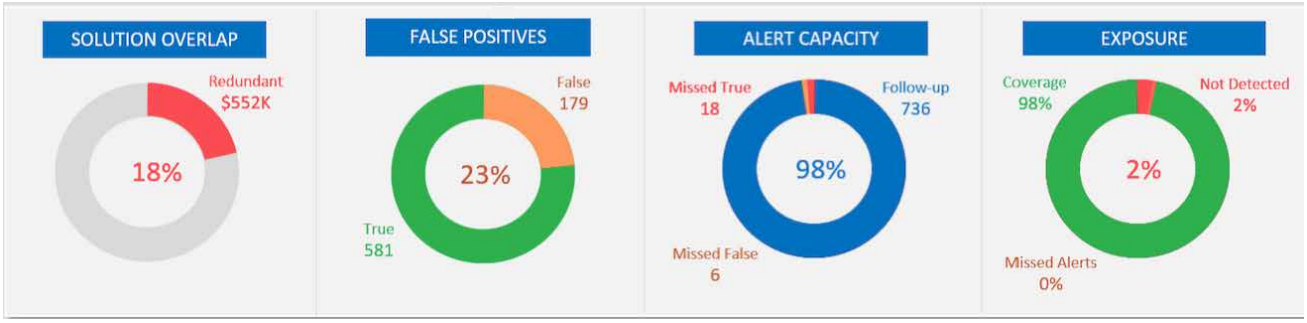
Virsec Security Platform protects against close to 100% of today's most dangerous threats, including unknown files, scripts, and process or memory exploits. This allows organizations to scale back on redundant security layers, while filling the significant holes left by legacy security technology.

	Network	Files (Known)	Files (Unknown)	Scripts	Process/ Memory	Average
Antivirus	0%	75%	0%	0%	0%	**15%**
Firewall	80%	0%	0%	0%	0%	**16%**
IPS	30%	10%	0%	0%	0%	**8%**
NGFW	70%	50%	0%	5%	0%	**25%**
WAF						
Host FW	10%	25%	0%	0%	0%	**7%**
NGAV						
Whitelist						
RASP						
VIRSEC	5%	90%	98%	98%	98%	**98%**
Net Coverage	96.4%	99.2%	98.0%	98.1%	98.0%	**98%**

Table 6: Virsec coverage and overall net coverage after eliminating redundant layers

Table 6 shows how Indenture Credit Union used Virsec to improve coverage and eliminate redundancy. They chose to leave their firewalls, conventional AV and IPS systems in place, to cover network threats and know file-based malware.

They also chose to keep their NGFW and Host FW layers, but reduced their subscriptions to non-premium levels. Finally, they eliminated four expensive, but ineffective layers—their WAF, NGAV, whitelisting, and RASP products. The net result delivers over 98% coverage across all of today's threat types.



Dramatic reduction in management costs

Virsec's deterministic model is extremely accurate and eliminates almost all false positives. Because Virsec protections operate at the application layer, it instantly sees rogue activity, while ignoring the noise and false alarms endemic to perimeter or pattern matching security products.

Table 7 shows the same model used in Section 2, but adding Virsec and eliminating the redundant and false-positive prone WAF, NGAV, whitelist, and RASP layers. Also, the NGFW and Host FW layers have been set in more permissive modes to reduce false positives.

	Alerts Per Week	False Positive Rate	FPs Per Week
Antivirus	180	20%	36
Firewall	100	5%	5
IPS	150	30%	45
NGFW	130	25%	32.5
WAF			
Host FW	200	30%	60
NGAV			
Whitelist			
RASP			
Virsec	**75**	**1%**	**1**
Total	**760**	**23%**	**179**

Weekly	
Total Alerts	760
False Positives	179
FP Rate	23%
FTEs	23
Alert Follow Up	1.25 hrs.
Alert Capacity	736
Alert Coverage	97%
Missed Alerts	24
Missed TPs	19
Missed TP Rate	2%

Table 7: Alerts and false positives with Virsec

The improvement and cost reduction are dramatic. Because they can eliminate redundant security layers, the IT security team can successfully follow-up on 97% of alerts while freeing resources to work in other areas. There are significantly fewer false positives, and the accuracy of Virsec reduces the overall average response time to 1.25 hrs. Because Virsec dramatically improves overall coverage to 98%, the gap in alert coverage represents a negligible threat of well under 1%.

Finally, on the cost side, Virsec also has a dramatic impact. Because Indenture Credit eliminated four costly layers of security and reduced subscription levels on the remaining layers, the total annual costs for the security operations team was reduced from $3.055M to $2.07M—a reduction of over 1/3.

Conclusion

Despite decades of investment, today's IT security situation is more precarious than ever. New threats are running rampant, while costs to maintain multiple layers of legacy for security are out of control.

Virsec believes it's time for a new approach to security. By focusing at the application, process and memory level, Virsec thwarts today's most damaging threats instantaneously where it matters most. Because Virsec is deterministic, not reactive, it is highly precise in eliminating the vast majority of guesswork and false alarms caused by conventional security tools. With greater accuracy, you can significantly reduce the overhead of your security operations, while dramatically improving security coverage and peace of mind.

We encourage you to use our online calculator (available **now, here**) to estimate the overlap, costs, and effectiveness of your current security operations, and see the significant benefits of deploying Virsec.

And, of course, seeing is believing, and we encourage you to set up a time for us to demonstrate the solution and deploy it your environment.

About Virsec

Virsec is an innovative cyber security leader protecting organizations from today's most sophisticated and damaging cyberattacks. Through its unique technology, Virsec definitively prevents zero-day threats, fileless attacks and memory corruption exploits that are invisible to conventional security tools. Virsec's patented Trusted Execution™ system deterministically stops advanced security attacks in real-time, delivering unprecedented accuracy, without false positives. Virsec is headquartered in San Jose, California with a global presence in Europe, Asia, and Australia.

virsec®

US West Coast:
226 Airport Parkway, Suite 350 • San Jose, CA 95110

Email: info@virsec.com • Phone: (877) 213-3558 • Web: www.virsec.com • Twitter: virsecsystems