CROWDSTRIKE

GUIDE TO AV REPLACEMENT

What you need to know before replacing your current antivirus solution

INTRODUCTION

Every year, thousands of attacks are successfully perpetrated against organizations of all sizes. Yet many of the victims had endpoint protection solutions in place. In fact, the adoption of antivirus (AV) is virtually universal, so why are so many attacks succeeding? In most cases, attackers expect their targets to be running some form of protection and have adapted their tools, techniques and procedures (TTPs) to evade detection.

From sophisticated morphism and obfuscation of malware, to malicious usage of legitimate applications or simple credential theft, opportunities to bypass traditional protection abound. Conventional antivirus, which focuses primarily on detecting and preventing known malware, is ill-equipped to handle this new generation of rapidly evolving threats. Consequently, an increasing number of organizations are looking for solutions that can effectively handle these emerging challenges. However, with so many options and buzzwords and so much hype, finding the right solution is a daunting task.

CrowdStrike has written this guide to help security professionals who are considering replacing their current AV and/or endpoint protection solutions. The goal is to clarify and simplify the decision-making process by focusing on the critical information you need to make an informed decision. This guide analyzes the most important elements to consider when replacing a current solution, including how to plan for the replacement and how to choose the best solution for your organization. It then examines the unique advantages of CrowdStrike's endpoint protection as a next-generation solution to replace your existing AV.

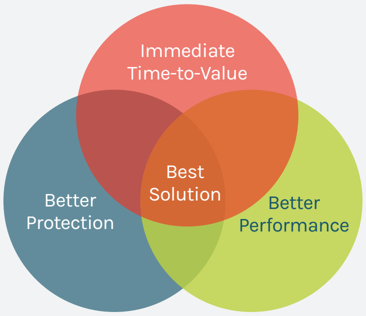
CHAPTER 1 HOW TO PLAN

CRITICAL ELEMENTS TO CONSIDER

Without specific criteria in mind, it is easy to get lost in the vast and confusing endpoint security market, where you could run the risk of exhausting your resources and spending months and tens of thousands of dollars, only to increase your security effectiveness by one or two percentage points. To avoid this pitfall, first think about why you are considering a change. The majority of customers recognize that they have two significant issues with their current endpoint protection: it is ineffective, as illustrated by the number of security incidents they have failed to stop; and it degrades performance, robbing endpoints and end users of their productivity. Thus, for most organizations, the goal of AV replacement is to gain better protection and better performance.

CROWDSTRIKE RECOMMENDATION: FOCUS ON PROTECTION, PERFORMANCE AND TIME-TO-VALUE

To gain significant value from the change, your decision criteria should focus first on protection and performance. However, there is another important criterion worth considering: time-to-value. As the name implies, time-to-value is the period of time required to derive value from a solution, and it directly reflects how easy that solution is to deploy and fully implement. This is a critical consideration, since even a solution offering superior performance and protection will be of little benefit if it takes years to implement.



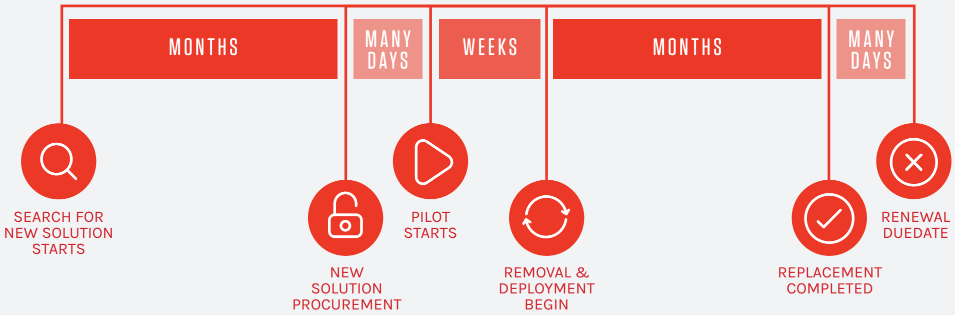
Decision criteria should be based on three simple concepts:

- Protection improvements: How much better will it protect?
- Performance improvements: How much lighter will it be?
- Time-to-value: How fast and easy will it be to deploy and make fully operational?

WHEN TO START PLANNING

One of the limitations you may encounter when replacing your current solution is time. Many organizations start the process too late, only to find themselves up against the deadline imposed by their renewal date.

Start early to avoid this pitfall. Use the timeline below to assess how much time you need and how soon you should begin the process by counting backwards from your renewal due date. The more endpoints you own, the sooner you should begin, because the removal and deployment processes will take longer. Don't wait until you get a budget to begin evaluating, build your business case early.



CHAPTER 2 HOW TO EVALUATE & REVIEW SOLUTIONS

At the time this guide is being written, there are over 90 endpoint protection solutions on the market and they are far from being equal. Yet, on paper, they can sound and look very similar, creating a confusing marketplace for the buyer. In addition, each vendor may use a different approach, making one-to-one comparisons difficult. Therefore, an in-depth evaluation is critical before making a decision.

Here are three key elements to ensure you have a thorough and effective evaluation process:

- Define your goals clearly to help you navigate through the claims, jargon and hype used by vendors.
- Use multiple sources of information and different methodologies to get a complete and accurate picture of the solutions you are considering.
- Try the products you are considering in your own environment to validate that they are a good fit and can deliver on their promises.

HOW TO EVALUATE AND MEASURE PROTECTION EFFICACY

Measuring the efficacy of traditional antivirus used to be a simple process. All that was needed was to run a collection of virus samples against the antivirus software and compare the number of samples each solution caught. The advent of today's sophisticated threats have made this methodology insufficient because today's attackers do not always use malware. In fact, a good portion of breaches are malware-free. Instead, they use exploits, credential thefts or tools that are part of the operating system, such as PowerShell. While measuring effectiveness against malware is a good start, it is not enough to allow you to assess the true efficacy of a solution. Before evaluating a next-generation endpoint solution, it is worth investing some time and research into the methodology you want to use.

USE MULTIPLE SOURCES OF INFORMATION AND DIFFERENT METHODOLOGIES TO GET A COMPLETE AND ACCURATE PICTURE OF THE SOLUTIONS YOU ARE CONSIDERING.

PROTECTION — WHAT TO MEASURE

Ability to prevent malware

An endpoint protection solution needs to at least block known malware. And even though malware protection solves only part of the problem, it is extremely important that your solution is able to eliminate commodity attacks and take some of the burden off your other security technologies.

Ability to prevent unknown or zero-day malware

Today's attackers are constantly crafting new techniques to bypass anti-malware protection. A common technique is to modify or morph known malware into a zero-day attack, for which no matching signature exists. To achieve this, attackers use tools such as packers to evade detection by constantly changing or obfuscating the malware's true nature. This is why an effective anti-malware solution needs to be great at detecting known malware, but also be able to prevent unknown or zero-day malware.

Ability to protect "beyond malware"

Today's attackers have found an even more effective way to avoid anti-malware detection than using zero-day or unknown malware — doing away with malware completely.
First, they can use exploits to gain access without using malware. To stop these types of attacks, an endpoint protection solution requires comprehensive exploit blocking for attacks such as ASLR, Buffer Overflows and others. Second, as the operating system (OS) has become increasingly powerful, new opportunities for exploitation have appeared. Why should an attacker use malware or exploits and risk detection when everything he needs is provided in the OS itself? Attackers can use trusted Windows processes to execute exploits knowing that they will almost certainly evade traditional endpoint security measures such as antivirus and whitelisting. This includes both PowerShell and Windows Management Instrumentation (WMI). CrowdStrike has observed a marked increase in malware-free attacks leveraging existing OS tools and processes. The malware-free malicious activities CrowdStrike has observed in real life include:

- Using PowerShell as a staging tool to execute other scripts to compromise a system
- Using WMI to install backdoors that allow persistence by enabling the adversary to launch malicious code automatically, after a specified period of system uptime, or per a specific schedule

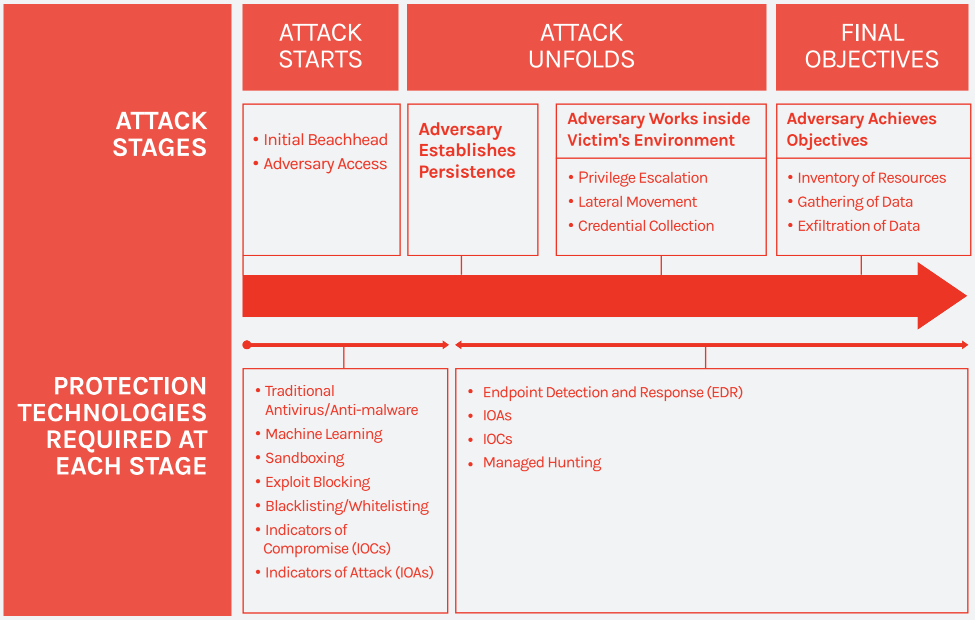
This is why protecting against malware-free attacks is more important than ever.

Ability to protect across the entire attack continuum

Even though prevention capabilities have reached rates of efficacy in the 90th percentile, there is still no silver bullet that can guarantee 100 percent prevention. That is why it is critical to evaluate what the solution can do in case an attack evades prevention. To avoid being breached without knowing it, the solution must keep track of events that occurred on the endpoint, so it can automatically detect and block an unfolding attack that managed to bypass the prevention methods. In addition, that ability enables security teams to perform retrospective searches for the purposes of an investigation.

The chart below provides an overview of the types of technologies that can help at different stages of an attack; capabilities you may want to consider as you evaluate a new solution.

PROTECTION THROUGHOUT AN ATTACK



ATTACK STAGES

ATTACK STARTS
- Initial Beachhead
- Adversary Access

ATTACK UNFOLDS

Adversary Establishes Persistence

Adversary Works inside Victim's Environment
- Privilege Escalation
- Lateral Movement
- Credential Collection

FINAL OBJECTIVES

Adversary Achieves Objectives
- Inventory of Resources
- Gathering of Data
- Exfiltration of Data

PROTECTION TECHNOLOGIES REQUIRED AT EACH STAGE

- Traditional Antivirus/Anti-malware
- Machine Learning
- Sandboxing
- Exploit Blocking
- Blacklisting/Whitelisting
- Indicators of Compromise (IOCs)
- Indicators of Attack (IOAs)

- Endpoint Detection and Response (EDR)
- IOAs
- IOCs
- Managed Hunting

Ability to protect the endpoints wherever they are

You should look for a solution that can protect endpoints wherever they are located and regardless of whether they are online or offline.

PROTECTION – HOW TO MEASURE

A common way to evaluate a solution is through testing, however, different tests can produce different results. A product that shines in one test might end up near the bottom in another set of tests. That’s because results are highly dependent on the testing methodologies, the configuration of the evaluated products, the tools being used to evaluate and even the expertise of the testers. One single test result is insufficient to accurately determine the protection efficacy of a product, but put together, the results from multiple sources of information, such as multiple independent test results and even your own internal results, can help you formulate a more objective opinion of the product’s true efficacy. To help you measure protection efficacy, we are going to cover the most prevalent protection technologies and how you can obtain evidence of their effectiveness.

Understanding protection technologies and what they mean

Understanding existing protection technologies can be useful when measuring and comparing endpoint protection solutions. The table on the following page describes the pros and cons of the most prevalent technologies.

HELPFUL FACTS	PROS	CONS
TRADITIONAL AV/SIGNATURE-BASED		
- The oldest technology	- Accuracy of identification - Extremely low risk of false positives	- Needs constant updates and maintenance - Huge footprint on the endpoint - Inefficient against zero-days and unknown malware - Protection is only as good as the last set of signatures - Does not protect against malware-free attacks
MACHINE LEARNING (ML)		
- Uses algorithms, or sets of calculation rules to identify malicious files - All ML not created equal - Equal vendor claims do not mean equivalent protection - Different vendors use different algorithms - Vendors should have ML engines available for testing on sites such as VirusTotal - ML is a field of Artificial Intelligence (AI) and terminologies may be used interchangeably	- Signatureless - Low footprint on the endpoint - Does not require updates - Effective against zero-day malware	- Risk of false positives depending on the quality of the algorithms - Ineffective against attacks that do not involve a malicious binary file
Sandboxing		
- A virtual machine (VM) in which executable files are run or detonated - Enables analysis of the file behavior	- Has the potential to provide a detailed analysis of the malware behavior	- Requires a file to be analyzed and is blind to attacks with no files - Malware writers expect sandboxing - If a VM is detected, the malware aborts execution to avoid detection
Indicators of Compromise (IOCs)		
- Often evidence that an attacker has been in the environment - Can be file hashes, IP addresses, domain names, URLs, registry keys and others - Make sure they are valid and coming from trusted sources to avoid blocking legitimate resources	- Easily shareable – can be used across multiple security solutions	- Often can only be detected if the malicious activity has already occurred - Can be removed by attackers as they cover their tracks - Their absence does not guarantee that an attacker was not in an environment

HELPFUL FACTS	PROS	CONS
Exploit Blocking or Exploit Prevention		
• Prevents malware-free attacks that make use of vulnerabilities • With many families of exploits, different techniques are needed to block them • Beware of vendors claiming exploit blocking when they can only block one or two types • Beware of vendors using signatures to block exploits, as they will only prevent known exploits – not zero-days	• Fills a gap that malware protection does not cover • Prevents exploitation of vulnerabilities • Protects systems that are not fully patched	
Indicators of Attack (IOAs)		
• Multiple activities based on behavior that indicates attack is occurring	• Allow users to act in real time on activity currently occurring on an endpoint based on behavior • May not only prevent malicious activities, can see and stop attackers' activities at any point in time during an attack • Even if the initial intrusion bypasses prevention, attacker's activities eventually will be caught and blocked • Lets users know that an attack or breach may be occurring right now, allowing users to take action immediately	
Whitelisting / Blacklisting		
• Users create a whitelist and/or a blacklist that defines what is allowed and not allowed to run • Better-suited for endpoints that seldom change (no updates, no new applications, etc.) as any change may require an adjustment of the whitelisting policies	• Gives users tight control over what applications are and are not allowed to run in their environments in addition to the prevention provided by the endpoint solution	• Ineffective against attacks that use legitimate and whitelisted applications to perform malicious activities • Ineffective against exploits • Requires extensive customization and tuning. The tasks of updating and tuning never end, especially in dynamic environments where new scripts, applications and updates occur regularly

HELPFUL FACTS	PROS	CONS
Endpoint Detection and Response (EDR)		
• Records all activities of interest on an endpoint for deeper inspection — on the fly and after the fact • Allows users to quickly detect and investigate attacks that passed through traditional prevention mechanisms	• Can help detect attacks that bypassed prevention technologies • Prevents attackers from dwelling in an environment for months before being discovered	

Self-administered vendor test results

Common sense dictates that vendors' self-administered tests should be taken with a grain of salt. They tend to demonstrate the strengths of the vendor's product and the weaknesses of its competitors', giving you only half the picture. It will be up to you to research and uncover the other half — the weaknesses of the vendor's solution and the strengths of the others. It is also important to fully understand the testing methodology used by the vendor. What samples and tools are they using, including which packer are they using to modify malware? How did they configure the other solutions? Although they might initially offer some attention-getting perspectives, their test results need to be corroborated with additional information.

External and independent tests

Independent testing is important to validate vendors' claims. Even though it can have limitations of its own, such as covering only a subset of the tested solution's abilities, independent testing provides some important advantages as an additional source of information. You should make sure the methodologies used are consistent, transparent and well-documented. This will allow you to fully understand the results and avoid making decisions based on a leap of faith.

Also, when considering third-party testing, make sure to get independent and competitive test results from a reputable and well-known testing house. A good way to judge this is if they are members of Anti-Malware Testing Standards Organization (AMTSO). Also, it's helpful to know how long they have been in the business of testing.

Testing internally: the importance of seeing for yourself

The final and probably most relevant evaluation is gained from conducting your own tests.

IMPORTANT NOTE: IF YOU INTEND TO USE LIVE MALWARE FOR INTERNAL TESTING, MAKE SURE ALL PRECAUTIONS ARE TAKEN TO AVOID COMPROMISING YOUR ENVIRONMENT. MAKE SURE YOU HAVE THE APPROVALS AND AUTHORIZATIONS REQUIRED TO PERFORM SUCH TESTS.

First, establish a testing scenario. Although some can be provided by vendors, for accurate external testing results, do not rely on scenarios from only one vendor as they may be biased toward their solution. Make sure the scenarios are realistic and mimic the real-life situations and techniques required by adversaries to execute a successful attack. For example, test a complete attack scenario rather than limiting the testing to one function, such as malware detection. This will allow you to assess how the solution responds to all the phases of an attack, not just one. This is key as today's attackers use combinations of moves as opposed to performing a one-time action. Realistic testing scenarios can demonstrate how a solution will protect you against adversaries who orchestrate various techniques into multi-stage attacks.

PROTECTION – QUESTIONS TO ASK

- What technologies does the solution use to prevent malware (signatures/DAT files, machine learning, blacklisting)? Specify which ones are used.
- How does the solution protect against unknown or zero-day malware?
- How does it detect attacks that do not leverage malware, such as those using PowerShell, WMI, or stolen credentials?
- How does the solution protect endpoints that are not on-premises?
- How does the solution protect endpoints that are not online?
- Does the solution prevent exploits? How and which ones?
- If an endpoint was compromised before the solution was installed, how can the solution help?
- How does the solution protect across each stage of the attack?
    - Before: what can the solution do pre-execution?
    - During: what can the solution do during execution?
    - After: what can the solution do if the attack was not prevented?

HOW TO EVALUATE AND MEASURE PERFORMANCE IMPROVEMENT

The second biggest criticism users have about traditional endpoint protection is the solution's impact on systems. Therefore, it is critical to assess the impact of the solutions you are considering on both the endpoint performance and the user experience. End users do not tolerate security products that impede their productivity and slow down their systems. Such solutions invariably result in increased calls to support and dissatisfaction with IT services.

PERFORMANCE – WHAT TO MEASURE

The user experience and impact on the endpoint need to be assessed in relation to deployment, but also for subsequent updates, ongoing maintenance and for the tasks the solution needs to perform to keep the endpoint safe. This assessment should also reflect the impact on network bandwidth and on your IT and desktop support teams. Consider the following measurements when assessing the total impact of a solution:

- Size of deployment package
- Footprint on the endpoint and on disk
- CPU usage at rest
- CPU usage when active
- Memory usage at rest
- Memory usage when active
- Tasks requiring endpoint resources. Measure CPU and memory usage while running tasks such as scanning endpoints, querying endpoints, etc.
- Bandwidth usage by the product on a regular basis (for communication, updates, configuration changes, etc.)
- Size and frequency of updates necessary to keep the solution at its optimal level of protection
- Required reboots – installation, updates (and the types of updates)
- False positive – at best they will take up IT time, at worst, they can halt operations

PERFORMANCE – HOW TO MEASURE

You can start by asking the vendor to answer your questions, but it is highly recommended that you also try the solutions on as many production endpoints as possible to truly test its impact and to gather user feedback.

PERFORMANCE

- Does the install require a reboot? How about updates?
- What is the impact of the solution on the endpoints? Footprint on disk, memory, CPU?
- How many agents/separate components do I need to install on my endpoint? What is the size of each?
- How many IT support calls were caused by the solution, and what were the complaints about?
- How is the new solution going to impact my users?
- What is your false positive rate?
- How often do you need to update signature or DAT files? What is the DAT file size?
- How much bandwidth does the product use? For deployment? For ongoing updates and maintenance?

HOW TO EVALUATE AND MEASURE TIME-TO-VALUE

Time-to-value measures the time it takes for a solution to be fully operational, including the ease with which it can be implemented and used. It goes beyond measuring the time required to deploy the solution in production and on some endpoints to include the time required to configure and tune the product so it can provide maximum value. Time-to-value is critical because a solution that can't be deployed or fully used, or one that remains on the shelf, leaves gaps that attackers can exploit to enter and remain in your environment undetected.

TIME-TO-VALUE – WHAT TO MEASURE

The following chart will help you estimate time-to-value:

	TASK	ESTIMATED DURATION
1.	Procurement of necessary additional software and hardware	
2.	Architecting a new solution management infrastructure: number and placement of management servers to service all endpoints regardless of their location, scalability determination, etc.	
3.	Deployment of supporting management infrastructure: management servers, backend databases, etc.	
4.	Deployment of the solution on 90 percent of production endpoints	
5.	Configuration of the solution: creating policies, rules, whitelists, etc.	
6.	Fine-tuning configuration	

TIME-TO-VALUE – HOW TO MEASURE

Insight can be gained from finding out if the vendor offers implementation services, as it could signify that their solution is complex to implement and that you will need additional help and expertise from the vendor. Talking to references, and running a trial or POV can also help with evaluating time-to-value.

TIME-TO-VALUE – QUESTIONS TO ASK

- How long does it take on average for an organization like mine to be fully operational?
- Does it require setting up a management infrastructure prior to deploying on endpoints?
- What additional hardware and software (servers, appliances, database licenses, components on the endpoints) are required to implement the product? Are they provided as part of the next-generation endpoint protection solution, or is there an additional cost?
- Do you recommend a professional services engagement to help with the deployment?
- Can the product be delivered via cloud infrastructure as a SaaS?
- If it is offered as a SaaS, does the cloud-delivered version offer parity of features with the on-premises version?
- Once deployed, how much tuning and configuration will the solution need before it is fully functional?
- How many distinct products/modules/agents/appliances do I need to cover all protection needs?
- How does the solution integrate with other security and enterprise tools?

WHAT ARE OTHERS SAYING?

Industry Analyst Reports

Industry analyst reports cover the results of market and product research to help customers in their decision-making process. They can be useful, providing in-depth analysis, product comparisons and sometimes insights that only analysts with inside information may be able to offer. They can provide you with a short list of vendors, if you want to narrow down your choices from the vast number of endpoint security vendors available. Finding out how many industry reports a vendor appears in can help you determine how well-established the vendor is in the market. Keep in mind that some reports are independent and some can be vendor-sponsored. The latter will usually specify which vendor sponsored the report.

References

Checking references is part of due diligence and ideally, you would not make a significant decision without first checking in with peers that have implemented the solution you're evaluating. Even though you know that references provided by a vendor will be positively predisposed towards their solution, you can still gain good insight from talking to a user of the solution. A valuable way to frame your discussion with references is to focus on critical areas, including:

- Product implementation and time-to-value
- Business value provided by the product
- Support: it is important to know how the vendor will treat you after you are a customer

To make the most of the time you have with a reference, prepare a list of questions ahead of time. This will also ensure that you follow a consistent process for each call. You may want to ask some general questions such as "Has the product met your expectations?" or "Why did you choose this solution over others?". Also, remember to ask specific, quantifiable questions, such as "How fast does support get back to you?" rather than just "How good is their support?" Or, "What percentage of the solution was deployed and how long did it take?", rather than a general question such as "How was deployment?"

Finally, if the vendor is providing references, ask for users that are similar to your organization. This can include factors such as size, industry, geographical diversity, etc.

Conducting A Proof Of Value (POV)

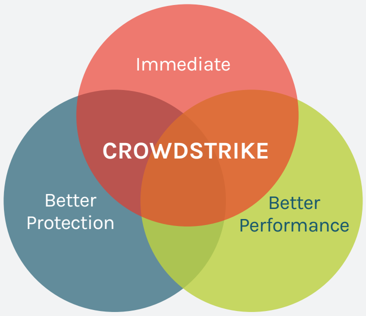
The goal of a POV is to experience the product hands-on, verify that it delivers what is expected and observe its behavior in your specific environment. POVs are often conducted with the help of the vendor and customers either build a prototype with a virtualized environment, or deploy the solution on a sample of production machines.

A POV that is done in a production environment will give you the best indication of what you can expect from the product. Evaluating in a lab might feel safer, but it might not truly reflect how the solution will perform in your specific environment.

Even with help from the vendor, a POV is typically the most time-consuming and resource-intensive evaluation method there is. As such, it is often the last step in a technical evaluation and should only be used for solutions that have made it to your short list.

If you decide to engage in a POV, make sure you are prepared to allocate the appropriate resources to conduct a meaningful hands-on evaluation. Prepare some scenarios ahead of time so you can compare each solution equally. An evaluation sheet like the one provided in this guide will help with assessing the results. Make sure the project has a defined length of time. This will prevent the POV from dragging on for months without reaching any useful conclusions.

CHAPTER 3 THE CROWDSTRIKE SOLUTION



CrowdStrike Falcon is a powerful, next-generation solution that should be considered as part of any comprehensive AV replacement. It is more effective against threats, has virtually no impact on endpoints and can be deployed and fully functional across tens of thousands of endpoints within hours, while also being easier to manage and maintain. CrowdStrike Falcon allows security teams to replace their legacy AV solution with confidence, offering superior protection from malware, exploits, malware-free intrusions and other advanced threats. Falcon also delivers an unprecedented level of visibility into attempted attacks by showing all details of the attack in an easy-to-read timeline.

BETTER PROTECTION

CrowdStrike Falcon does more than just stop malware – it extends beyond malware defense to prevent advanced targeted attacks – including sophisticated attacks that do not use malware. Employing the right detection and prevention features at the right time, Falcon is unique in its ability to stop attacks and breaches across the entire attack continuum, regardless of the tools, techniques and procedures (TTPs) used by attackers. The Falcon platform fills the wide security gap left by solutions that focus primarily on malware.

PREVENTION OF KNOWN AND UNKNOWN MALWARE

Machine learning

Falcon uses machine learning (ML) for pre-execution prevention. Located both on the sensor and in the cloud, CrowdStrike ML employs sophisticated machine-learning algorithms that can analyze millions of file characteristics in real time to determine if a file is malicious. This signatureless technology enables Falcon to detect and block both known and unknown malware, even when the endpoint is not connected to the cloud. CrowdStrike ML technology has been independently tested and you can find the latest results here: https://www.crowdstrike.com/products/compliance/

Blacklisting and whitelisting

This gives users the ability to upload custom hashes from their own whitelists or blacklists to set either an "always block" or "always allow" policy for known malware and machine learning. This allows other methods such as behavioral indicators of attack (IOAs) to still detect and prevent whitelisted processes from performing malicious activities.

PREVENTION OF MALWARE-FREE ATTACKS

Exploit mitigation

When a malicious actor leverages an exploit as part of either a malware-based or malware-free attack, CrowdStrike Falcon provides extensive exploit mitigation protection, consisting of stopping vulnerability exploit attempts and preventing hosts from being compromised. Falcon looks at the pre-execution technique that is being used, rather than the exploit itself, to prevent both known and zero-day exploits.

Indicators of attack

Detecting and blocking indicators of attack (IOAs) is a cutting-edge approach to stopping increasingly stealthy attacks. Sophisticated attackers will not limit their tactics to the use of malware and exploits. As we have previously discussed, they can access tools that are part of the operating system and use them for malicious purposes. Since those executables appear legitimate, preventing the malicious activity can be difficult for most endpoint security solutions. In contrast, IOAs allow Falcon to excel at blocking these types of techniques. This approach focuses on revealing the intent – what an attacker is trying to accomplish – by observing the TTPs used as the attack unfolds, and blocking it at any point in the attack life cycle. Capturing the timeline and context of relevant endpoint activities and matching them to IOAs allows users to not only stop attacks in real time, but to fully understand what has taken place and how the adversaries are trying to break in. Falcon also identifies your adversaries, providing crucial information that can help you proactively adapt your security posture to defend against them going forward.

For more information on IOAs, read the white paper, "Indicators of Attack vs. Indicators of Compromise": https://www.crowdstrike.com/resources/white-papers/indicators-attack-vs-indicators-compromise/

Online and offline prevention

The CrowdStrike Falcon intelligent sensor offers prevention whether online or offline and supports data processing and decision-making on the endpoint. This not only enables highly accurate detection and prevention, it keeps the endpoint protected everywhere – in the office or on the road, online or off.

BETTER PERFORMANCE

The Falcon agent was designed from the ground up to be as unobtrusive and lightweight as possible. As a result, there is no noticeable performance impact to the client and no reboot is required for installation or updates. The installation package is approximately 20MB and the footprint on the hard drive is close to the same size, with all files included. The agent uses approximately one percent of the CPU and 2MB of RAM, even at peak times. The Falcon agent will consume between 4MB to 6MB of bandwidth per day, streaming events to the cloud.

THE FALCON SENSOR HAS VIRTUALLY NO IMPACT ON THE ENDPOINT, MAKING IT AN EXCELLENT CHOICE FOR VIRTUAL ENVIRONMENTS.

Because Falcon uses machine learning to defend against malware, it does not use signatures or DAT files. This makes a significant difference with endpoint performance and also relieves security teams from having to worry about daily updates. Falcon does not need to perform scans to protect the system, eliminating the dreaded daily scans that are renowned for slowing endpoint performance. The minimal endpoint resource requirements of the Falcon agent also make it an excellent choice for virtual environments.

The CrowdStrike solution also simplifies management for IT and security teams. The console for the Falcon platform is 100 percent managed in the cloud, eliminating the need to configure, upgrade, backup, or patch any management servers.

IMMEDIATE TIME-TO-VALUE

Deploys and operational in hours

Since Falcon is both lightweight and cloud-enabled, it allows customers to operationalize it — that is to deploy, use and maintain it — with unprecedented speed. Falcon can be deployed within hours, not weeks or months, and requires no hardware or additional software, no tuning or configuration and has virtually no impact on the endpoint. For example, it is not uncommon when responding to a breach for the CrowdStrike Incident Response team to deploy and start using the Falcon sensor within hours across thousands of endpoints.
The Falcon Platform is designed with simplicity in mind. Because customers are already burdened with managing multiple, complex products in their environments, CrowdStrike designed the Falcon Platform to integrate seamlessly into your environment without adding complexity. It immediately begins to record activity and enable proactive hunting, offering you the fastest time-to-value in the industry.

	FALCON TASKS	ESTIMATED DURATION
1.	Procurement of necessary additional software	0
2.	Architecting a new solution management infrastructure: number and placement of management servers to service all endpoints regardless of their location, scalability determination, etc.	0
3.	Deployment of supporting management infrastructure: management servers, backend databases, etc.	0
4.	Deployment of the solution on 90% of production endpoints	Days
5.	Configuration of the solution: creating policies, rules, whitelists, etc.	2-4 hours
6.	Fine-tuning the configuration	0

Integration with existing solutions

Falcon integrates easily with your existing investments such as a SIEM, pulling in the events collected from your endpoints by the Falcon Sensor. The Falcon Platform's APIs allow you to integrate your existing third-party intelligence and IOCs (Indicators of Compromise) with Falcon, enabling you to take advantage of all the sources of intelligence available to you.

> CROWDSTRIKE CUSTOMERS REPORT A HIGH LEVEL OF SATISFACTION WITH CROWDSTRIKE'S ABILITY TO PREVENT AND DETECT THREATS TO THEIR ENVIRONMENT, WITH VIRTUALLY NO IMPACT ON ENDPOINT USER EXPERIENCE.

TESTING THE CROWDSTRIKE SOLUTION

The simplicity of the CrowdStrike solution makes it easy to test. There are no appliances, management servers, or virtual machine (VM) images to implement and no architecture changes are required. The only thing needed to get started is an endpoint machine where the sensor can be installed. At the time of this writing the sensor runs on Windows, Linux and Mac.

Once you have the sensor on your test machine, simply execute it and complete the install. Again, it is important to note the size and speed at which the sensor installs. Once the sensor is installed you can jump to several testing scenarios or you can continue to deploy more sensors. When the platform is engaged, CrowdStrike will provide testing scenarios based on real-life attacks observed by our incident response consultants, our Intelligence team and our managed hunting teams. The scenarios will simulate attacks and show you how CrowdStrike prevention and threat hunting address them. These scenarios will give you a preview of Falcon capabilities, however, the best testing occurs on actual production machines. This means once you deploy the sensor on a few test machines, it is highly recommended that you deploy the sensor to production servers and clients, fully loaded with your standard software. This will test the compatibility and impact of the sensor on real machines in your environment instead of just previewing features and functionality.

Depending on your time and budget, another testing option is to try a compromise assessment engagement from CrowdStrike. The compromise assessment team will use the sensor to conduct their investigation. This approach not only allows you to evaluate the Falcon sensor in production, it proactively identifies suspicious activity within your environment and pinpoints potential areas of concern.

CONCLUSION

One can argue that obtaining a security budget is no longer the hardest task security professionals encounter. The new struggle is finding the right solution in a sea of options, making sense of all the new technologies, and cutting through the hyperbole to arrive at an accurate assessment.

This confusing situation can make it easy to lose track of initial goals and to succumb to the siren calls of buzzwords and exaggerated claims. To avoid falling into that trap and to gain significant value from your AV replacement, try to focus your decision criteria on protection, performance and time-to-value. Also, be sure to ask these questions: Does this solution provide better protection? Does it deliver better performance? Is this solution easy to deploy, manage and maintain? Finally, you should always validate statements made by vendors. Cross-check the provider's claims with independent third-party testing, analyst reports, your own testing and other sources of information, so you can make the best-informed decision.

> "IN MY CAREER, THE DEPLOYMENT OF CROWDSTRIKE FALCON WAS PERHAPS THE EASIEST GLOBAL SECURITY TECHNOLOGY ROLLOUT I'VE SEEN. BY LEVERAGING THE TECHNOLOGY'S CLOUD ARCHITECTURE AND CROWDSTRIKE'S EXPERTISE, WE WERE ABLE TO DEPLOY WITH INCREDIBLE SPEED AND EFFICACY. WE REALIZED THE VALUE IMMEDIATELY."
>
> **ROLAND CLOUTIER**,
> STAFF VP AND CHIEF SECURITY OFFICER
> ADP

CrowdStrike Falcon's next-gen antivirus solution, meets all of these criteria, offering better protection by going beyond malware to protect systems at every stage of an attack. In addition, the lightweight agent has virtually no impact on endpoints and it is so easy to implement that the time-to-value is immediate. The CrowdStrike Falcon solution has also been tested and validated by independent third parties and analyst firms, allowing you to replace your legacy AV solution with confidence.

ABOUT CROWDSTRIKE

CrowdStrike is the pioneer of cloud-delivered endpoint protection. The company has revolutionized endpoint security by being the first and only company to unify next-generation antivirus, endpoint detection and response (EDR), and a 24/7 threat hunting service — all delivered via a single lightweight agent. Through its massive cloud, the company collects and analyzes 30 billion events per day from millions of sensors deployed across 176 countries.

With CrowdStrike Falcon, customers are able to effectively and efficiently replace their legacy AV, preventing all attacks with advanced signatureless artificial intelligence/machine learning and Indicator of Attack (IOA) based threat prevention. At the same time, CrowdStrike leverages its Threat Graph™ — one of the biggest threat data telemetry repositories in the industry — to provide unprecedented real-time visibility and crowdsourced protection for the entire customer community.

Many of the world's largest organizations put their trust in CrowdStrike, including three of the 10 largest global companies by revenue, five of the 10 largest financial institutions, three of the top 10 health care providers, and three of the top 10 energy companies.

CROWDSTRIKE

crowdstrike.com

15440 Laguna Canyon Road, Suite 250, Irvine, CA 92618