A Forrester Total Economic Impact™
Study Commissioned By Microsoft
July 2017

The Total Economic Impact™ Of Microsoft Windows Defender Advanced Threat Protection

Cost Savings And Business Benefits Enabled By Windows Defender Advanced Threat Protection

FORRESTER®

Table Of Contents

Project Director:
Sarah Musto

July 2017

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Key Benefits

Windows Defender ATP
catches 1.7x as many threats as other EDR tools

Reduction in risk of a data breach due to Windows Defender ATP:
40% reduction

Impact on end users from Windows Defender ATP:
4 hours of productivity savings per threat

Executive Summary

Microsoft commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) that enterprises may realize by deploying Windows Defender Advanced Threat Protection (WDATP). The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Windows Defender ATP on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed several customers with years of experience using Windows Defender ATP. Windows Defender ATP helps organizations detect, investigate, and respond to advanced attacks and data breaches on their networks.

Prior to using Windows Defender ATP, these organizations either used only antivirus, firewall, and other pre-breach tools or used a comparable endpoint detection and response (EDR) tool. The customers all noted that these prior tools were not sufficient to catch more sophisticated attacks. It would take a long time to detect a threat, if it was caught, and it would take more time to investigate and remediate these threats due to data overload, limited reporting capability, and increased scope of impact. This lack of visibility increased the risk of costly breaches involving data loss, ransomware, and business disruption.

With Windows Defender ATP, organizations can detect more breaches and are alerted to these breaches immediately. In order to understand what is happening on an endpoint, WDATP collects behavior events and sends that data to the cloud analytics service, using Microsoft threat intelligence and machine learning techniques to identify potential attacks and provide a detailed timeline to aid investigation into the scope of the breach. Security teams spend less time investigating threats, can act earlier when the scope of the breach is smaller, and can provide more targeted remediation, reducing overall response time and the impact on end users. By identifying more suspicious threats and addressing them faster, organizations can reduce their overall security risk, avoiding costly breaches. Because WDATP is built into Windows 10 (Anniversary Update and above), WDATP is continuously up to date, requires minimal administrator time for updates, and is invisible to the end user. Overall, WDATP allows organizations to cost effectively and efficiently reduce risk while having minimal impact on end users.

Key Findings

Quantified benefits. The following risk-adjusted quantified benefits are representative of those experienced by the companies interviewed:

- **Organizations identify more real threats with WDATP and resolve those threats faster.** A key benefit emphasized by interviewees is that WDATP identified 1.7 times as many threats as their prior EDR solution, on average, reducing the risk posed by undetected threats. Interviewees remarked that these threats were caught very early and WDATP provided analytics to aid four-times faster investigation and remediation.
- **WDATP reduces the risk of a breach by 40%.** By identifying actual serious threats earlier and remediating those faster, organizations can reduce their overall risk of incurring data breach costs by up to 40%, avoiding costly fallouts.

FORRESTER®

ROI
53%

Benefits PV
$2.3 million

NPV
$793,000

- **Fast threat detection and rich investigation timelines reduce the impact on end users due to remediation efforts.** Security teams can identify malicious threats before they spread and isolate the impact to specific files or applications, reducing the likelihood of user downtime or disruption. On average, end users lost 5 hours of productivity per threat before WDATP and lose 1 hour of productivity per threat with WDATP.
- **Minimal administration time for WDATP provides time savings compared with prior tools.** Because WDATP is built into the Windows OS, updates require minimal testing or troubleshooting compared with other EDR tools. The Windows-as-a-service delivery model ensures that WDATP is continuously up to date.
- **Replacing prior EDR and antivirus tools results in cost savings while enabling the incremental benefits above.** Organizations with a prior EDR tool can replace that tool with WDATP, enabling cost savings. Additionally, organizations can replace their third-party antivirus tool with Windows Defender Antivirus, which is part of Windows and is included in the WDATP license.

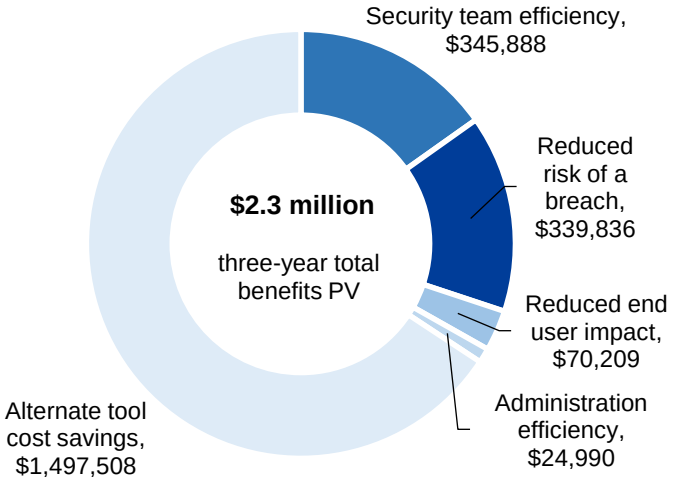
Costs. The interviewed organizations experienced the following risk-adjusted costs:

- **WDATP subscription costs.** Organizations pay an additional fee to upgrade from the E3 to E5 license to access WDATP. Subscription costs begin upon purchase.
- **Time spent on WDATP deployment and management.** All interviewees noted the minimal time spent on deployment and training for WDATP. Organizations spent upfront time on planning, testing, configuration, and training. Within a few hours each year, organizations can scale WDATP to many endpoints.

Forrester's interviews with four existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of $2.3 million over three years versus costs of $1.5 million, adding up to a net present value (NPV) of $793,000 and an ROI of 53%.

"WDATP has really changed the way we troubleshoot. Before, once we realized we had a problem, we had to figure out what it was and then how to clean up the infestation. With WDATP, I get an alert, I click on the machine, and I can see exactly what transpired, what files it's touched, and pretty much everything that there is to know about what all devices and registry keys and attempted communications were going on. It also tells me the last user. Before, we would only have an IP address. We'd have to figure out whose IP that belongs to, especially at that point in time, and that would be a challenge. With WDATP, I've got it right in front of me. Boom! I know who I need to talk to, and I can take a look at his machine. All of that aids how quickly you can reach out and take care of a problem."

Manager of information technology, automotive company



FORRESTER®

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Microsoft Windows Defender ATP.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Microsoft Windows Defender ATP can have on an organization:

DUE DILIGENCE
Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Windows Defender ATP.

CUSTOMER INTERVIEWS
Interviewed four organizations using Windows Defender ATP to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION
Designed a composite organization based on characteristics of the interviewed organizations.

FINANCIAL MODEL FRAMEWORK
Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organizations.

CASE STUDY
Employed four fundamental elements of TEI in modeling Microsoft Windows Defender ATP's impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Windows Defender Advanced Threat Protection Customer Journey

BEFORE AND AFTER THE WINDOWS DEFENDER ATP INVESTMENT

Interviewed Organizations

For this study, Forrester conducted four interviews with Windows Defender ATP customers. Interviewed customers include the following:

INDUSTRY	EMPLOYEES	INTERVIEWEE	ENDPOINTS ON ATP
Energy	75,000	Senior enterprise architect, security	4,430 today
Automotive	650	Manager of information technology	200 today
Food, beverage, and tobacco	100,000	IS architect	53,000 today
Information technology and services	400	Internal IT manager	180 today

Key Challenges

The interviewed organizations highlighted the following challenges prior to investing in Windows Defender ATP:

- **They had lower visibility into threat levels.** Most organizations noted that prior to WDATP, they could not catch as many threats or catch threats as quickly. While none of the organizations suffered a major breach, they were not confident in their level of risk, and often would only notice threats after they had spread.
- **Prior tools did not provide sufficient threat identification or reporting.** Whether using a comparative EDR tool or relying on antivirus software and firewalls, organizations felt that their prior tools did not provide the level of security needed. Organizations had trouble identifying threats quickly, before they could spread and cause real damage. Reporting was also spread across multiple interfaces and was presented in a more complex way, increasing the amount of time spent on investigation and analysis.
- **Their goal was to improve security while minimizing the burden on users.** All organizations noted the key goal of delivering an appropriate level of security to protect the business, while also maximizing the flexibility afforded to users to do their jobs effectively. Organizations wanted employees to be able to work remotely and download applications or files as needed, but they also wanted a more effective EDR tool to catch threats introduced by these user behaviors. Further, the organization wanted to minimize the number of security tools on endpoints to improve endpoint performance and provide less disruption to users.

> "Our Windows 7 was built on a security approach where we had a number of different venues that bring different solutions across the field, which adds complexity to performance within the build. With Windows 10, we decided to go as naked as possible to the core Microsoft product, and that's what we've done, is leverage the full Microsoft stack rather than hiring on just a brief solution."
>
> *Senior enterprise architect, energy company*

> "The question is that before, with no visibility, did we have a breach? We don't know. We never noticed that something was breached. But we were not able to validate this. Now, we have a view and we can react and try to increase the level of protection and we can reduce the risk of breach."
>
> *IS architect, food, beverage, and tobacco company*

Key Results

The interviews revealed that key results from the Windows Defender ATP investment include:

FORRESTER®

- **Security team efficiency with improved alerting and reporting.** Interviewees noted that immediate alerting with WDATP eliminates time spent monitoring endpoint security, and that the WDATP dashboard presents information more clearly, allowing for faster analysis. Windows Defender Antivirus events are surfaced in the same management console as WDATP, compared with having separate antivirus and EDR consoles before, simplifying overall visibility, investigation, and management. With WDATP, organizations can see the criticality of an alert, machine timelines to aid in investigation, inventory information to analyze if other machines are affected, and the prevalence of the threat across the world to assess if it is a custom attack. Organizations can also "detonate" suspicious files by sending them to a sandbox in the cloud to test their impact. These features allow security teams to quickly detect, assess, and respond to threats.
- **Improved visibility into threats and reduction of overall risk.** In addition to efficiencies in investigating and responding to threats, organizations noted that WDATP's behavioral-based approach and machine learning techniques identify more threats than prior solutions. Identifying more threats and identifying those threats quickly improves overall visibility and reduces the risk of a costly attack.
- **Reduced impact on users.** Because WDATP is built into the Windows OS, users do not see additional icons in their toolbar or experience performance issues from additional tools on their endpoints. More targeted investigation and remediation combined with earlier threat detection also reduce the scope of a threat and the amount of user productivity lost due to remediation.

"We are audited twice a year for some of our certifications, and now with WDATP, it's much easier because we can show them which machines have been enrolled, what infections we have had on the machines, and what was done to remediate because that is the standard report in the dashboard. We just run it and show the result. Before, we had to do manual work to produce the report. Now, we just click on a button and we get it."

Internal IT manager, information technology and services company

Composite Organization

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization that Forrester synthesized from the customer interviews has the following characteristics:

Description of composite. The organization is a global company with 20,000 employees and 15,000 total endpoints. Prior to WDATP, the organization was using Windows 7 on its endpoints, a comparative EDR tool, and a third-party antivirus tool. The security team consisted of three people who monitored the EDR tool and investigated and remediated threats. While the organization had not suffered a major breach, it considered its risk level to be high. Most threats entered the organization's network through user activity, and because it took longer to detect threats, often remediation would involve re-imaging machines.

Deployment characteristics. The organization follows a 1.5-year migration plan to update all of its endpoints to Windows 10 E5. It begins the migration effort with 300 endpoints belonging to power users or highly sensitive users, and then it continuously migrates additional machines. As it adds additional endpoints to WDATP, it removes them from the prior EDR tool and prior antivirus tool. The organization chooses the US data center, retains data for 180 days, and does not impose any restrictions on data shared with the cloud for analytics.

Key assumptions

15,000 endpoints

Using a prior EDR tool and third-party antivirus

Covers 100% of endpoints with WDATP

Retains data for 180 days

FORRESTER®

Financial Analysis

QUANTIFIED BENEFIT AND COST DATA AS APPLIED TO THE COMPOSITE

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Security team efficiency	$57,428	$177,584	$195,548	$430,559	$345,888
Btr	Reduced risk of a breach	$70,200	$163,800	$187,200	$421,200	$339,836
Ctr	Reduced end user impact	$11,628	$36,062	$39,710	$87,400	$70,209
Dtr	Administration efficiency	$4,241	$12,722	$14,136	$31,099	$24,990
Etr	Alternate tool cost savings	$305,188	$742,188	$807,500	$1,854,875	$1,497,508
	Total benefits (risk-adjusted)	$448,684	$1,132,355	$1,244,094	$2,825,133	$2,278,432

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of almost $2.3 million.

Security Team Efficiency

Interviewed organizations described the following security team efficiency benefits:

- Several organizations noted that WDATP caught more threats than their prior solution and provided clearer insight into those threats with better reporting, increasing visibility into current risk levels.
- WDATP provides organizations with a rich timeline to investigate the scope of threats quickly. WDATP also provides earlier detection of threats and immediate alerting, minimizing the scope of impact. The combination of early detection and fast investigation allows for more targeted remediation, providing efficiencies to both the security team and end users.
- Interviewees noted that investigation with WDATP takes “minutes.” One organization noted that it has taken advanced action on 100% of threats with WDATP, resolving threats before an attack can happen.

For the composite organization, Forrester assumes that:

- With its prior EDR tool, the organization had a 2.4% incident rate across its 15,000 endpoints, and 12% of those incidents were false positives. Each incident required, on average, 2 hours to investigate and 8 hours to remediate.
- With WDATP, the organization has a 4% incident rate and a 10% false positive rate. Each incident requires 30 minutes to investigate and 2 hours to remediate. False positives are usually unrecognized files.
- Time savings are driven by faster threat detection and faster investigation with WDATP analytics. The composite can immediately act on a threat, reducing the scope of impact and effort required to remediate the threat, and it can easily and quickly investigate affected endpoints to remediate the threat with minimal impact to users.
- The security team only opens WDATP when it receives alerts. The team saves 1,500 hours per year once all endpoints are migrated by eliminating time that was spent monitoring its prior EDR tool.

Investigate and remediate threats **4x faster** with WDATP compared with prior EDR tool

FORRESTER®

› In the table below, these time savings are converted to a monetary savings by using an average hourly security analyst salary of $62.

Risks that can affect this benefit include:

› The relative effectiveness of an organization's prior EDR tool. Forrester heard a variety of comparative impacts in terms of threat detection, false positives, and response time.

› The number of threats introduced by users. Prioritizing security training may reduce incident rates.

› The WDATP deployment timeline. Deploying WDATP faster will allow benefits to accrue more quickly. Organizations varied in the speed of deployment, with some deploying within a year and others deploying over several years based on their hardware refresh cycle.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of almost $346,000.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

Security Team Efficiency: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Average total threat alerts per year with prior EDR tool	2.4% incident rate	106	327	360
A2	False positive rate with prior EDR tool		12%	12%	12%
A3	Threat alerts that require investigation with prior EDR tool	A1*(1-A2)	93	288	317
A4	Hours to investigate a threat, prior EDR tool		2	2	2
A5	Hours to remediate a threat, prior EDR tool		8	8	8
A6	**Security hours spent with prior EDR tool**	**A3*(A4+A5)**	**930**	**2,880**	**3,170**
A7	Average total threat alerts per year with WDATP	4% incident rate	177	545	600
A8	False positive rate with WDATP		10%	10%	10%
A9	Threat alerts that require investigation with WDATP	A7*(1-A8)	159	491	540
A10	Hours to investigate a threat with WDATP		0.50	0.50	0.50
A11	Hours to remediate a threat with WDATP		2	2	2
A12	**Security hours spent with WDATP**	**A9*(A10+A11)**	**398**	**1,228**	**1,350**
A13	Average number of endpoints on WDATP during the year		4,425	13,625	15,000
A14	Average time spent per endpoint on monitoring with prior EDR tool, hours		0.10	0.10	0.10
A15	Average security hourly fully loaded compensation		$62	$62	$62
At	Security team efficiency	((A6-A12) +(A13*A14))*A15	$60,450	$186,930	$205,840
	Risk adjustment	↓5%			
Atr	**Security team efficiency (risk-adjusted)**		**$57,428**	**$177,584**	**$195,548**

Reduced Risk Of A Breach

Interviewed organizations described the following risk reduction benefits:

- Organizations noted that most of their security risk came from poor security practices by end users, particularly mobile users. The organizations wanted to minimize this risk as much as possible while still providing flexibility for users to work effectively.
- Prior to WDATP, organizations identified fewer threats, and threats that were identified had existed on the network longer and had a broader scope of impact. On average, organizations identified 1.7 times as many threats with WDATP compared with a prior EDR solution, and threats were identified early and could be remediated before an attack could escalate.

For the composite organization, Forrester assumes that:

- The average cost of a breach is $4 million, and the average probability of a breach is 13% each year.[1]
- Due to the improved ability to detect and respond to more threats faster with WDATP, the composite is able to lower its risk of a costly breach by 40% once all of its endpoints have been migrated.

Risks that can affect this benefit include:

- The Ponemon Institute data used represents global average figures. An organization's actual risk level may differ from these figures based on size, industry, region, and other factors.
- The ability for WDATP to detect threats is partially based on visibility into events on the endpoint and the ability to correlate those behaviors. Organizations can choose how long data is retained for analytics.
- Interviewees noted that most threats are introduced via user behavior. Organizations that prioritize security training for users may see lower incident rates and therefore lower risk levels.
- The WDATP deployment timeline. Deploying WDATP faster will allow for faster risk reduction due to broader endpoint coverage.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of approximately $340,000.

40% reduction in the risk of a breach compared with prior EDR tool

"The upside with WDATP is the way the analytics run on the back end. It does a very good job of pointing out exactly what's happening on the machine, what forces it, what file is hidden, what it's trying to do, what sites it's trying to hit. And it does a very good job of correlating all of those events so we can actively get right to the root of whatever is going on, and they're able to get zero-day diagnostics."

Manager of information technology, automotive company

Reduced Risk Of A Breach: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	Average cost of breach		$4,000,000	$4,000,000	$4,000,000
B2	Average probability of breach		13%	13%	13%
B3	Reduction in risk due to WDATP		15%	35%	40%
Bt	Reduced risk of a breach	B1*B2*B3	$78,000	$182,000	$208,000
	Risk adjustment	↓10%			
Btr	**Reduced risk of a breach (risk-adjusted)**		**$70,200**	**$163,800**	**$187,200**

FORRESTER®

Reduced End User Impact

Interviewed organizations described the following end user benefits:

- Prior to using WDATP, organizations struggled to identify the scope of an attack once it had happened. This would lead to more time spent on remediation, including running scans on computers and re-imaging machines more often. When machines are re-imaged, users lose access to their device and have to spend time reinstalling settings and recreating lost data.
- With WDATP, organizations have visibility into the changes that an attacker has made, allowing the security team to methodically address those specific changes without the need to run scans or re-image machines, reducing the productivity impact for end users.
- Additionally, because WDATP is built into the OS, users report fewer performance issues or interruptions. One organization mentioned a dramatic reduction in help desk calls due to WDATP, and another mentioned that updates to its prior EDR tool would often cause issues that could affect users.

> "Our expectation is that a main benefit will be that WDATP is more of an integrated stack, and so the benefit comes from less impact on the end user in terms of the client OS, less complexity on the endpoint."
>
> *Senior enterprise architect, energy company*

For the composite organization, Forrester assumes that:

- Most end user downtime is related to re-imaging of machines, including the time without a machine and the time spent on customizing re-imaged machines and recreating lost data.
- With its prior EDR tool, the composite had less visibility and addressed fewer detections, but threats took longer to identify and therefore more often resulted in re-imaging machines. Even when machines weren't re-imaged, the organization would spend more time investigating threats, scanning machines, and taking other response actions. On average, users would lose 5 hours of productive time per threat.
- With WDATP, threats are caught earlier and investigative timelines reduce response time. Security teams can identify specific changes that attackers made on machines that are affected by the attack, reducing the need to re-image a machine and allowing for faster remediation and minimal impact to users. On average, each threat with WDATP results in 1 hour of lost productivity.

1 hour of user time spent on remediation per threat with WDATP: **an 80% reduction** compared with prior EDR tool

Risks that can affect this benefit include:

- Organizations provided a range of remediation processes and impacts in both their prior environments and with WDATP, depending on visibility into the impact of threats, user behavior, and corporate policy.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of approximately $70,000.

Reduced End User Impact: Calculation Table					
REF.	**METRIC**	**CALC.**	**YEAR 1**	**YEAR 2**	**YEAR 3**
C1	Average total threat alerts with prior EDR tool	A3	93	288	317
C2	Average user remediation time spent per threat with prior EDR tool, hours		5	5	5
C3	Average total threat alerts with WDATP	A9	159	491	540
C4	Average user remediation time per threat with WDATP, hours		1	1	1
C5	User remediation time avoided, hours	(C1*C2)-(C3*C4)	306	949	1,045
C6	Average end user hourly fully loaded compensation		$40	$40	$40
Ct	Reduced end user impact	C5*C6	$12,240	$37,960	$41,800
	Risk adjustment	↓5%			
Ctr	**Reduced end user impact (risk-adjusted)**		**$11,628**	**$36,062**	**$39,710**

Administration Efficiency

Interviewed organizations described the following administrative benefits:

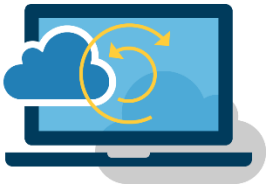
- Prior to using WDATP, the organizations were often using different security solutions from different vendors, adding complexity to administration and endpoint performance.
- Organizations mentioned that prior EDR tools were more likely to "break something" when updated, requiring more time spent on testing and remediation. Additionally, OS upgrades could result in blue screens. With WDATP, organizations spend minimal time on updates because WDATP is built in to the Windows OS.
- Organizations mentioned that their prior antivirus tool was managed in a separate console from their prior EDR tool. With WDATP, Windows Defender Antivirus events and WDATP threats are displayed in the same console, simplifying overall visibility, investigation, and management.

For the composite organization, Forrester assumes that:

- The composite used to spend time administering its prior EDR tool, including troubleshooting and updates. Updates required more testing before deployment, time spent on deployment, and time spent resolving issues post-deployment.
- With WDATP, the composite spends minimal time on administration. Continuous updates require very little security team time spent on updates, and because WDATP is built in to the Windows OS, there are very few issues that arise post-update.
- The composite maintains its prior tool during the WDATP migration, so administration savings scale as additional endpoints are migrated.

Risks that can affect this benefit include:

> "Before, any antivirus alerts would have to be integrated to a software where the software would then have to correlate with things like our prior EDR tool to get an overall view, whereas now, Microsoft is using ATP much more as a reporting agent for all ATP and malware-type threats. So you get everything through the one portal, and you get a much better view of the client machine."
>
> *Senior enterprise architect, security, energy company*



240 administration hours saved per year compared with prior EDR tool

FORRESTER®

- The administration effort required by prior tools for updates, particularly around testing pre-deployment and troubleshooting post-deployment.
- How quickly organizations remove other EDR and antivirus tools from endpoints once they have WDATP.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of approximately $25,000.

Administration Efficiency: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
D1	Administrative hours with prior EDR tool		72	216	240
D2	Average administrator hourly fully loaded compensation		$62	$62	$62
Dt	Administration efficiency	D1*D2	$4,464	$13,392	$14,880
	Risk adjustment	↓5%			
Dtr	**Administration efficiency (risk-adjusted)**		**$4,241**	**$12,722**	**$14,136**

Alternate Tool Cost Savings

Interviewed organizations described the following cost saving benefits:

- Organizations noted that prior EDR tools were similar in cost to WDATP but provided the incremental benefits listed in the sections above. As Microsoft continues to add new features to WDATP, organizations are more confident in the comparative benefit of using WDATP over other tools. Alternate tool cost savings can include both software license and hardware cost avoidances.

For the composite organization, Forrester assumes that:

- The composite was using a similar EDR tool prior to WDATP, and this tool cost $50 per endpoint per year.
- The composite was also using a third-party antivirus tool prior to WDATP and paid annual maintenance for this tool. Because the WDATP license cost includes Windows Defender Antivirus, the composite can eliminate spending on third-party tools.
- The composite removes these prior tools from endpoints at roughly the same time as WDATP is added, minimizing overlap.
- Because the migration effort occurs over the first 1.5 years, the organization can save a specific number of subscription months over each year as each endpoint is removed from the prior license.

Risks that can affect this benefit include:

- The cost of prior EDR and antivirus tools, including license costs and possible hardware costs.
- The deployment timeline for WDATP, and the amount of overlap between the prior EDR and antivirus tools and WDATP.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of almost $1.5 million.

$50 saved per year per endpoint by eliminating a prior EDR tool

Alternate Tool Cost Savings: Calculation Table					
REF.	**METRIC**	**CALC.**	**YEAR 1**	**YEAR 2**	**YEAR 3**
E1	Number of prior tool subscription months saved		53,100	163,500	180,000
E2	Average cost per endpoint per year with prior EDR tool		$50	$50	$50
E3	Prior EDR tool cost avoided	E1*(E2/12)	$221,250	$681,250	$750,000
E4	Prior antivirus cost avoided		$100,000	$100,000	$100,000
Et	Alternate tool cost savings	E3+E4	$321,250	$781,250	$850,000
	Risk adjustment	↓5%			
Etr	**Alternate tool cost savings (risk-adjusted)**		**$305,188**	**$742,188**	**$807,500**

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement Windows Defender Advanced Threat Protection and later realize additional uses and business opportunities, including:

- **Continuously improving WDATP functionality opens new doors for additional benefit.** New updates to WDATP include updates to memory and kernel sensors to improve detection and enhancements to response capabilities like the ability to isolate machines or kill and quarantine files. These updates will help to further reduce the risk posed by undetected breaches and improve investigation and remediation time.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

FORRESTER®

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Ftr	Windows Defender ATP license costs	$0	$246,750	$758,100	$834,750	$1,839,600	$1,478,007
Gtr	Deployment and management time	$5,695	$1,569	$171	$0	$7,434	$7,262
	Total costs (risk-adjusted)	$5,695	$248,319	$758,271	$834,750	$1,847,034	$1,485,269

Windows Defender ATP License Costs

For the composite organization, Forrester assumes that:

- The composite begins paying subscription costs for WDATP upon deployment of WDATP to new endpoints. The organization pays an incremental cost per user to step up from the E3 to E5 license to access WDATP.
- The composite begins its deployment with 300 endpoints at the start of Year 1 via group policy. These endpoints belong to users who are either power users or otherwise considered more sensitive users. The composite assumes that each user has one endpoint.
- In months two through 12 of the first year, 750 additional endpoints are added each month. In months one through five of Year 2, 1,050 endpoints are added in each month. In month six, the remaining 1,200 endpoints are added to complete the migration.

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of almost $1.5 million.

Risks that can affect this cost include:

- Software license costs are variable from organization to organization based on differing licensing options, vendor discounts based on volume or other products licensed from that vendor, and other factors.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $1.48 million.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

Windows Defender ATP License Costs: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
Ft	Windows Defender ATP license costs		$0	$235,000	$722,000	$795,000
	Risk adjustment	↑5%				
Ftr	**Windows Defender ATP license costs (risk-adjusted)**		**$0**	**$246,750**	**$758,100**	**$834,750**

Deployment And Management Time

Interviewed organizations mentioned the following deployment and management efforts:

- Prior to deploying WDATP, organizations spent time on discussions with Microsoft, internal planning, configuration and testing, and training.

› All interviewees noted that very little time was spent on deploying ATP to endpoints and that administration of WDATP was minimal.

For the composite organization, Forrester assumes that:

› The composite spent a total of 80 hours on upfront planning, testing, and configuration. The organization spent 20 hours in Year 1 on additional testing as more endpoints were enrolled with WDATP.

› Time spent on deployment was minimal, with 30 minutes spent on the first 300 machines, and then 3 hours over the course of Year 1 and 2.5 hours in Year 2.

› The three-person security team participated in a 1-hour training upfront with Microsoft.

Risks that can affect this cost include:

› Whether organizations use WDATP out of the box or require a customization deployment for their environment.

› The pace of an organization's Windows 10 migration.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $7,262.

1.5 years
Total deployment timeline for 15,000 endpoints

Deployment And Management Time: Calculation Table

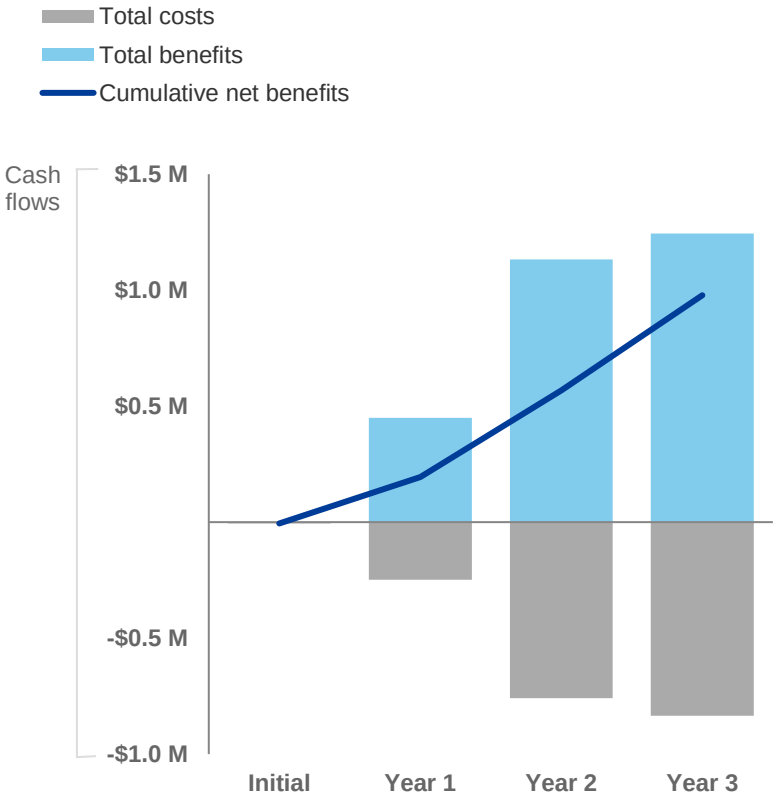
REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
G1	Planning, testing, evaluation time, hours		80	20		
G2	Training time, hours		3			
G3	Deployment time, hours		0.50	3.00	2.50	
G4	Average hourly fully loaded compensation		$62	$62	$62	$62
Gt	Deployment and management time	(G1+G2+G3)*G4	$5,177	$1,426	$155	$0
	Risk adjustment	↑10%				
Gtr	**Deployment and management time (risk-adjusted)**		**$5,695**	**$1,569**	**$171**	**$0**

FORRESTER®

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI and NPV for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI and NPV values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($5,695)	($248,319)	($758,271)	($834,750)	($1,847,034)	($1,485,269)
Total benefits	$0	$448,684	$1,132,355	$1,244,094	$2,825,133	$2,278,432
Net benefits	($5,695)	$200,365	$374,085	$409,344	$978,099	$793,163
ROI						53%

FORRESTER®

Microsoft Windows Defender Advanced Threat Protection: Overview

The following information is provided by Microsoft. Forrester has not validated any claims and does not endorse Microsoft or its offerings.

Windows Defender Advanced Threat Protection ATP helps enterprise customers detect, investigate, and respond to advanced attacks and data breaches on their networks.

Windows Defender ATP combines sensors built in to the operating system with a powerful security cloud service enabling security operations to detect, investigate, contain, and respond to advanced attacks against their network.

Windows Defender ATP is powered by behavioral sensors built into Windows 10. The security analytics cloud detects attacks that have made it past all other defenses, using behavioral and machine learning detections over new and historical information to identify attacks, fueled by a combination of unparalleled threat optics and deep OS security and big data expertise.

The Windows Defender ATP advantage:

Detecting the undetectable	**Built in, not bolted on**	**Single pane of glass for windows security**	**The power of the Microsoft graph**
Sensors built deep into the operating system kernel, Windows security experts, and unique optics from over 1 billion machines and signals across all Microsoft services	Agentless with best-in-class performance, cloud powered, easy management with no deployment	Explore six months of rich machine timeline that unifies security events from Windows Defender ATP, Windows Defender Antivirus and Windows Defender Device Guard; quickly pivot to explore files, users, domains, and IPs	Leverages the Microsoft Intelligence Security Graph to integrate detection and exploration with Office 365 ATP subscription, to track back and respond to attacks arriving via email attachments

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

Total Economic Impact Approach

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

FORRESTER®

Appendix B: Endnotes

[1] Source: “2016 Cost of Data Breach Study: Global Analysis,” Ponemon Institute (https://securityintelligence.com/cost-of-a-data-breach-2016/).