FORRESTER®

The Total Economic Impact™ Of Broadcom VMware vDefend

Cost Savings And Business Benefits Enabled By vDefend

A Forrester Total Economic Impact™ Study
Commissioned By Broadcom VMware, March 2025

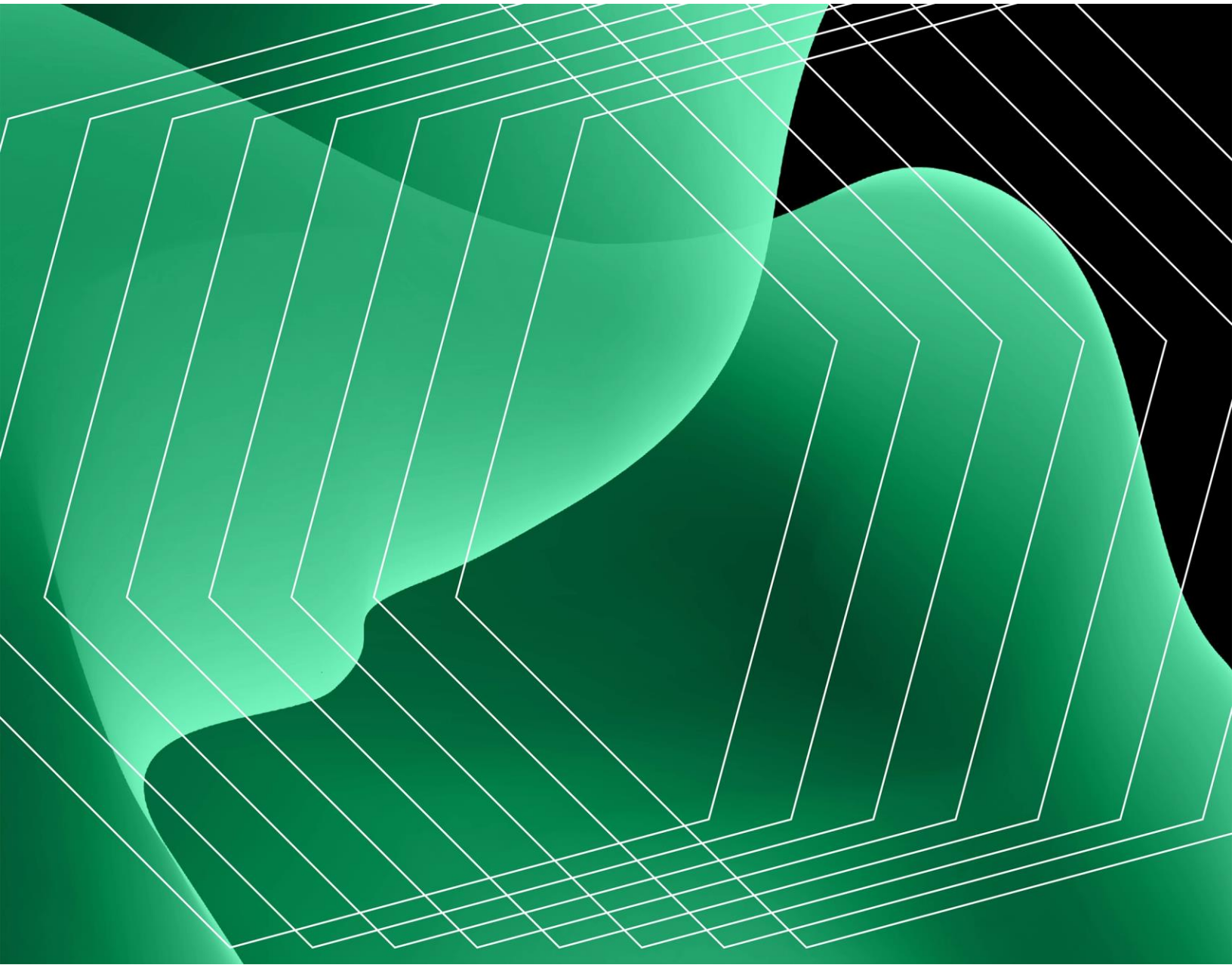


Table Of Contents

Consulting Team:

Leigh Greene

Sean Owens

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

To protect private cloud workloads — critical and noncritical — from malware and ransomware attacks, enterprises must prioritize zero-trust lateral security in addition to perimeter protection. Organizations need application and threat visibility, multilevel segmentation, and restricted east-west threat movement to achieve comprehensive lateral security. vDefend for zero-trust lateral security offers enterprises a full-stack, integrated security solution to implement multilayer defense, in-depth security for all application workloads with a single pane of glass — optimizing operational efficiency at the speed of applications.

VMware vDefend ("vDefend") is a software-defined, distributed security solution that offers organizations the ability to protect networks from ransomware and advanced malware threats — and their costly impact — from a single platform with a single console. The VMware vDefend Firewall solution includes a Layer 7 distributed firewall; gateway firewall; and Security Intelligence, a visibility and policy recommendation engine. The VMware vDefend Advanced Threat Prevention (ATP) solution offers distributed and gateway intrusion detection and prevention systems (IDS/IPS), malware prevention, network traffic analysis (NTA), and network detection and response (NDR).

Broadcom VMware commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying vDefend.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of vDefend on their organizations.

Return on investment (ROI)
116%

Net present value (NPV)
$3.11M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four decision-makers with experience using vDefend. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that has an annual revenue of $10 billion per year, 20,000 employees, and five data centers powering global operations.

TEI Composite Assumptions

$10 billion annual revenue
20,000 employees
5 data centers
Phased vDefend deployment

Interviewees said that prior to using vDefend, their organizations struggled to detect and identify threats in a timely way. They lacked the tools and resources to improve their network visibility, and this often meant a siloed and resource-heavy approach to security. To keep pace with the increasing complexity of network attacks and establish a zero-trust framework, interviewees needed to protect their networks using a more sophisticated, collaborative, and automated solution. Their organizations needed to scale their networks without making significant investments in hardware or added personnel.

After the investment in vDefend, interviewees' organizations could deploy the software solution quickly and saw improved visibility into their networks. They quickly identified internal threats and took steps to fortify their infrastructure with effective network rules to prevent future malware attacks. With efficient deployment of vDefend, interviewees' organizations improved their security profiles and documentation processes, reduced the risk and cost of data breaches, and saved security operations teams' time without needing to invest in multiple hardware and software solutions. Strengthening their organization's lateral security had additional benefits, like fewer increases in cyber insurance premiums and improved collaboration and proactivity among their IT teams.

> "Having a single pane of glass across our complete set of workloads gives us great visibility. We can easily get the information we need and make necessary changes, even with a smaller team. It absolutely saves us time and dollars."
>
> IT TECHNICAL MANAGER, HEALTHCARE

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Reduced risk of security breaches and associated costs by 40%.** Implementing vDefend allows the composite to improve its overall network security. With increased visibility into east-west traffic, plus the use of an automated, centralized tool to quickly pinpoint and isolate any foreign presence in its data centers, the composite decreases the impact of security incidents and fortifies its networks against future attacks. The composite uses Security Intelligence, a vDefend capability, to gain knowledge about network infiltrators and, from these experiences, can design granular security rules to prevent future breaches and costly outages. The composite organization saves $933,000 during Years 1, 2, and 3 due to reduced risk and cost of security breaches.
- **Improved security operations team productivity by 25%.** The vDefend solution facilitates a variety of network security tasks. vDefend lets the composite organization efficiently define firewall rules and policies and easily apply them across multiple environments so security operations teams don't have to start over with each application update. Threat mitigation and identification are also much faster with vDefend, since teams can quickly visualize any foreign presence in the network. From there, the security operations staff can analyze threats using signatures and behavior-based techniques, find the most efficient way to contain them, and minimize network impact. The composite organization saves $1.66 million over three years from improved security operations productivity.

- **Saved security hardware costs of $750,000 per data center deployed.** Organizations can financially benefit from their investment in vDefend by reducing capital expenditures. Instead of buying expensive taps and other costly pieces of physical hardware, companies can instead leverage vDefend's software-defined distributed firewall and dynamic threat protection capabilities to secure networks and modernize their infrastructure. The composite organization can save hundreds of thousands of dollars once it repurposes or sunsets some of its most expensive centralized security devices. It ultimately saves $2.69 million on security hardware for its five data centers over the three-year period.
- **Avoided increases in cyber insurance premiums.** With the help of vDefend, the composite can demonstrate its improved security risk profile to cyber insurance companies and benefit from flat or smaller increases in premiums. The composite organization saves $502,000 by avoiding premium increases over the three-year period.

> "Instead of having a central group that manages core network devices and policies [like we did prior to vDefend], we're now able to be more granular and provide self-service access to specific sections for application or security owners to be able to manage policies themselves."
>
> SOLUTIONS LEADER, TECHNOLOGY SERVICES

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified for this study include:

- **Improved proactivity and confidence within IT security teams.** Previously, the composite's teams were often reactive to network threats; however, vDefend has helped them become more sophisticated and proactive with network security. Instead of creating simple firewall rules between two servers, the composite's teams can instead focus on high-level system design and metadata rules to help them stay ahead of potential threats. The evolution from a manual, one-off approach to a preventative

network defense strategy imbues the security operations teams with confidence as it develops a strategic network security approach.

- **Increased collaboration to break down silos.** Before vDefend, the composite had siloed approaches to network security. After implementing vDefend, the composite benefits from having a stack of multiple detection technologies in a single console, making management, self-service, and interteam collaboration easier. While this consolidation offers some quantifiable productivity benefits (detailed in Benefit B), there is also an added benefit of collaboration, making security operations teams' jobs easier. Application owners and firewall teams all have the same network visibility and access and therefore can work together seamlessly.
- **Better regulatory alignment and compliance.** The composite organization benefits from vDefend's ability to help with network security documentation, which proves helpful with audits or compliance issue resolution. Before vDefend, the composite had security documentation that lacked detail and contained unclear protocols. The ability to present clear information to auditors showing separations and rules is an improvement over the composite's previous solution.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **VMware vDefend licensing and professional services costs.** Software licensing costs for the vDefend solution include Firewall and ATP costs. The firewall solution includes a Layer 7 distributed firewall, gateway firewall, and Security Intelligence. ATP includes distributed and gateway IDS/IPS, malware prevention, NTA, and NDR. The composite also uses VMware professional services costs to help with implementation and ongoing management. The total cost over the three-year period is $2.02 million.
- **Planning, implementation, and training costs.** The costs for the composite organization to implement vDefend include planning activities, implementation work, network mapping, change management resources, and solution training. The total cost over the three-year period is $347,000.
- **Ongoing management costs.** There are costs that the composite organization incurs for ongoing management of vDefend. After deployment, the solution requires some resources to manage the represented platform, including firewall rule updates, network monitoring, threat identification, and issue resolution. The total cost over the three-year period is $314,000.

The representative interviews and financial analysis found that a composite organization experiences benefits of $5.79 million over three years versus costs of $2.68 million, adding up to a net present value (NPV) of $3.11 million and an ROI of 116%.

Return on investment (ROI)

116%

Benefits PV

$5.79M

Net present value (NPV)

$3.11M

Payback

8 months

Benefits (Three-Year)

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in vDefend.

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 vDefend can have on an organization.

DISCLOSURES
Readers should be aware of the following:

This study is commissioned by Broadcom VMware and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in vDefend.

Broadcom VMware reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Broadcom VMware provided the customer names for the interviews but did not participate in the interviews.

Due Diligence
Interviewed Broadcom VMware stakeholders and Forrester analysts to gather data relative to vDefend.

Interviews
Interviewed four people at organizations using vDefend to obtain data about costs, benefits, and risks.

Composite Organization
Designed a composite organization based on characteristics of the interviewees' 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 interviewees.

Case Study
Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

KEY CHALLENGES

Prior to implementing vDefend, interviewees' organizations found it difficult to improve network security and visibility without investing significant resources. Application owners could not manage policies on their own, and the central firewall teams often became a bottleneck as they were overwhelmed with network requests.

The interviewees noted how their organizations struggled with common challenges, including:

- **Lack of visibility into network traffic and potential threats.** All interviewees struggled with gaining visibility into their network security operations and were unable to pinpoint and identify issues with granularity and purpose. The solutions leader at the technology services company described their organization's visibility challenges prior to vDefend: "It was like having multiple islands in an archipelago with no bridges. In that scenario, it makes it hard to have a holistic, broad view about what's happening in the enterprise. We were always forced to stitch data from disparate systems together just to be able to get a basic understanding of what was happening in our network."
- **A manual, time-consuming approach to network security.** Before vDefend, few of the interviewees' organizations had lateral security configured with logical, automated rule sets, which impacted scalability. Many instances involved manual and one-off requests that were not reflective of a cohesive approach to security and were unhelpful in establishing a zero-trust architecture. These organizations needed a solution that could be deployed quickly to keep up with their dynamic security landscape. The IT automation manager at the government services organization described one example of how time-consuming certain common server requests were before vDefend: "Every one of our servers needs access to the time server to keep time correct and consistent across the network. Before vDefend, there would be instances where the time would drift off in one of the servers. People wouldn't even realize it until it was too late, and then they would have to make a request to the central firewall team to gain access to the time server."
- **An inability to rely solely on perimeter security.** All interviewees discussed the increasing sophistication and nuance of attacks from bad actors. Having a secure perimeter was not enough to protect their organization's networks against ransomware and other security threats. The senior infrastructure engineer at the financial services

company described their organization's previous reliance on a strong perimeter: "Everyone relied on the perimeter. They'd say, 'Yeah, our perimeter is super secure.' The thing is, it's the users and the applications inside that are the weak points or the low-hanging fruit. East-west traffic became a main focal point for everyone because the perimeter was no longer the issue that we needed to solve for."

> "The previous methodology we had was akin to having a hard candy shell with a soft inside. We had a pretty good security posture from the outside, but it was all north-south."
>
> **IT TECHNICAL MANAGER, HEALTHCARE**

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the interviewees' organizations, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

- **Description of composite.** The composite organization is a for-profit, global company with headquarters in the United States. The annual revenue is $10 billion, and the company employs 20,000 people internationally. The organization invests in cyber insurance as part of its overall network security strategy, and it uses five data centers.
- **Deployment characteristics.** The composite organization deploys the vDefend solution in phases. It implements vDefend in two of its five data centers in Year 1, two data centers in Year 2, and the last data center in Year 3. The licensing costs and related implementation costs are also prorated based on this phased approach. The composite organization uses VMware vDefend Firewall with ATP. The VMware vDefend Firewall includes distributed firewall, gateway firewall, and Security Intelligence. ATP includes distributed and gateway IDS/IPS, malware prevention, NTA, and NDR.

Key Assumptions

$10 billion annual revenue

20,000 employees

5 data centers

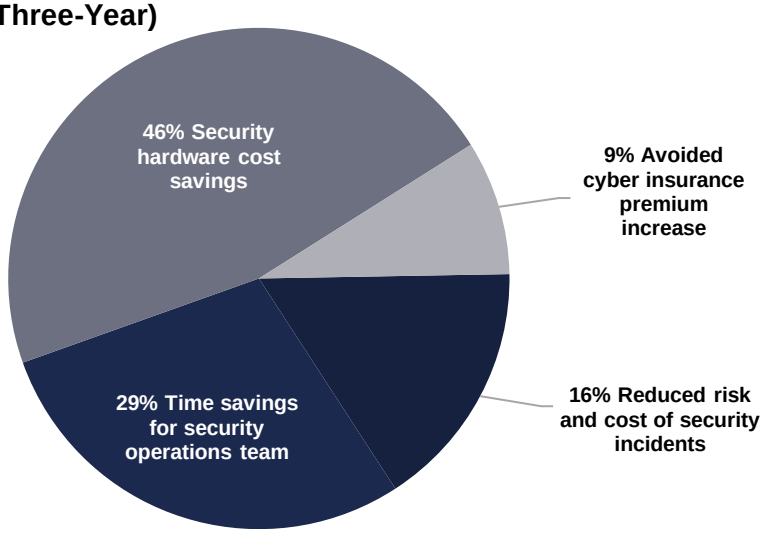
Phased vDefend deployment

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Reduced risk and cost of security incidents	$196,729	$432,804	$527,234	$1,156,767	$932,652
Btr	Time savings for security operations team	$374,400	$748,800	$936,000	$2,059,200	$1,662,437
Ctr	Security hardware cost savings	$1,275,000	$1,275,000	$637,500	$3,187,500	$2,691,773
Dtr	Avoided cyber insurance premium increase	$172,500	$212,175	$226,541	$611,216	$502,373
	Total benefits (risk-adjusted)	$2,018,629	$2,668,779	$2,327,275	$7,014,683	$5,789,235

Benefits (Three-Year)



REDUCED RISK AND COST OF SECURITY INCIDENTS

Evidence and data. vDefend helps organizations improve their security posture, thereby reducing their risk of experiencing adverse security incidents and costly breaches.

- Interviewees discussed how vDefend helped improve their overall security profile. Security teams could quickly identify more security threats than they could in the past, then isolate those threats to minimize the impact of breaches and reduce overall network security costs.
- The solutions leader at the technology services company summarized the security-enhancing benefits of vDefend as follows: “One of the main benefits is the overall visibility everywhere in your network and environment. That, plus the ability to quickly respond to threats, issues, breaches, and other problems within the network rapidly instead of after the fact.”
- The IT automation manager at the government services organization said, “If, for any reason, it’s determined that we have a foreign presence in our data center, we now have a tool to encapsulate that vulnerable part of the network.”
- The IT technical manager at the healthcare organization described the unique impact that breaches have on revenue: “For example, if we have a breach, we have to notify our electronic medical record vendor, and they will immediately turn off the connectivity between us. The soonest the vendor releases an organization like ours after having a breach is typically 10 days. So, we would go a minimum of 10 days without our medical record system, which means no patient registrations and no recording of treatment, which means that billing is essentially shut down.”

40%

Reduced risk of breach or security incident due to vDefend

Modeling and assumptions. For the financial analysis, Forrester assumes the following:

- This benefit outlines the cost savings due to reduced risk and impact of data breaches and does not reflect any time savings or productivity improvements garnered with vDefend. Those benefits will be discussed in Benefit B.

- According to Forrester's 2024 Security Survey, 62% of security decision-makers at enterprise organizations estimated they experienced one or more breaches in the past year.[2] This data point and the data represented in A2 and A3 below outline the cost savings for the composite organization in this benefit.

> "You can't protect what you can't see. Since implementing vDefend, we've actually been able to see an uptick in attempted threats, so we now have much greater visibility."
>
> SOLUTIONS LEADER, TECHNOLOGY SERVICES

Risks. The following risks can potentially impact this benefit:

- Every organization's network is different with varying levels of risk and security protocols. Cost savings could vary depending on the industry, network structure, and level of data sensitivity.
- In addition to vDefend, organizations could attribute cost savings to other security measures, such as improved security training or enhanced employee skills and experience.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $933,000.

Reduced Risk And Cost Of Security Incidents					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Likelihood of experiencing one or more breaches per year	Forrester research	62%	62%	62%
A2	Mean cumulative cost of breaches	Forrester research	$3,733,000	$3,733,000	$3,733,000
A3	Percentage of breaches related to physical or virtual network workloads now managed by vDefend	Forrester research	25%	55%	67%
A4	Annual risk exposure addressable with vDefend	A1*A2*A3	$578,615	$1,272,953	$1,550,688
A5	Reduced risk and cost of security incidents	Interviews	40%	40%	40%
At	Reduced risk and cost of security incidents	A4*A5	$231,446	$509,181	$620,275
	Risk adjustment	↓15%			
Atr	Reduced risk and cost of security incidents (risk-adjusted)		$196,729	$432,804	$527,234
	Three-year total: $1,156,767			**Three-year present value: $932,652**	

TIME SAVINGS FOR SECURITY OPERATIONS TEAM

Evidence and data. The vDefend platform, including ATP, allows network security personnel to complete tasks more efficiently via a single console and save time with network monitoring and threat identification.

- Interviewees emphasized how vDefend helped their organizations increase productivity and enhance scalability while improving their strong security posture. They saved time with vDefend when defining firewall rules, testing and validating network policies to apply across their environments, and identifying and isolating threats within their network.
- The senior infrastructure engineer at the financial services company explained how vDefend helped their teams save time by having its distributed firewall within the same consolidated technology stack as the IDS/IPS, NTA, NDR and Security Intelligence features: “Overall management is a lot easier with vDefend. Instead of having multiple device interfaces, we now have one centralized console. Being able

to manage from a central place and have a holistic view of your network is definitely a time saver."

- The IT technical manager at the healthcare company described the time-saving aspects of vDefend: "In a 24/7/365 operation, it would take us two months to be able to get enough downtime windows to be able to test and validate a new policy. Now, we can make a policy, add machines to the group, and then the policy is in place. With vDefend, you can do something in minutes that would otherwise take far more time to test and validate."

> "A big bottleneck was having the firewall team make all the judgment calls for what traffic is valid or not. Now this is with the application owners, and it's a huge leap in awareness and bandwidth."
>
> **IT AUTOMATION MANAGER, GOVERNMENT SERVICES**

Modeling and assumptions. For the financial analysis, Forrester assumes the following:

- vDefend helps the composite improve efficiency by 25% for all security and operations tasks that it facilitates.
- The composite organization can save 2.5 FTEs in Year 1, 5 FTEs in Year 2, and 6.25 FTEs in Year 3. These savings increase as the composite organization expands its use of vDefend to all five data centers by Year 3.

> **25%**
>
> Security team time savings due to vDefend efficiency gains

Risks. The following risks can potentially impact time savings benefits:

- The size of the security team could vary, which would affect the number of FTEs benefiting from vDefend time savings and therefore impact the total cost savings.
- The average fully burdened hourly rate for a security operations FTE could vary based on experience level and geographic location.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.7 million.

Time Savings For Security Operations Team					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	IT security operations FTEs	Composite	10	20	25
B2	Percentage of time saved due to faster security task completion	Interviews	25%	25%	25%
B3	Fully burdened hourly rate for a security operations FTE	Composite	$80	$80	$80
Bt	Time savings for security operations team	B1*B2*B3*2080	$416,000	$832,000	$1,040,000
	Risk adjustment	↓10%			
Btr	Time savings for security operations team (risk-adjusted)		$374,400	$748,800	$936,000
	Three-year total: $2,059,200		**Three-year present value: $1,662,437**		

SECURITY HARDWARE COST SAVINGS

Evidence and data. vDefend can help organizations reduce their capital expenditures and decrease the hardware and physical devices needed to maintain network security.

- Interviewees noted how their organizations could consolidate and begin sunsetting physical security hardware by using vDefend and its software-defined firewall and threat protection capabilities.
- The senior infrastructure engineer at the financial services company described how vDefend helped them save money on physical hardware: “One of our apps had three dedicated demilitarized zones with 30 pieces of physical networking gear that we

were able to replace with just six. … We've probably been able to save a few hundred thousand dollars per year for each data environment."

- The solutions leader at the technology services company outlined how vDefend has helped their organization save money on large capital expenditures related to security: "With vDefend, we can now define the apps, see our flows, and make tactical decisions as the application owner, which is huge. We no longer have to put expensive taps everywhere in the data center, and those are big central devices that cost a lot of money. Everything with vDefend is built-in software that comes as huge value to our teams."

Modeling and assumptions. For the financial analysis, Forrester assumes the following:

- As described in earlier benefits, the composite organization uses a phased approach to implement vDefend across its five data centers. The security hardware savings reflect this deployment pattern.
- The types of hardware represented in these savings include routers, firewalls, switches, taps, intrusion detection systems, and other physical networking devices.

$750,000

Cost savings per data center due to reusing, retiring, or reselling security hardware

Risks. The following risks can potentially impact security hardware cost savings benefits:

- The implementation schedule could differ, affecting when the composite organization can capitalize on security hardware cost savings.
- Factors including depreciation, hardware age, and the types of devices being retired can impact the size of this benefit's cost savings.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.7 million.

Security Hardware Cost Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Security hardware cost savings per data center	Interviews	$750,000	$750,000	$750,000
C2	Number of data centers protected by vDefend	Composite	2	2	1
Ct	Security hardware cost savings	C1*C2	$1,500,000	$1,500,000	$750,000
	Risk adjustment	↓15%			
Ctr	Security hardware cost savings (risk-adjusted)		$1,275,000	$1,275,000	$637,500
	Three-year total: $3,187,500			**Three-year present value: $2,691,773**	

AVOIDED CYBER INSURANCE PREMIUM INCREASE

Evidence and data. This final benefit section shows how vDefend can help organizations improve network security and avoid increases in cyber insurance premiums.

- Interviewees noted how vDefend helped effectively streamline and document security protocols. This allowed their organizations to demonstrate security improvements to cyber insurance companies during risk level assessments that determined premium payments.
- The IT technical manager at the healthcare organization said: “I know with the efforts we’ve made, including implementing vDefend, we have not seen cyber insurance premium increases. A significant factor, which our Head of Risk has been quite happy with.”

10%

Avoided cyber insurance premium increases in Year 1

Modeling and assumptions. Forrester assumes that the composite invests in cyber insurance for coverage in the event of a security breach. Although not all enterprise companies invest in

cyber insurance, the composite organization maintains coverage. It has also implemented processes and technology to adequately manage and audit security in other areas of the business that might affect cyber insurance premiums.

Risks. The following risks can potentially impact the cyber insurance cost savings benefit:

- The specific cyber insurance coverage an organization needs can vary depending on its industry, the type of data stored within its network, and the revenue impact of a potential breach.
- Insurance premium rate increases in the cyber insurance industry have been volatile over the last several years. Although they cannot be predicted with certainty, insurance premium increases can be estimated based on prior industry trends.
- There could be other factors that contribute to the composite organization's ability to avoid cyber insurance premium increases , such as market conditions, previous security incidents, and security protocols that can't be directly tied to vDefend.

Results. To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $502,000.

Avoided Cyber Insurance Premium Increase					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Annual commercial cyber insurance premiums related to vDefend assets and data	Composite	$2,300,000	$2,357,500	$2,416,438
D2	Expected avoided increase in cyber insurance premiums as a result of vDefend	Composite	10.0%	12.0%	12.5%
Dt	Avoided cyber insurance premium increase	D1*D2	$230,000	$282,900	$302,055
	Risk adjustment	↓25%			
Dtr	Avoided cyber insurance premium increase (risk-adjusted)		$172,500	$212,175	$226,541
	Three-year total: $611,216			**Three-year present value: $502,373**	

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Improved proactivity and confidence within IT security teams.** Interviewees agreed that vDefend helped change their teams' operations, increasing their sophistication and allowing them to dedicate time to strategic initiatives instead of tactical ones. The IT automation manager at the government services organization described their team's enlightenment with vDefend: "Since we got going with vDefend, the team has started to see the light. Instead of creating firewall rules from IP-A to IP-B, the team is starting to implement more network metadata rules that apply across multiple environments. The team's overall work pattern has gone from being reactive to being proactive. They're spending more time on higher level design, and less time on simply configuring rules."
- **Increased collaboration to break down silos.** Interviewees explained that vDefend's ability to consolidate multiple technologies within a single stack through ATP helped their organizations bring disparate security and IT teams together. Interviewees could not quantify time savings through improved collaboration but noted that their organizations often felt siloed and disconnected before vDefend. The senior infrastructure engineer at the financial services company discussed how different teams now worked together: "Back in the day, before vDefend, everything was very much siloed. Whereas now, the teams can be much more blended. It's not you, the firewall guy, and me, the networking guy. Those barriers don't exist the way they used to since we're now able to work within the same platform to improve our network security."

> "The overall story of vDefend is powerful, and ATP enhances microsegmentation by adding an additional layer of security with distributed IDS/IPS. vDefend has upgraded the security of our applications, which auditors recognize as a huge benefit."
>
> SOLUTIONS LEADER, TECHNOLOGY SERVICES

- **Better regulatory alignment and compliance.** Interviewees discussed how vDefend improved their ability to document and detail the firewall rules and security protocols within their network. Having their security infrastructure clearly outlined was invaluable during any corporate audit or compliance discussion. The senior infrastructure engineer at the financial services company described how vDefend first allowed them to improve and clarify their documentation, which became helpful when presenting the information to auditors: “Being able to showcase that our organization is creating the right separations and maintaining security protocols through automation is obviously huge. Anything you can do to make it easier for auditors is obviously a lifesaver.”

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement vDefend and later realize additional uses and business opportunities, including:

- **Modernization of network infrastructure to increase future growth and scalability.** Interviewees referenced how vDefend helped their organizations streamline, scale, and modernize their network security infrastructure. Beyond the time-saving benefit quantified in the financial model, interviewees cited how vDefend allowed their teams to grow their network and enhance their security profile while maintaining the same resources into the future. The senior infrastructure engineer at the financial services organization explained their experience: “With the virtualization aspect of bringing in vDefend, it allows us to consolidate and modernize our organization. Moving forward into the future, it allows us to be more effective and more agile without the cost of additional overhead and infrastructure to maintain our network security. It’s a vital piece of our business — we can’t do without it at this point.”
- **Improved vendor and partner organizations’ security protocols to further fortify network protection.** Enterprise organizations have complex networks that often connect to and integrate with data sources belonging to their partner organizations. Interviewees spoke about how implementing vDefend and tightening their lateral security in-house helped spur their vendor and partner organizations to improve their documentation and security protocols. The IT technical manager at the healthcare organization described it as follows: “After seeing our experience with vDefend, hopefully more organizations will use this tool. Now that we’ve started down this realm, our

vendors are beginning to follow suit with playbooks and tightened security protocols of their own. This is another way we will continue to harden our environment by strengthening those adjacent to ours."

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	vDefend costs	$456,750	$808,500	$997,500	$0	$2,262,750	$2,016,130
Ftr	Planning, implementation, and training costs	$148,890	$148,890	$76,020	$0	$373,800	$347,071
Gtr	Ongoing operations costs	$0	$84,084	$134,534	$168,168	$386,786	$313,973
	Total costs (risk-adjusted)	$605,640	$1,041,474	$1,208,054	$168,168	$3,023,336	$2,677,174

VDEFEND COSTS

Evidence and data. This cost section details the software licensing and professional services costs for the vDefend solution. This includes all costs paid to Broadcom VMware for software and services but does not include internal resources used to implement and operate vDefend.

- The licensing costs for vDefend with ATP are based on an organization's size and network complexity.
- Professional services costs are also based on an organization's size and network complexity.
- Pricing may vary. Contact Broadcom VMware for additional details.

> "When you think about the areas we've saved — whether it's ongoing costs or hardware refreshes where we would've needed to spend $300,000 for new hardware — the cost of vDefend is a fraction of these savings."
>
> SENIOR INFRASTRUCTURE ENGINEER, FINANCIAL SERVICES

Modeling and assumptions. For the financial analysis, Forrester assumes the following:

- While benefits are measured for the year they are enabled, it is assumed that license costs are prepaid in the previous year. So license costs measured during the initial period enable benefits captured in Year 1; costs in Year 1 enable benefits in Year 2, and so on. While costs may continue into Year 3 and beyond, because the cost/benefit analysis covers three years, they are not included. License costs in Year 3 would apply to benefits enabled in Year 4, which is outside the analysis period.
- To migrate five data centers over the three-year period, the composite organization has licensing terms for $900,000 per year until it completes full deployment. However, licensing costs are adjusted in the initial period and Year 1 — to 40% and 80% of the total, respectively — based on the number of data centers that have deployed vDefend.
- The professional services costs reflect vDefend implementation time and effort for the five data centers considering the composite organization's deployment schedule as well as learnings and efficiencies gained from the initial period and Year 1 implementations.
- Costs in Year 2 assume the composite organization will have implemented vDefend by the start of Year 3 at all five of its data centers.

Risks. The following risks can potentially impact the vDefend costs:

- The composite organization could opt to pay for licensing and professional services fees upfront or commit to a different proration schedule.
- The composite organization could choose to outsource more professional services to Broadcom VMware to help with implementation or ongoing management.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.0 million.

vDefend Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Licensing costs for three-year term of vDefend	Composite	$360,000	$720,000	$900,000	
E2	Professional services for vDefend	Composite	$75,000	$50,000	$50,000	
Et	vDefend costs	E1+E2	$435,000	$770,000	$950,000	
	Risk adjustment	↑5%				
Etr	vDefend costs (risk-adjusted)		$456,750	$808,500	$997,500	
	Three-year total: $2,262,750			**Three-year present value: $2,016,130**		

PLANNING, IMPLEMENTATION, AND TRAINING COSTS

Evidence and data. This cost section discusses the resources required for the organization to initially deploy the vDefend solution, including planning activities, implementation work, change management, and training.

- Interviewees' organizations often implemented vDefend in phases rather than deploying the solution simultaneously across their entire global network.
- Most interviewees were customers of Broadcom or VMware before the merger of these two companies. With the subsequent changes and improvements to the vDefend solution during the intervening years, there may be variations in how new customers dedicate resources to planning, implementation, and training.

> "The vDefend platform is worth every penny that we've spent on the licensing and acquiring the knowledge of how to use it. I would say it's invaluable."
>
> IT TECHNICAL MANAGER, HEALTHCARE

Modeling and assumptions. For the financial analysis, Forrester assumes the following:

- The composite organization's planning and implementation costs are spread over the three-year period, matching its data center deployment schedule. The first 40% of the total is spent in the initial period (first two of five data centers deployed), the second 40% is spent in Year 1 (two additional data centers deployed), and the final 20% is spent in Year 2 (final data center deployed).
- The security team planning and implementation process takes 20% of their time over the 20-week deployment period, which equates to 8 hours per person per week.
- The IT team also dedicates resources to planning and implementation, taking 15% of their time over the 20-week deployment period, which equates to 6 hours per person per week.

Risks. The following risks can potentially impact planning, implementation, and training costs:

- The composite organization could elect to use a professional services organization or outsource a greater portion of its implementation work to VMware professional services, which would change the number of internal resources dedicated to planning and implementation.
- The average fully burdened hourly rate for a security operations FTE or an IT admin FTE could vary based on experience level and geographic location.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $347,000.

Planning, Implementation, And Training Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Security team FTEs involved in planning and implementation	Composite	6	6	6	
F2	Percentage of time dedicated to planning and implementation	Interviews	20%	20%	10%	
F3	Time spent on implementation (weeks)	Interviews	20	20	20	
F4	Fully burdened hourly rate for a security operations FTE	Composite	$80	$80	$80	
F5	**Subtotal: security team planning and implementation costs**	**F1*F2*F4* 2080/52*F3**	**$76,800**	**$76,800**	**$38,400**	
F6	IT admins involved in planning and implementation	Composite	5	5	5	
F7	Percentage of time dedicated to planning and implementation	Interviews	15%	15%	8%	
F8	Fully burdened hourly rate for an IT admin FTE	Composite	$75	$75	$75	
F9	**Subtotal: IT planning and implementation costs**	**F6*F7*F3* 2080/52*F8**	**$45,000**	**$45,000**	**$24,000**	
F10	**Subtotal: other planning and implementation costs**	**Composite**	**$20,000**	**$20,000**	**$10,000**	
Ft	Planning, implementation, and training costs	F5+F9+F10	$141,800	$141,800	$72,400	$0
	Risk adjustment	↑5%				
Ftr	Planning, implementation, and training costs (risk-adjusted)		$148,890	$148,890	$76,020	$0
	Three-year total: $373,800			**Three-year present value: $347,071**		

ONGOING OPERATIONS COSTS

Evidence and data. This cost section outlines the resources required for ongoing vDefend management.

- Once interviewees' organizations implemented vDefend, they needed IT administrative and security operations resources for platform management.
- Interviewees spoke of the ease with which they can manage the platform. The implementation and change management components were a more significant resource investment than the resources required for ongoing management.

Modeling and assumptions. For the financial analysis, Forrester assumes the following:

- The team responsible for managing vDefend spends 4 hours per person per week. This is equivalent to one FTE by Year 3.

- The average fully burdened hourly rate for this FTE is a blended average of security operations personnel and IT administrative personnel involved in ongoing vDefend management.
- The composite scales ongoing management resources based on the data center migration outlined in Benefit C.

Risks. The following risks can potentially impact ongoing operations costs:

- The resources required for ongoing management of vDefend could vary based on the complexity and growth of the composite organization's network.
- The average fully burdened hourly rate for an FTE within this benefit could vary based on experience level and geographic location.

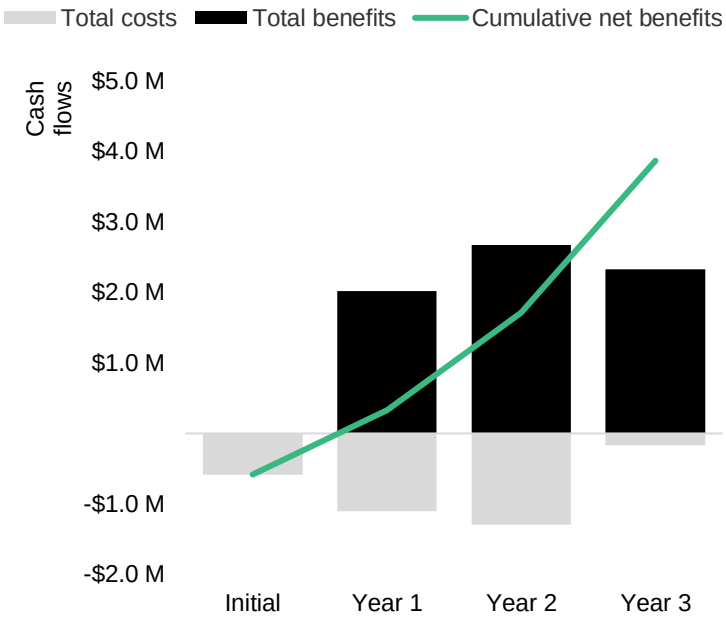
Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $314,000.

Ongoing Operations Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	IT and security resources responsible for managing vDefend	Interviews		5	8	10
G2	Percentage of time dedicated to ongoing management	Interviews		10%	10%	10%
G3	Fully burdened hourly rate for an IT admin/security FTE	Composite		$77	$77	$77
Gt	Ongoing operations costs	G1*G2*G3*2080		$80,080	$128,128	$160,160
	Risk adjustment	↑5%				
Gtr	Ongoing operations costs (risk-adjusted)			$84,084	$134,534	$168,168
	Three-year total: $386,786			**Three-year present value: $313,973**		

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, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

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

Cash Flow Analysis (Risk-Adjusted)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($605,640)	($1,041,474)	($1,208,054)	($168,168)	($3,023,336)	($2,677,174)
Total benefits	$0	$2,018,629	$2,668,779	$2,327,275	$7,014,683	$5,789,235
Net benefits	($605,640)	$977,155	$1,460,724	$2,159,107	$3,991,346	$3,112,061
ROI						116%
Payback						8 months

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 solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

Total Economic Impact Approach

Benefits represent the value the solution delivers to the business. The TEI methodology places equal weight on the measure of benefits and costs, allowing for a full examination of the solution's effect on the entire organization.

Costs comprise all expenses necessary to deliver the proposed value, or benefits, of the solution. The methodology captures implementation and 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. 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."

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.

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.

APPENDIX B: ENDNOTES

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

[2] Source: Forrester's Security Survey, 2024, "How many times do you estimate that your organization's sensitive data was potentially compromised or breached in the past 12 months?" Base: 209 security decision-makers at enterprise organizations with 2,500 or more employees and $2 billion or more annual revenue.

FORRESTER®