EXECUTIVE SUMMARY

The Total Economic Impact™ Of Broadcom VMware vDefend

KEY STATISTICS

ROI	BENEFITS PV	NPV	PAYBACK
116%	$5.79M	$3.11M	8 months

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.

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.

Interviewees said that prior to using vDefend, their organizations struggled to detect and identify threats in a timely way.

READ THE FULL STUDY

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.

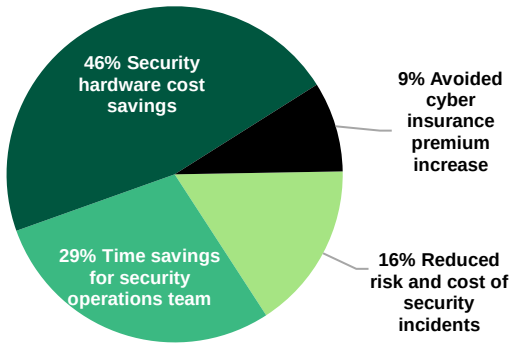
After the investment in vDefend, interviewees' organizations could deploy the software solution quickly and saw improved visibility into their networks. They quickly identified internal threats and took steps to fortify their infrastructure with effective network rules to prevent future malware attacks. 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.

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.

Benefits (Three-Year)



Unquantified benefits. Benefits that are not quantified in 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%.

> “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**

DISCLOSURES

The reader should be aware of the following:

- The study is commissioned by Broadcom VMware and delivered by Forrester Consulting. It is not meant to be 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 report to determine the appropriateness of an investment in VMware vDefend.
- Broadcom VMware reviewed and provided feedback to Forrester. 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.
- Broadcom VMware provided the customer names for the interviews but did not participate in the interviews.

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.

Appendix: 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.