

TECHNICAL VALIDATION

# Empower Your Security Operators to Defend the Private Cloud

Built-in Defense-in-depth With VMware vDefend by Broadcom

By Justin Boyer, Senior Validation Analyst  
Enterprise Strategy Group

July 2025

# Contents

Introduction .....	3
Background .....	3
VMware vDefend.....	4
Enterprise Strategy Group Technical Validation .....	5
Integrated Private Cloud Protection .....	5
Enterprise Strategy Group Analysis .....	5
Enhanced Private Cloud Detection and Response .....	7
Enterprise Strategy Group Analysis .....	7
Intelligent Assist.....	10
Enterprise Strategy Group Analysis .....	10
Conclusion.....	13

# Introduction

This Technical Validation conducted by Enterprise Strategy Group outlines our evaluation of the VMware vDefend platform. We validated how VMware vDefend provides advanced and fully integrated protection capabilities for VMware Cloud Foundation (VCF) environments.

## Background

As organizations continue to take advantage of cloud technologies, the burden of securing cloud environments also grows. Especially within private cloud environments, perimeter-focused security solutions aren't enough to protect against all threats. If attackers make their way through the perimeter, a flat network structure within allows for easy lateral movement and compromise.

Cloud environments vary from private clouds built within an organization's infrastructure to clouds run by communication service providers (CSP), who offer the VCF stack as a service on behalf of customers. To combat this threat, many organizations have turned to micro-segmentation and zero-trust initiatives. According to research conducted by Enterprise Strategy Group, 47% of survey respondents said their organization would most likely use micro-segmentation to support its cloud-native applications. Another 40% indicated that they consider consistent coverage for cloud and on-premises environments one of the most important attributes for technologies supporting zero trust.<sup>1</sup>

However, while micro-segmentation can help limit lateral movement and reduce the blast radius when attacks do occur, it is not enough on its own. Micro-segmentation solutions enforce policy with regard to which workloads can communicate with one another. It does not detect malicious activity or scan traffic for ransomware. Such needs require intrusion detection/prevention (IDS/IPS) and network detection and response (NDR) to identify malware and spotlight potential malicious activity that may not be prevented by micro-segmentation.

Due to these shortcomings, security teams struggle with separate tools that create fractured views of threats and increase complexity and costs. Enterprise Strategy Group research shows that 86% of surveyed organizations are using ten or more tools for security operations.<sup>2</sup> Protecting a private cloud encourages such sprawl to continue. The cybersecurity skills shortage also contributes to the overwhelm felt by security operators.

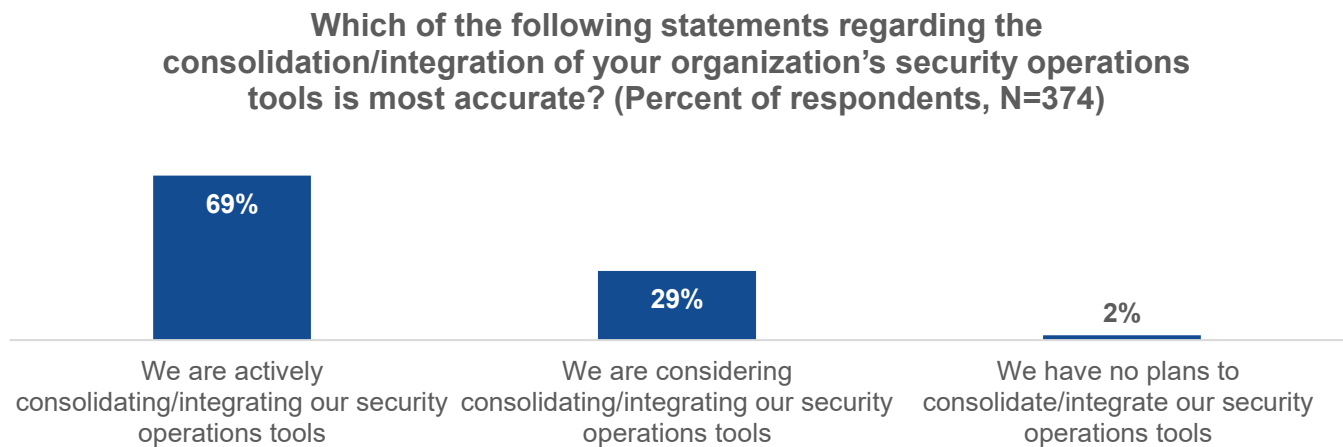
To combat this overwhelming environment, security operations teams are working to consolidate tools. As shown in Figure 1, 69% of respondents are actively consolidating their security operations tools.<sup>3</sup> This consolidation is necessary to provide ease of integration, deployment, and management, while driving better security outcomes for private cloud environments.

---

<sup>1</sup> Source: Enterprise Strategy Group Research Report, [Trends in Zero Trust: Strategies and Practices Remain Fragmented, but Many Are Seeing Success](#), March 2024.

<sup>2</sup> Source: Enterprise Strategy Group Research Report, [The Triad of Security Operations Infrastructure: XDR, SIEM, and MDR](#), June 2024.

<sup>3</sup> Ibid.

**Figure 1. Security Teams Are Working to Consolidate Tools**

*Source: Enterprise Strategy Group, now part of Omdia*

Through solutions that combine regular, workload-level network policy enforcement with multi-layered threat detection capabilities, network and SOC teams can help their organizations improve operational efficiency, streamline compliance, prevent ransomware, and, ultimately, deliver better security outcomes.

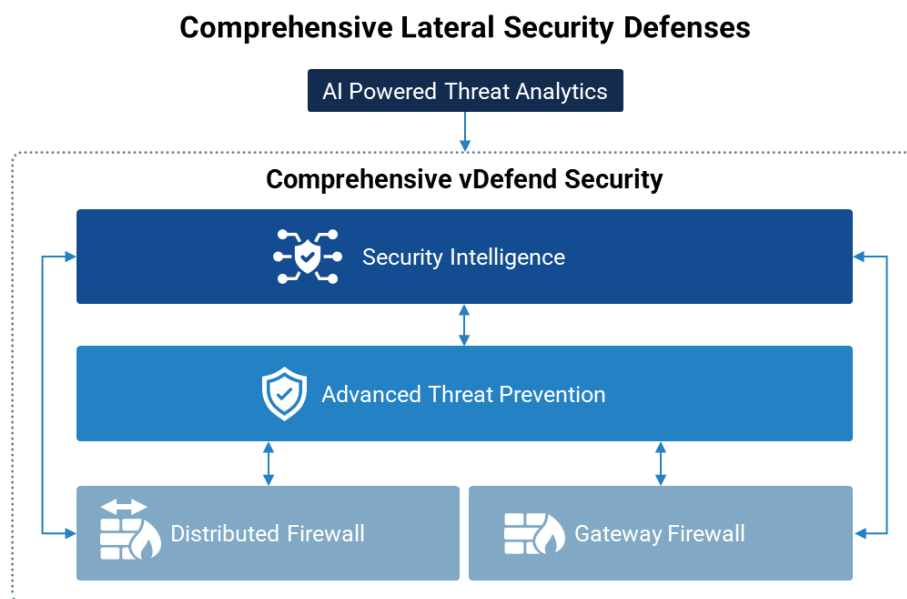
### VMware vDefend

VMware vDefend is a comprehensive security platform built to provide multi-layered defense in depth for private clouds built on VCF. It features distributed L7 stateful firewalling along with advanced threat prevention. VMware vDefend is integrated with VCF, providing control and visibility while scaling with the organization.

VMware vDefend helps organizations achieve their zero-trust goals and protect their private cloud environments from ransomware and other sophisticated threats through granular network micro-segmentation and advanced threat prevention (ATP). vDefend enables organizations to eliminate blind spots, identify intruders, and prevent vulnerability exploitation and the spread of malware.

To accomplish this, VMware vDefend features several tools (see Figure 2):

- **Security Intelligence for vDefend.** vDefend uses advanced network traffic analysis to discover business applications in use and build a comprehensive application topology. It uses this topology to provide intelligent micro-segmentation policy recommendations.
- **vDefend Distributed Firewall and Gateway Firewall.** Distributed firewalls provide protection to east-west traffic between workloads within the cloud environment in addition to perimeter protection around it. vDefend enables organizations to create and enforce micro-segmentation across virtual, container, and physical workloads with an object-based policy automation engine.
- **vDefend Advanced Threat Prevention (ATP).** ATP works to prevent and block threats early in the attack lifecycle. Featuring signature and behavior-based IDS/IPS capabilities along with network traffic analysis, ATP provides advanced network detection and response and sandboxing for malware detection and prevention. IDS/IPS remains a critical network security function that helps organizations meet compliance requirements such as PCI DSS, GDPR, and HIPPA and act as a first line of defense against malicious traffic. Network Traffic Analysis (NTA) ensures that security teams have visibility into stealthy advanced threats that evade traditional signature-based detections. VMware vDefend features NDR capabilities that reduce noise and enable the SOC to triage potential threats more effectively.

**Figure 2.** VMware vDefend

Source: Broadcom and Enterprise Strategy Group, now part of Omdia

## Enterprise Strategy Group Technical Validation

Enterprise Strategy Group validated how VMware vDefend provides the tools to protect VCF environments. Via remote demonstration, we validated how vDefend's integration with VCF provides administration and protection benefits, how security operators can use vDefend to find and remediate threats, and how it intelligently helps analysts take action on potential threats.

### Integrated Private Cloud Protection

Enterprise Strategy Group validated vDefend's integration with VCF, helping to provide a complete security solution for VCF environments.

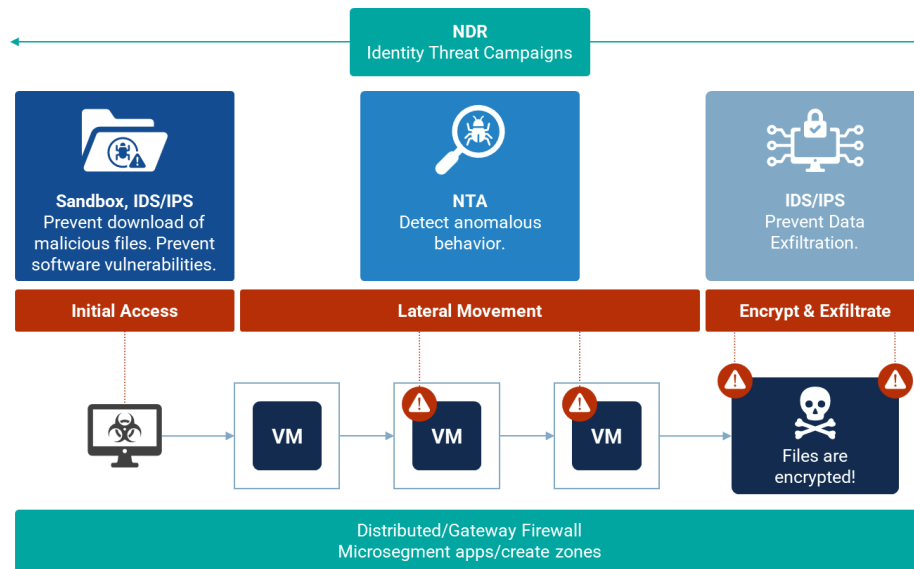
### Enterprise Strategy Group Analysis

When building a private cloud infrastructure to support business requirements, security is often reduced to micro-segmentation. However, micro-segmentation alone may not be enough to protect against sophisticated attacks featuring social engineering, malware, and ransomware. Attackers who manage to spend long amounts of time within an environment can continually search for vulnerable workloads using open protocols such as Remote Desktop Protocol (RDP) or Server Message Block (SMB). Application vulnerabilities, operating system vulnerabilities, and human error can also be used to bypass micro-segmentation controls. Typically, security teams would be forced to deploy multiple solutions to cover various potential security vulnerabilities. Doing so can increase costs and complexity and require security operators to learn new skills or tools.

VMware vDefend is plug and play for VCF environments, greatly reducing the number of tools required to protect private cloud workloads. By integrating fully with VCF, vDefend provides complete visibility into east-west traffic within the private cloud. Additionally, this integration also enables fast deployment. Security teams can add protection to their existing VCF environments with only a few clicks.

Figure 3 shows the typical attack path an attacker may take through a VCF environment and how vDefend's components work together to weave layers of defense against compromise and lateral movement.

**Figure 3.** vDefend Protects Against Advanced Attack Scenarios



Source: Broadcom and Enterprise Strategy Group, now part of Omdia

Initial access is usually achieved by gaining access to an endpoint, typically by finding a way to download a malicious file to it, taking advantage of a vulnerability, and setting up a connection to a command-and-control server. VMware vDefend features a sandbox that integrates machine learning (ML), static and dynamic analysis, and memory analysis to detect malicious files, including those trying to exploit zero-day vulnerabilities. Further, vDefend's IDS/IPS prevents and detects command-and-control beaconing, determining that malware is already present and an attacker is trying to gain a foothold within the environment.

Once an attacker gains access to an environment, their goal becomes reconnaissance and lateral movement throughout the environment, looking for valuable data. Ransomware has become big business, and data is the resource attackers need to make their money. While micro-segmentation provides protection by creating zones for applications and workloads, some critical network infrastructure cannot be segmented in this way. VMware vDefend uses NTA to detect anomalous behavior across the private cloud network. Additionally, vDefend's IDS/IPS capabilities inspect all traffic entering or leaving the network, looking for malicious traffic patterns such as data exfiltration.

IDS/IPS also provides virtual patching, helping organizations to prevent attackers from taking advantage of the same vulnerabilities repeatedly until a permanent solution can be implemented. VMware vDefend applies these protections at the hypervisor for every workload, rather than at wider control points as with traditional network-based IDS/IPS solutions. Additionally, organizations using a traditional network-based security model would have to manually route traffic to four separate tools (i.e., the firewall, the IDS/IPS, the sandbox, and the NDR/NTA solution) and, in many cases, hairpin to a physical device outside of the hypervisor. Incorporating all these tools into VCF to provide a native security solution vastly increases time to value and performance and improves overall security posture.

## Why This Matters

Organizations have continued to expand their IT capabilities to take advantage of the flexibility and scalability of cloud technologies. Many have used technologies like VCF to build private clouds or use CSPs to access their capabilities. However, complex environments have led to challenges in defending these cloud environments from attackers, often necessitating a host of security tools to keep up with the growing attack surface. Research conducted by Enterprise Strategy Group shows that organizations are actively trying to consolidate and integrate their security operations tools because they believe doing so will improve their advanced threat detection capabilities and incident response activities while better optimizing costs.<sup>4</sup>

VMware vDefend provides organizations with a comprehensive solution built into VCF and used to protect VCF environments. By fully integrating with VCF hypervisors, vDefend enables organizations to turn on protection for their existing VCF environments with a few clicks. vDefend features a sandbox to detect malicious files and prevent initial infection. Advanced micro-segmentation, along with NTA and IDS/IPS capabilities, continuously monitor traffic throughout the cloud network, looking for anomalous and malicious activity.

By providing advanced security tools built into VCF, VMware provides a solution that protects private clouds with minimal cost to deploy and administer. Security operators have full visibility into the cloud and access to intelligent tools designed to help guide security teams to the most secure configuration. Additionally, vDefend's integration with VCF enables security teams to reduce time to value while increasing security posture.

## Enhanced Private Cloud Detection and Response

Enterprise Strategy Group validated how security operators can use VMware vDefend to find, investigate, and stop potential attacks.

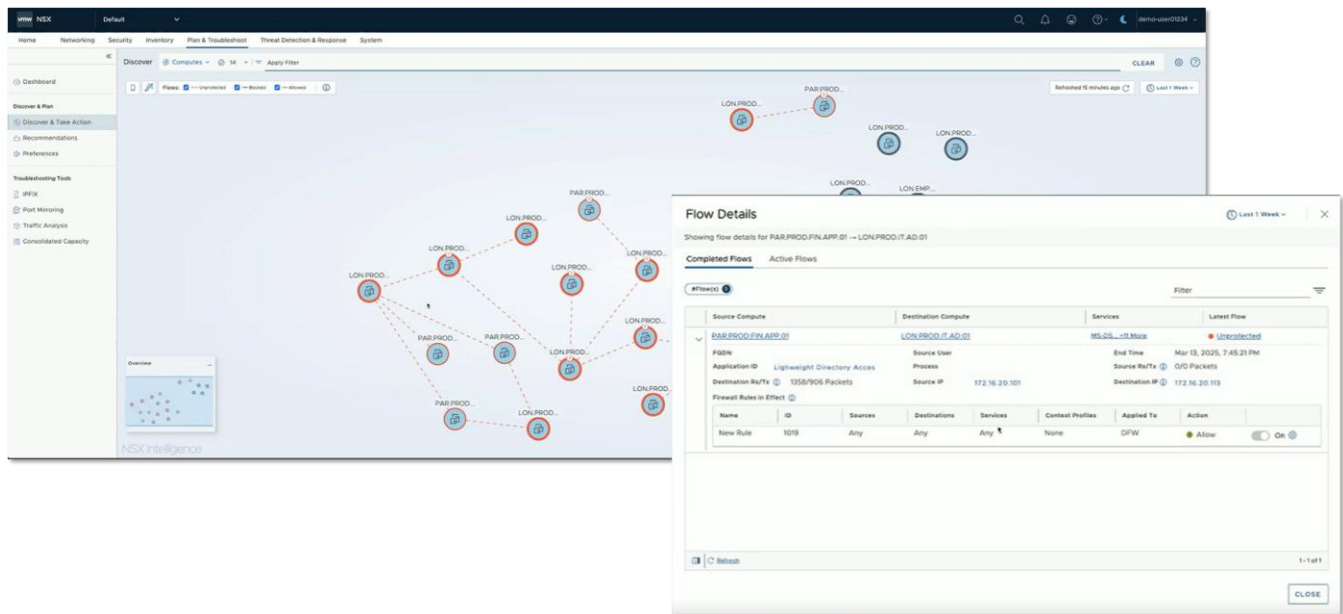
### Enterprise Strategy Group Analysis

First, Enterprise Strategy Group walked through how a security operator uses Security Intelligence for vDefend to gain visibility into workload flows and potentially malicious activity within the VCF environment. We saw how vDefend displays the various workflows and data around the flows. Security Intelligence collects the context around network traffic, identifying the process that generated the flow, the user that initiated the process, and the application or network protocol used, such as Lightweight Directory Access Protocol (LDAP). This increased visibility into the environment can not only find malicious activity but also warn security operators of incorrect application and network configuration. For example, Security Intelligence will determine and show if a workload is using TLS 1.1, a deprecated protocol that shouldn't be used in the environment (see Figure 4).

---

<sup>4</sup> Ibid.

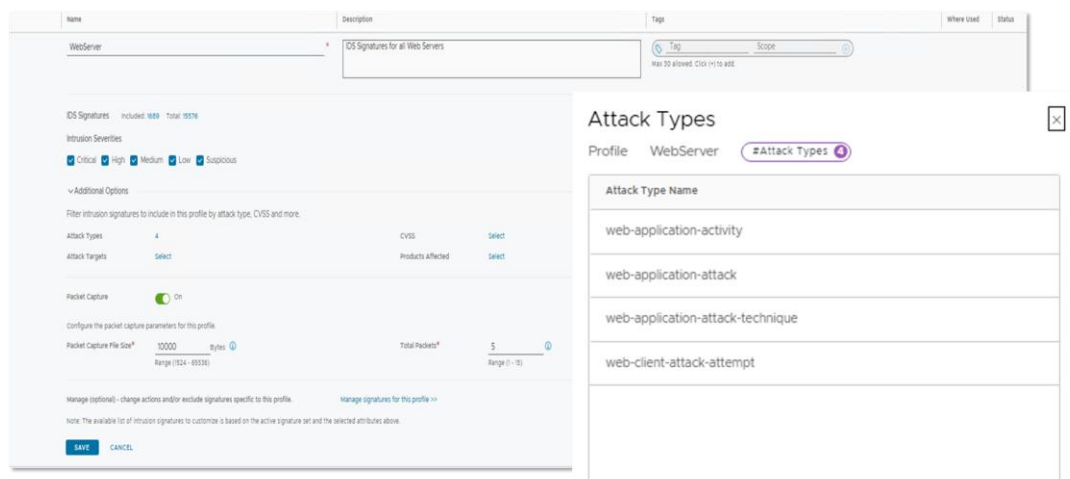
Figure 4. Security Intelligence View With Flow Details



Source: Enterprise Strategy Group, now part of Omdia

Next, we explored the Threat Detection & Response view within vDefend, where the NTA, IDS/IPS, and malware detection and prevention capabilities are brought together to create a unified view of risk across the environment. VMware vDefend offers organizations the ability to create IDS profiles—collections of IDS signatures for use in an inspection policy. IDS profiles enable security teams to apply a group of IDS signatures, including imported, created, or default signatures, to specific workloads and traffic types within VCF. There are several options for configuring and filtering the signatures based on attack types, CVSS scores, attack targets, or products affected. Security teams also have the option to turn on packet captures for the profile, enabling easier forensic investigations. In our scenario, we filtered attack types specific to web application attacks for use on web server workloads within a VCF environment (see Figure 5).

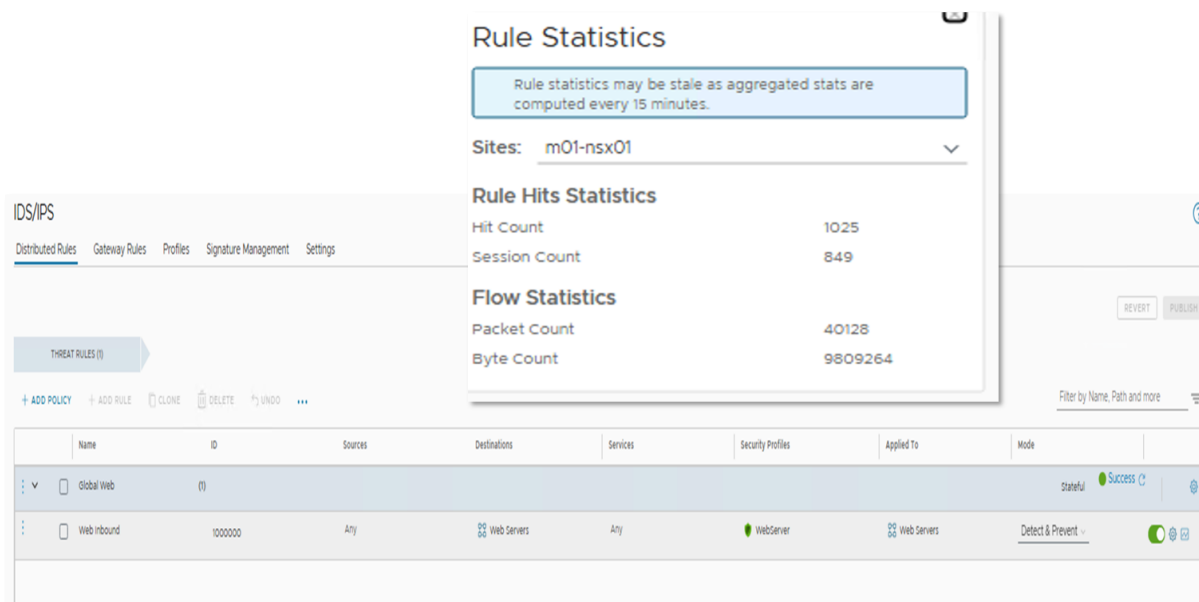
Figure 5. Creating an IDS Profile and Filtering Signatures to Target Web Application Attacks



Source: Broadcom and Enterprise Strategy Group, now part of Omdia

Next, we created an IDS Rule to inspect inbound traffic to a web server using the IDS profile we created (see Figure 6). Creating IDS profiles helps to reduce complexity and false positives when creating IDS rules. A typical VCF environment will have many types of workloads, such as web servers and databases, each with different attack vectors and attack types. IDS profiles provide the flexibility to apply these signatures to specific workloads as needed. Broadcom customers also have access to a portal where they can research IDS signatures and learn more about which are the best fit for their profiles.

**Figure 6.** Creating an IDS Rule Using the Previously Created Profile



Source: Broadcom and Enterprise Strategy Group, now part of Omdia

Since vDefend ATP is built directly into the hypervisor, accessing the virtual network interfaces of each workload, it has full visibility into east-west traffic across the environment. NTA uses this integration to understand typical network traffic patterns and use it to intelligently find malicious activity. For example, RDP traffic is not unusual for most corporate environments, as it is used for IT support purposes. However, when vDefend ATP detects RDP on a workload that has never used it before or has RDP paired with identifiable command and control activity, vDefend raises the threat level and combines these signals to alert security teams to a potential attack.

Malware detection also benefits from vDefend's integration with VCF, enabling ATP to scan files transmitted over encrypted channels, such as HTTPS. Many VCF environments use VMware Tools to gain deep access and visibility into workloads, and vDefend ATP taps into VMware Tools to provide advanced malware detection and prevention. ATP has access to each workload's file disk operations. As a file is written to disk, ATP creates an in-memory copy of the file and inspects the file hash to determine if it's a known malicious file. Since ATP does this after the file download, there is no need to decrypt the file first. ATP also uses static analysis and a cloud sandbox where it can execute the payload and watch what it does to determine if it's malicious. This enables vDefend to detect new types of malware that purely signature-based methods may miss.

The Plan & Troubleshoot view also highlights suspicious traffic that NTA discovers across the environment. NTA uses ML algorithms to determine the baseline of network activity and then looks for deviations from the norm. Further, when it detects an anomaly, NTA will use additional ML and rule-based techniques to determine the likelihood of this activity being malicious or part of a larger attack. For example, while DNS requests are a normal traffic flow, DNS requests to a seemingly computer-generated domain, along with a high volume of data leaving a workload that typically doesn't send out data frequently, will be flagged as possible DNS exfiltration.

## Why This Matters

Dynamic and challenging environments, such as a private cloud, make cybersecurity a challenge. Many organizations are turning to zero-trust practices and tools to help mitigate the risk posed by such a rapidly changing environment. According to research conducted by Enterprise Strategy Group, organizations have identified several critical attributes zero-trust technologies must meet, such as the use of AI and ML and consistent cloud and on-premises coverage. Additionally, a third of surveyed organizations indicated the desire to have zero trust tools that are a part of a broader platform from a single vendor.<sup>5</sup>

Enterprise Strategy Group validated that VMware vDefend helps organizations implement zero trust across their VCF environments and provides advanced threat detection and response capabilities. We saw how NTA and IDS/IPS solutions, fully integrated with VCF, gather a picture of “normal” traffic within the environment. It can then detect anomalous traffic and correlate multiple signals to detect malicious activity. It provides a complete view to security operators of how an attack started, where an attacker moved through the environment, and any potential data exfiltration. The malware detection and response platform also uses VCF integration to scan incoming files, not trusting anything, and determines whether a file is malicious without having to decrypt traffic.

By integrating fully with VCF, VMware vDefend provides security teams with the tools necessary to protect and enforce zero trust throughout a VCF environment. VMware vDefend provides a comprehensive, prioritized view of potential threats, saving security teams significant investigation time. This advanced protection can be turned on with a few clicks, reducing time and costs associated with implementing these tools separately.

## Intelligent Assist

Enterprise Strategy Group validated VMware vDefend’s Intelligent Assist capability, helping to close the skills gap and mitigating threats found within the VCF environment.

## Enterprise Strategy Group Analysis

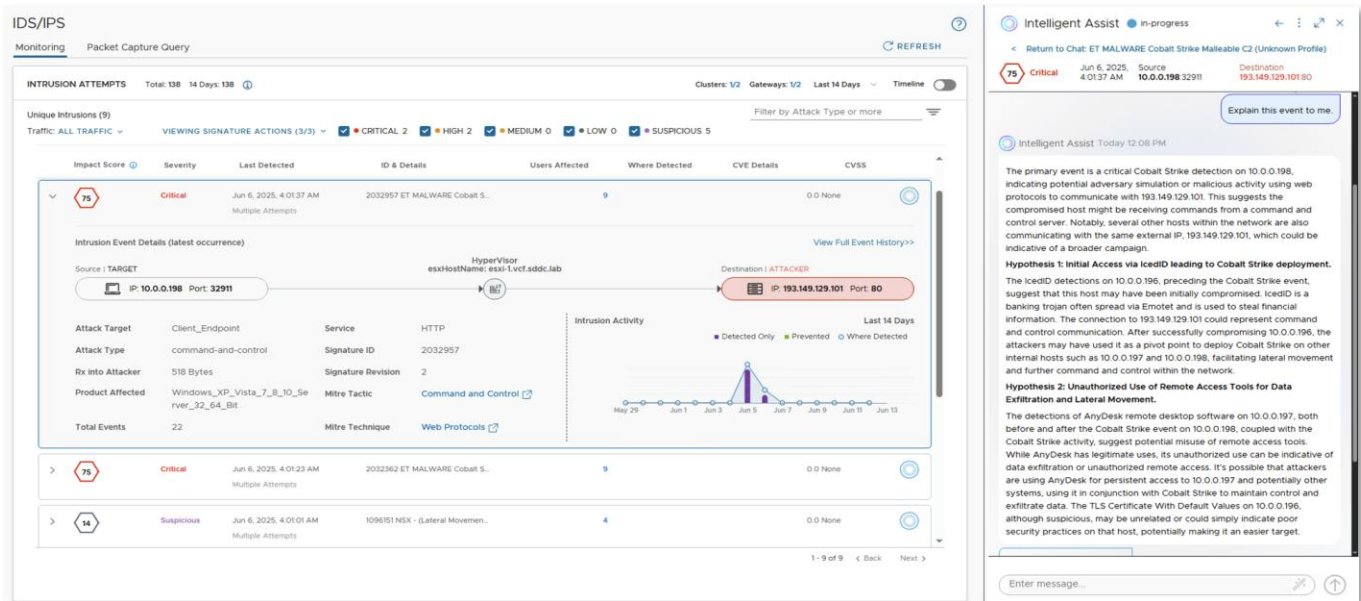
VMware vDefend enables security teams to monitor VCF environments for threats while providing a clear picture of what is happening. However, only viewing what has happened or individual suspicious events isn’t enough. Security teams must act on the information and work to mitigate any threats and prevent them from happening again. However, the ever-present skills gap can impact the effectiveness of mitigation strategies, especially when working with junior security analysts.

VMware vDefend provides Intelligent Assist to help bridge this gap and provide guidance to security operators through a generative AI interface. Deployed via a browser plugin, Intelligent Assist integrates with vDefend to take the context within a specific attack campaign and provide explanations and remediation guidance.

Enterprise Strategy Group walked through an example of how a security operator might use Intelligent Assist to understand better what happened during an attack, what parts of the environment were affected, and how to mitigate it. First, we asked Intelligent Assist to explain a specific IDS event (see Figure 7).

<sup>5</sup> Source: Enterprise Strategy Group Research Report, [Trends in Zero Trust: Strategies and Practices Remain Fragmented, but Many Are Seeing Success](#), March 2024.

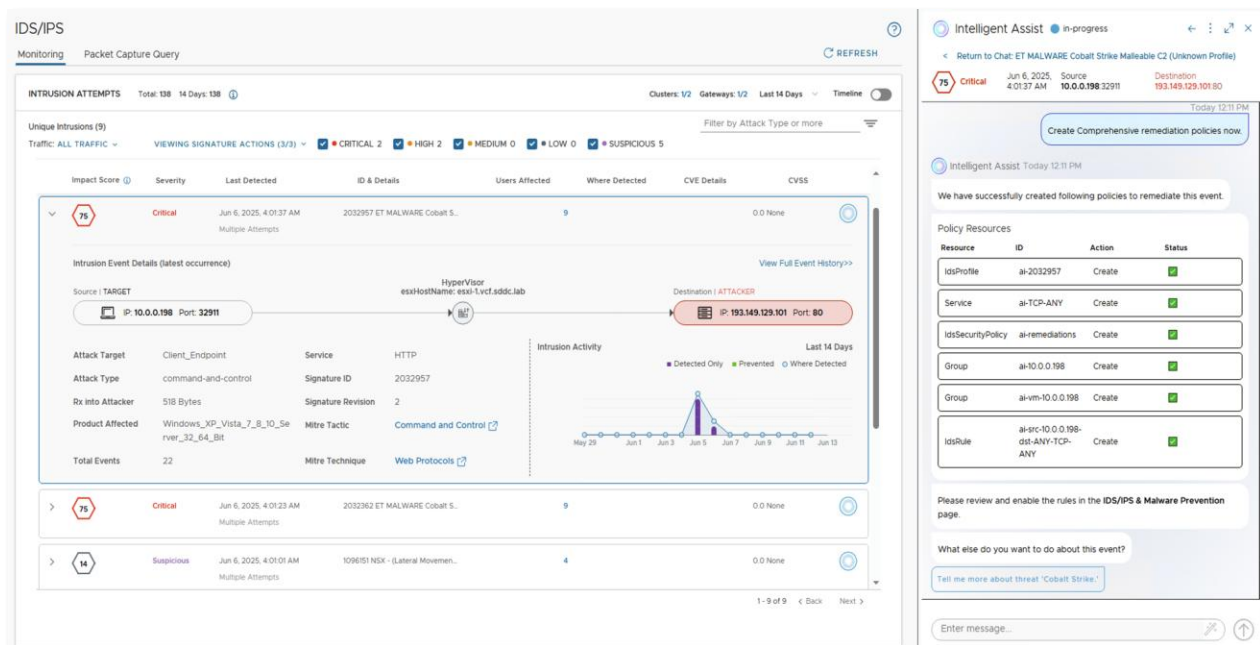
Figure 7. Intelligent Assist Explains an IDS Event



Source: Broadcom and Enterprise Strategy Group, now part of Omdia

Intelligent Assist provided helpful information about the signatures found and how this event may fit into a larger campaign. In this example, Intelligent Assist identified IcedID as a banking trojan designed to steal financial information and credentials. It also explains how the use of Cobalt Strike, a popular red teaming application, indicated that the attacker was attempting to gain a permanent foothold in the environment. Intelligent Assist proposed that this campaign was a targeted attack aimed at stealing sensitive data as well as establishing a foothold from which to launch further attacks.

Finally, we asked Intelligent Assist how to remediate the threat posed by this campaign. Intelligent Assist then provided two remediation strategies: a targeted strategy that affects mainly the workloads involved in the campaign or a comprehensive strategy that creates a broader application of policies that will prevent this attack across the environment. After we clicked to remediate using the comprehensive strategy, Intelligent Assist then provided a list of proposed remediation policies. After choosing to create these policies, Intelligent Assist created them in disabled mode, giving the security team the opportunity to audit and review them before implementation (see Figure 8).

**Figure 8.** Intelligent Assist Creates Remediation Policies

Source: Broadcom and Enterprise Strategy Group, now part of Omdia

## Why This Matters

Detection of malicious activity is only the beginning. Once an investigation is over, remediation strategies are necessary to prevent the same type of attack from occurring in the future. However, deciding on a remediation strategy that applies to the entire environment without interrupting business operations can be challenging, especially for more junior analysts.

Enterprise Strategy Group validated that VMware vDefend provides the needed remediation guidance through Intelligent Assist. Installed as a browser plugin, Intelligent Assist has access to all of the information gathered by vDefend's IDS/IPS and malware detection capabilities. Through Intelligent Assist, we were able to summarize an IDS event. We were then able to use Intelligent Assist to choose remediation strategies, after which it created the necessary policies for review.

Using Intelligent Assist enables security teams to quickly assess an IDS event, understand what happened and how it happened, and create the necessary policies to prevent it from happening again. Intelligent Assist greatly reduces the time needed to develop remediation strategies and creates policies that will apply across the environment with the least likelihood of interruption.

## Conclusion

The march toward the cloud continues. However, the public cloud isn't the only option for many organizations. Instead, they create a private cloud using VCF or use a CSP to provide private cloud services to them. This helps to protect critical business data while enabling an organization to take advantage of the flexibility and scalability of cloud services. However, private cloud environments can be challenging to defend as their complexity grows. While many organizations are implementing zero-trust principles into their environments and using micro-segmentation to enhance their security posture, micro-segmentation alone isn't enough.

Security teams still struggle with several different network security tools, such as IDS/IPS and NDR, to detect and prevent malicious software and ransomware from gaining a foothold within an environment. Enterprise Strategy Group research shows that security operations teams are looking to consolidate their tools to improve their advanced threat detection capabilities and optimize costs.<sup>6</sup> Private cloud environments riddled with tool sprawl become much harder and more expensive to protect from advanced attacks. Further, as organizations move toward zero-trust methodologies to protect their environments, they need tools to make the transition easier.

Enterprise Strategy Group validated that VMware vDefend provides the tools necessary to protect VCF environments and save time and effort for security teams. VMware vDefend is fully integrated with VCF, allowing for easy deployment and a comprehensive view of the environment. We saw how vDefend used this integration to inspect network traffic and downloaded files to find potentially malicious activity. We also saw how vDefend's NDR used ML-based detection to correlate signals and create a prioritized list of attack campaigns. Additionally, we saw how vDefend's Intelligent Assist saves time and effort for security teams by providing detailed summaries of attacks, a list of IOCs, and specific, context-aware remediation policies that it then created for us. By providing all of this functionality built in with VCF, security teams have all the tools necessary to increase their security posture, maintain compliance, and more efficiently run a network security infrastructure for their private cloud.

VMware vDefend offers built-in protection for VCF environments. If your organization is using VCF to run business-critical workloads and needs integrated protection from advanced threats and malware, Enterprise Strategy Group recommends that you consider VMware vDefend by Broadcom.

---

<sup>6</sup> Source: Enterprise Strategy Group Research Report, [The Triad of Security Operations Infrastructure: XDR, SIEM, and MDR](#), June 2024.

©2025 TechTarget, Inc. All rights reserved. The Informa TechTarget name and logo are subject to license. All other logos are trademarks of their respective owners. Informa TechTarget reserves the right to make changes in specifications and other information contained in this document without prior notice.



Information contained in this publication has been obtained by sources Informa TechTarget considers to be reliable but is not warranted by Informa TechTarget. This publication may contain opinions of Informa TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent Informa TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, Informa TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of Informa TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at [cr@esg-global.com](mailto:cr@esg-global.com).

---

#### About Enterprise Strategy Group

Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 [contact@esg-global.com](mailto:contact@esg-global.com)  
 [www.esg-global.com](http://www.esg-global.com)