



ESG Lab Validation

vArmour DSS Distributed Security System: Scalable and Simple Security for the Modern Data Center

Inline Workload-level Security for Physical, Virtual, Cloud-based, and Container-based Networks

By Tony Palmer, Senior ESG Lab Analyst
May 2017

This ESG Lab Report was commissioned by vArmour and is distributed under license from ESG.

Contents

Introduction	3
Background	3
vArmour DSS Distributed Security System.....	4
ESG Lab Validation	5
Simplified and Efficient Security Operations	5
ESG Lab Testing	5
Highly Scalable Elastic Platform	8
ESG Lab Testing.....	8
Automated and Extensible Segmentation	11
ESG Lab Testing.....	11
Integrated Deception Security Services	13
ESG Lab Testing.....	14
The Bigger Truth.....	17
Appendix	18

ESG Lab Reports

The goal of ESG Lab reports is to educate IT professionals about data center technology products for companies of all types and sizes. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

Introduction

ESG Lab validated the vArmour DSS Distributed Security System with a focus on its ability to simplify and efficiently protect applications and workloads from intrusion, regardless of where those assets are located. Also of interest was vArmour's ability to scale quickly and easily, the capability to automate the addition of new assets, the product's deception capability, and its overall ease of use and efficiency.

Background

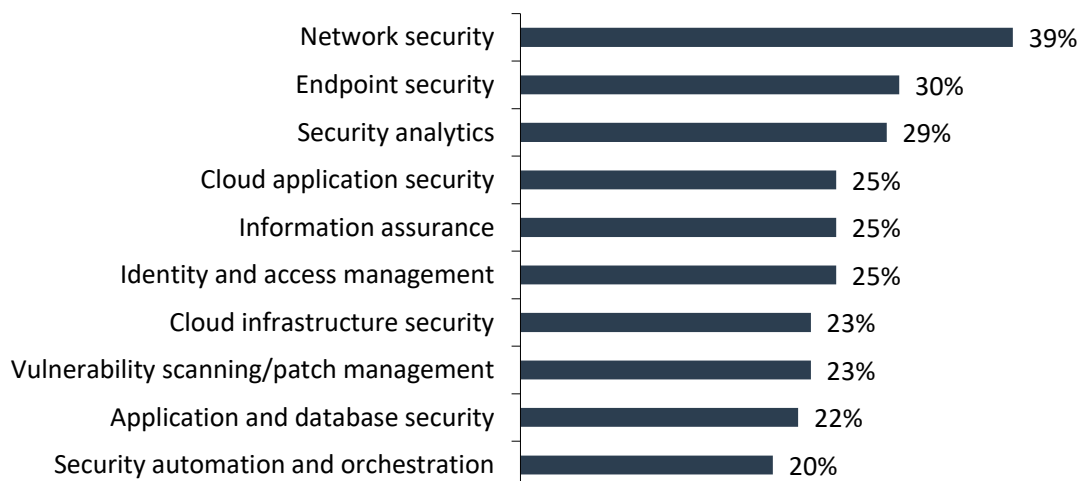
Traditional network security products can be complex and time-consuming to deploy, manage, and maintain. For example, traditional next-generation firewalls (NGFWs) sit at the network or data center perimeter with limited visibility *inside* the data center; they must manage their policies across a sprawl of multiple single instance systems; and they can only scale up by adding additional hardware to improve performance, which adds operational burden. Likewise, software-defined networks (SDNs) require network reconfiguration and provide basic layer-4 policy controls. To deliver application layer policy at layer 7, organizations must build complex traffic steering methods with NGFWs just to collect application-layer context. This presents significant complexity of troubleshooting and management functions.

Every time a new application or system is added to the network, every aspect of the new system must be secured. Until recently, new applications and systems would take weeks to roll out, allowing time for a thorough security analysis to be performed. Nowadays, systems are often rolled out very quickly, sometimes in hours, and even though security requirements are stricter than ever, time that was once dedicated to security analysis is lost and IT security teams can find themselves forced to play catch up after applications have been released.

Cybersecurity is consistently the most often cited IT Priority in annual ESG IT spending intention surveys¹ by a wide margin. The chart in Figure 1² shows how respondents plan to spend their cybersecurity budgets over the next 12-18 months, including network security, endpoint security, and security analytics.

Figure 1. Specific Spending Plans for Cybersecurity Over the Next 12-18 Months

We would like to learn more about your specific spending plans for cybersecurity. In which of the following areas will your organization make the most significant investments over the next 12-18 months? (Percent of respondents, N=418, five responses accepted)



Source: Enterprise Strategy Group, 2017

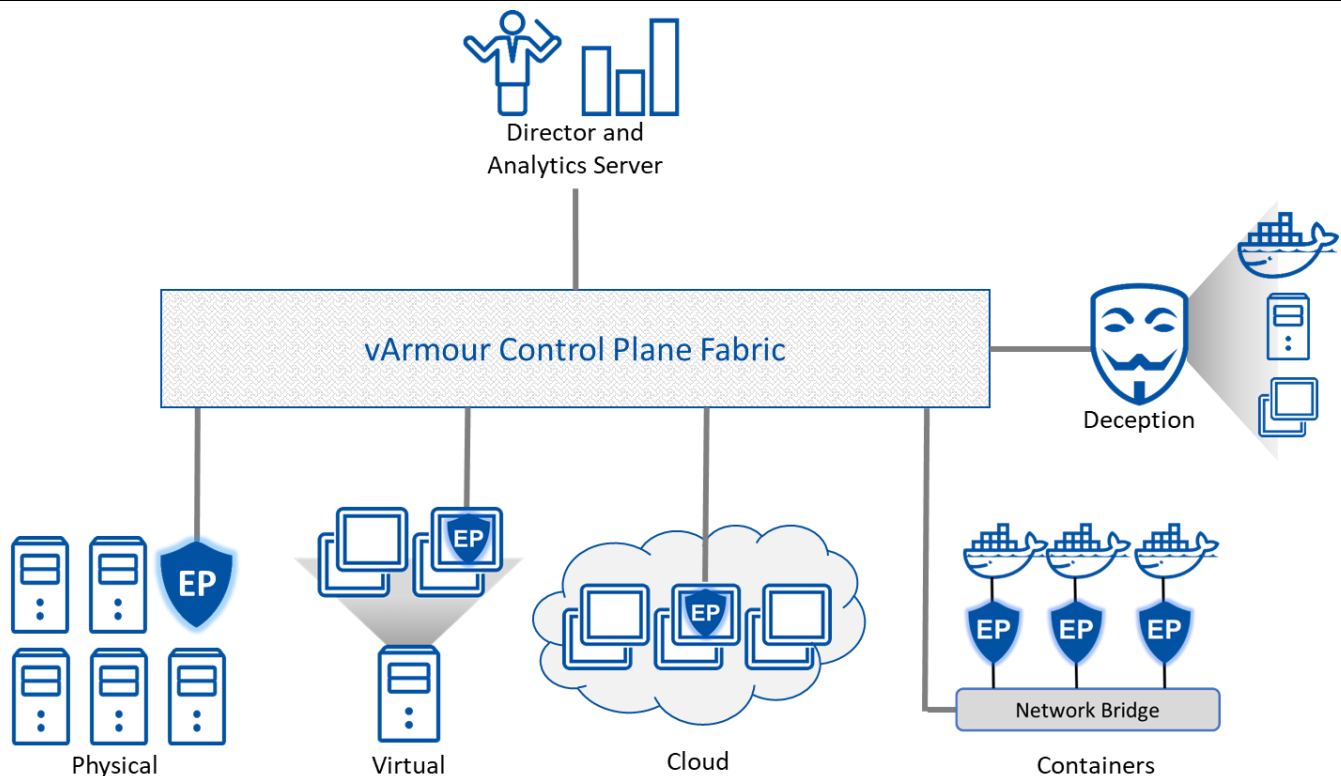
¹ Source: ESG Research Report, [2017 IT Spending Intentions Survey](#), March 2017.

² Ibid.

vArmour DSS Distributed Security System

vArmour DSS is a distributed platform with integrated security services for the modern cloud and data center. It delivers software-based, application-aware segmentation, micro-segmentation, monitoring, centralized policy modeling, and cyber deception designed to help organizations protect critical applications and workloads. As shown in Figure 2, vArmour DSS is an API-driven, distributed, and agent-less security system engineered to protect workloads and applications in physical, virtual, cloud, and container environments, and is agnostic to the underlying infrastructure. All management takes place through a web-based console and/or CLI, and vArmour's APIs allow integration with a variety of third-party tools and systems of record.

Figure 2. vArmour Data Center and Cloud Security



Source: Enterprise Strategy Group, 2017

vArmour's approach to security is about reducing risk by limiting network communications to authorized systems and applications, increasing operational efficiency by enabling the pooling of resources with different security requirements on the same shared infrastructure, and improving compliance by logically separating regulated from unregulated workloads without relying on hardware-bound zones as the primary policy construct. vArmour deploys Enforcement Points (EPs), which sit transparently on the network and monitor all traffic going in and out of managed workloads. Unlike traditional network security systems, which typically sit on the network or data center perimeter and get their information from switches and other network devices, vArmour can see all traffic, including all internal "east-west" traffic. The EPs perform layer-7 deep packet inspection, which allows vArmour to associate traffic with an application rather than a network port (e.g., http traffic can be identified even if it is not directed to port 80), and generate layer-7 metadata on all network traffic, which is leveraged for analytics, policy design and reporting.

Instead of requiring labor-intensive tuning across multiple single-instance traditional firewalls, vArmour is a distributed security platform that places layer-7 controls directly adjacent to the workloads themselves. vArmour's segmentation and micro-segmentation capabilities allow network traffic to be restricted to the systems, applications, users, and network

segments it belongs to, and make it easier to identify inappropriate traffic. As workloads are deployed inline as part of the vArmour platform, other security services such as cyber deception can be called. vArmour's deception functionality redirects any traffic matching a redirect policy action, regardless of target IP to a Deception Point, where attackers can be identified as they attempt to infiltrate the network. Attacker activity can also easily be monitored, investigated, quarantined, and remediated using vArmour's analytics and segmentation capabilities.

ESG Lab Validation

ESG Lab tested vArmour DSS with a goal of validating the platform's ability to reduce risks and attack surfaces, improve operational efficiency, and enable improved compliance adherence in a highly scalable and extensible package.

Simplified and Efficient Security Operations

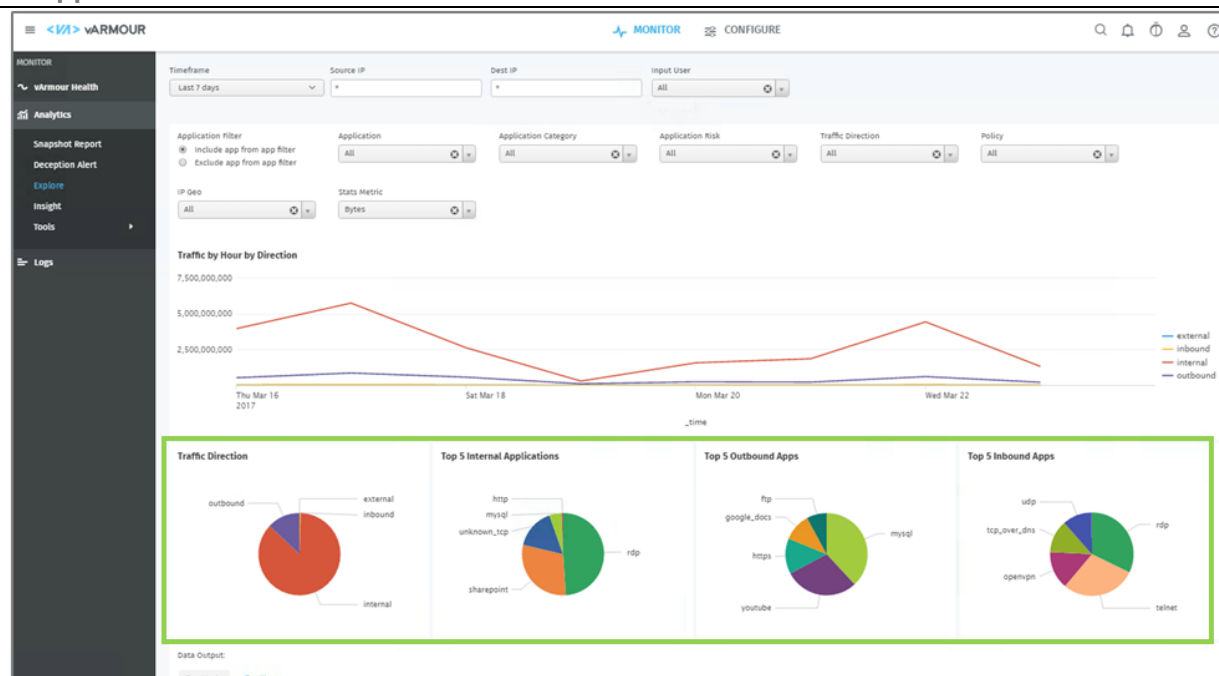
First, ESG Lab examined ease of installation and configuration of the integrated platform, looking at how policy controls can span physical, virtual, cloud, and container-based environments with a single fabric.

ESG Lab Testing

Testing began by simply downloading an OVA file, importing the file into vCenter, and powering the VM on. After logging into the installation web browser interface and pointing the installer to vCenter, vArmour quickly ingested all vCenter objects, prompted the administrator to select the hypervisors to install vArmour on, and choose the underlying switches to tap into to gain visibility into the application traffic. This installation process took less than 30 minutes.

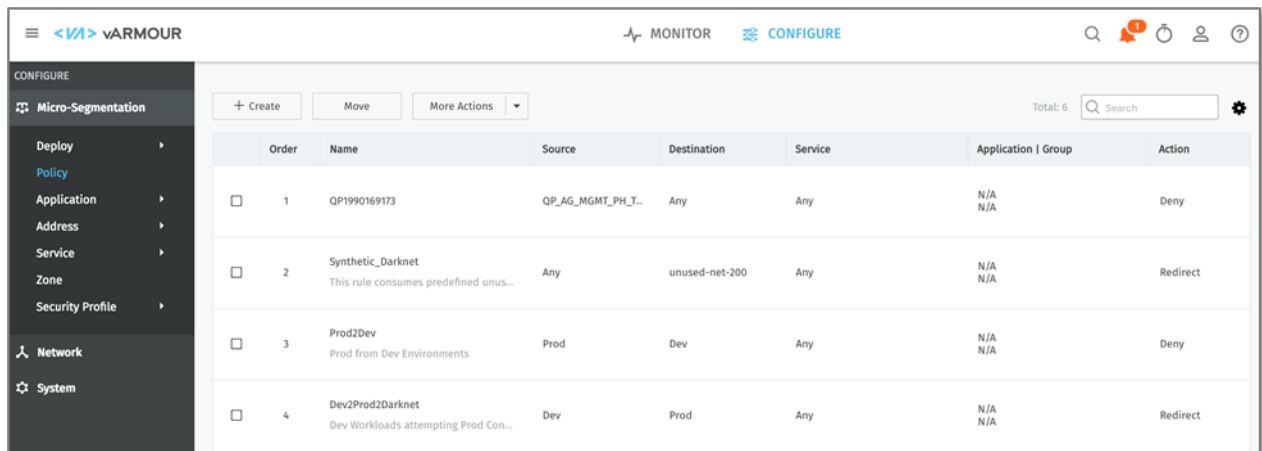
Once DSS was installed, ESG Lab deployed DSS in tap—or learning—mode as a guest VM to get full layer-7 application-level visibility and better understand the relationships, communications, and dependencies of the applications on the workloads. Next, ESG Lab looked at application-level traffic flows and, as seen in Figure 3, DSS provides a simple visualization that breaks out applications by relevant attributes and enables rapid, granular analysis that can inform policy construction.

Figure 3. Application-level Traffic Flows



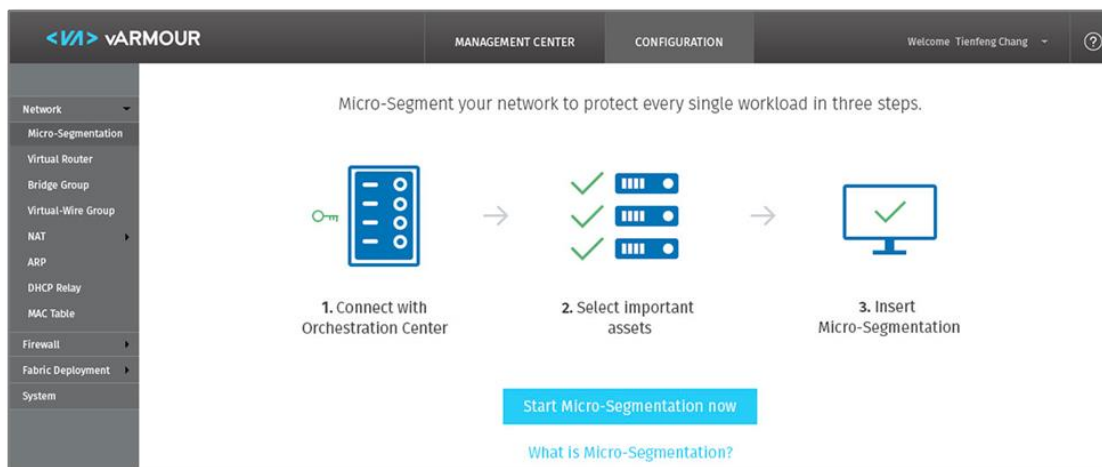
Next, ESG Lab constructed policies (see Figure 4) and tested them in tap mode to troubleshoot and refine them.

Figure 4. Constructing Policies



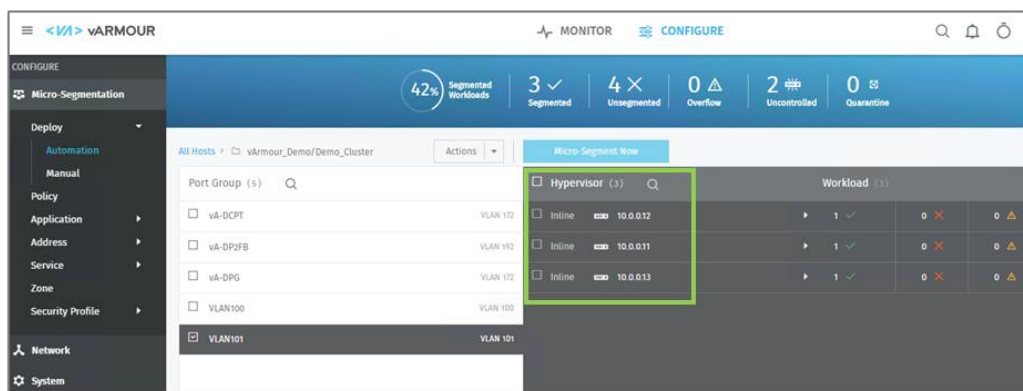
Finally, ESG Lab took the environment inline and enabled micro-segmentation with three just steps, seen in Figure 5. First, ESG Lab connected with the VMware vSphere environment and selected three assets: a host, a port group, and a VLAN.

Figure 5. Deploying vArmour DSS Using the vArmour Installer



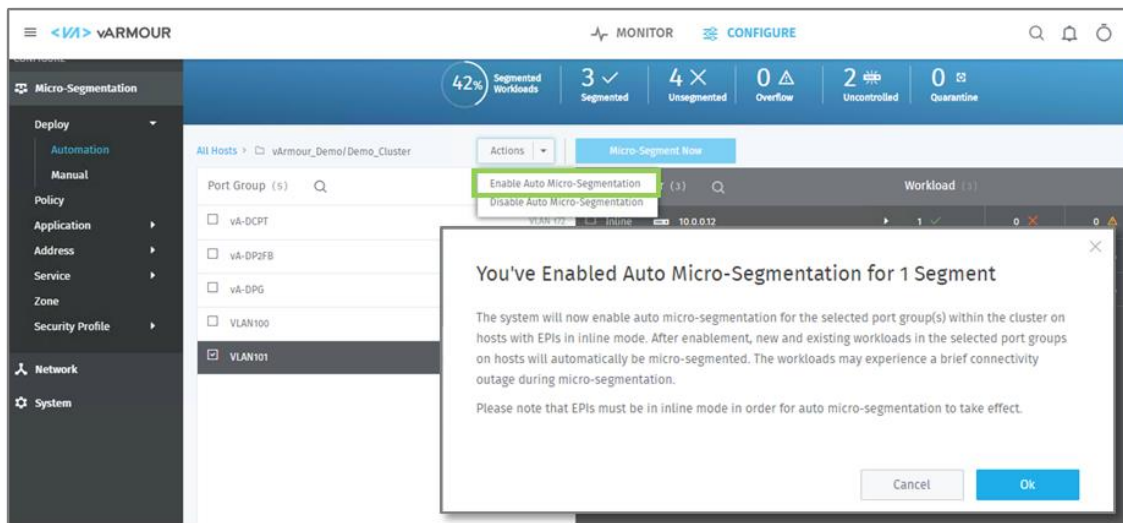
We clicked the **Start Micro-Segmentation now** button and were presented with a dialog box indicating that three workloads currently tapped were available for micro-segmentation. We clicked **OK**, and a few seconds later micro-segmentation was completed and the vArmour DSS EPs were inline, as seen in Figure 6.

Figure 6. Micro-segmentation Complete



Finally, ESG Lab enabled automated micro-segmentation, where new VMs added to vCenter are automatically micro-segmented and moved inline with vArmour, providing instant protection without administrator interaction. Auto micro-segmentation was enabled for port group *VLAN 101* with just one click.

Figure 7. Setting Up Automatic Micro-Segmentation



Why This Matters

Of organizations prioritizing cybersecurity initiatives in 2017, 39% expect to allocate funding to fortifying network security.³ In the same survey, 45% of organizations report a problematic shortage of cybersecurity skills. This threatens the implementation of their network security projects. Smart organizations will consider both investing in skills development and seeking products that improve operational efficiency.

ESG Lab validated that vArmour DSS can be installed and protecting workloads in less than an hour on any combination of physical, virtual, cloud, or container-based platforms. ESG Lab testing revealed that vArmour provides layer-7 application identification and inspection, enabling operators to identify risks, policy violations, and suspicious behaviors and respond immediately. vArmour provides deep context for application communication to expose not only the connections between entities, but also can abstract rich metadata from those sessions.

ESG Lab also saw vArmour global policy objects protect physical and virtual workloads, providing consistent, automated policy enforcement across heterogeneous environments. Finally ESG Lab confirmed that newly instantiated workloads can be automatically micro-segmented to speed and simplify security operations.

³ Source: ESG Research Report, [2017 IT Spending Intentions Survey](#), March 2017.

Highly Scalable Elastic Platform

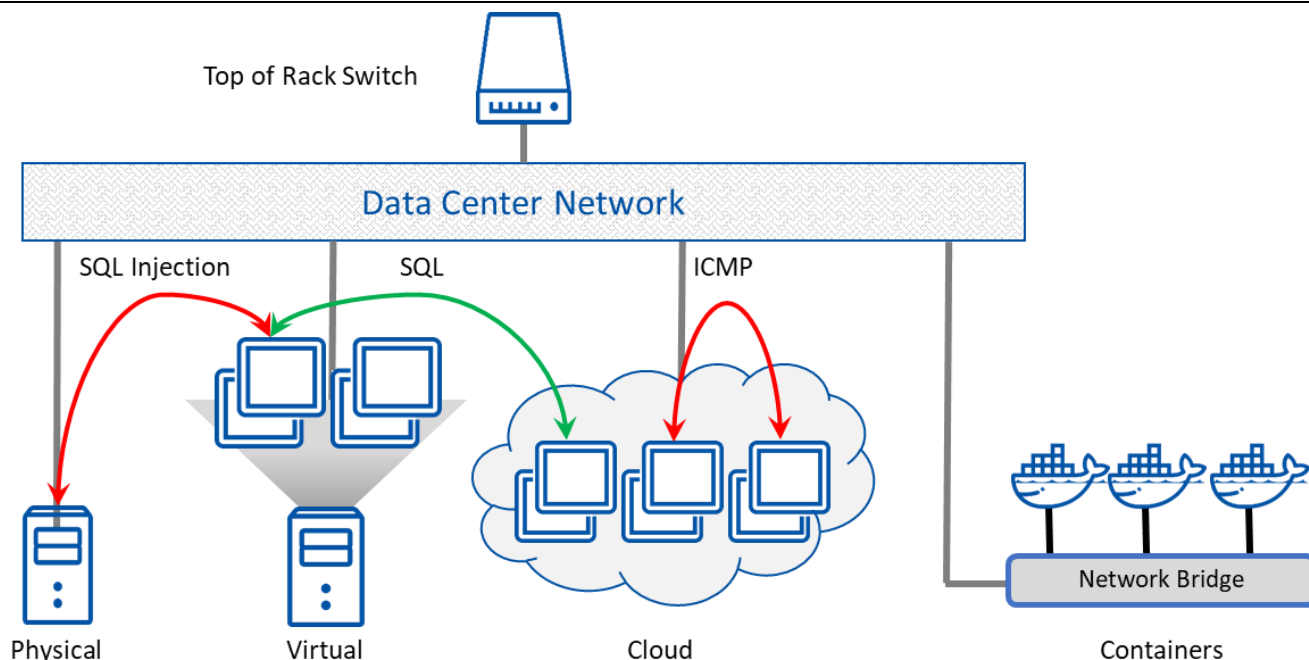
Next, ESG Lab examined the simplicity, elasticity, and scale of the vArmour DSS. An elastic platform should enable building security into the IT infrastructure so that security is tied to compute. If a hypervisor cluster reaches capacity and needs to add more hypervisors, vArmour DSS fabric expansion can be automated to spin up and deploy new EPs through a series of API calls. Since vArmour DSS uses a single policy, there isn't a need to configure the expanded assets with policy as would be necessary with a typical firewall. To put that another way, the vArmour DSS scales automatically to match the compute resources in the environment, which makes it more efficient and easier to manage than traditional approaches where organizations scale by manually adding or replacing single-instance appliances, then manually tune and apply policies to them.

The alternative approaches to delivering layer-7 control require several additional steps compared to vArmour. The first step is deploying an SDN in order to achieve traffic interception adjacent to the workload to deliver micro-segmentation. Next, redirection policy must be configured on the SDN platform to direct the traffic through the layer-7 single instance firewall. Once the layer-4 ports have been identified and the service chain policy configuration is complete, the actual layer-7 firewall policies can be created. Some of the biggest challenges with this architecture lie in managing the aggregated hypervisor traffic. Single instance firewalls are not distributed in nature which means load must be engineered and balanced accordingly. When load capacity is met, analysis must be done in order to engineer growth of the firewall cluster or the firewall size must be increased. This adds cost and complexity and can also present challenges regarding workload mobility. When designing these solutions one must account for the fact that workload moving from one hypervisor to another could mean traffic would flow to a different firewall with a different policy and state table interrupting application availability. This is a very different architecture from the vArmour solution where the layer-7 security enforcement is always local, natively layer-7, and directly matched to the compute platform ensuring that security expansion occurs naturally with the addition of compute. As that hypervisor is deployed, the vArmour fabric and single policy simply expands to support those workloads or any workloads that migrate there.

ESG Lab Testing

Before installing and deploying vArmour DSS, ESG Lab generated unauthorized traffic to illustrate how packets traverse an unfiltered network freely. As seen in Figure 8, the green arrow represents a legitimate SQL connection between a web server and database server in the test environment, while the red arrows show two different types of unauthorized traffic, a SQL injection attack and an ICMP connection between two internal systems.

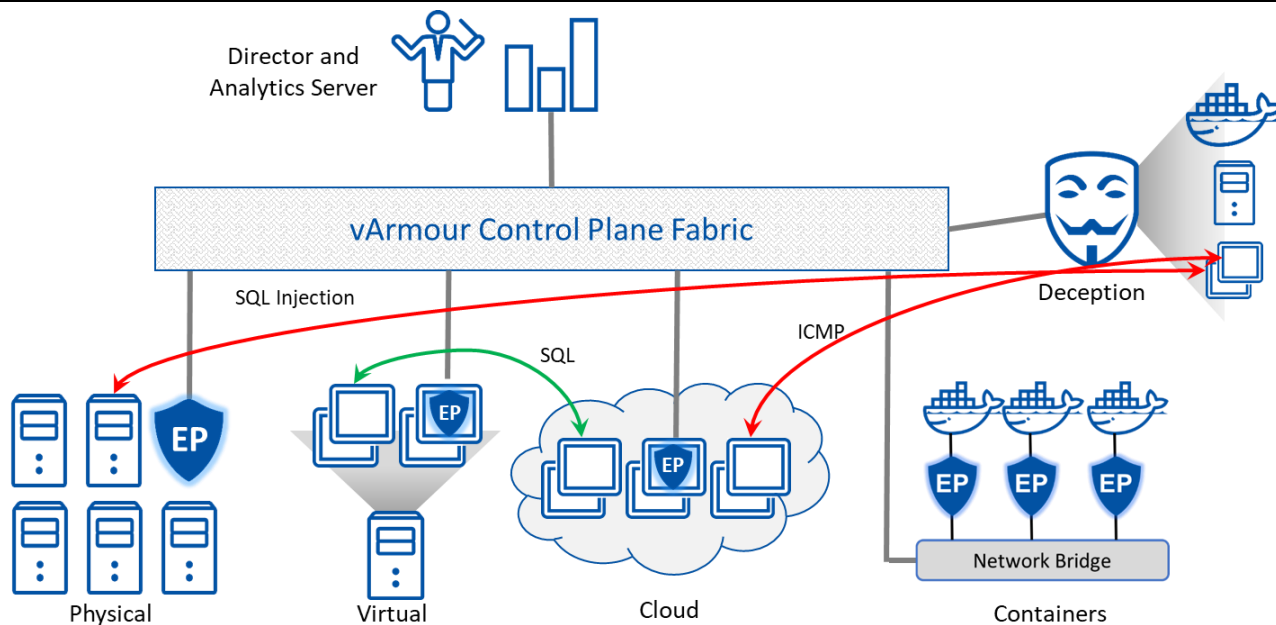
Figure 8. Traffic Between Endpoints without Enforcement Point Protection



Source: Enterprise Strategy Group, 2017

ESG Lab then reran the test after enabling vArmour policies, including workload attributes for SQL traffic and a layer-7 policy to block ICMP via an access list. The policy was constructed to enable only necessary application traffic. Only the web servers could query the SQL server. Since the physical server was not a web server, the physical server's SQL injection attack was automatically redirected to the Deception Point, as was the ICMP stream. This was accomplished without using signatures or detection logic. It was a simple firewall policy violation rule with a redirect to deception action rather than a simple deny rule as a traditional firewall would. This is an important distinction as it means that valid traffic can't be accidentally intercepted by deception.

Figure 9. Traffic Between Endpoints with Inspection, Enforcement, and Deception



Source: Enterprise Strategy Group, 2017

ESG Lab also audited performance and scalability testing of DSS. vArmour Quality Assurance testing is executed for each major and minor release against individual elements and at the system level. Raw and application throughput is measured, as well as the supportable number of concurrent sessions and latency. Automation tests are executed against the system to measure the time needed to automatically micro-segment various numbers of workloads. Testing is performed using Ixia IxAutomate for UDP throughput and IxLoad for TCP and application throughput. ESG Lab analyzed the results of the most recent round of testing and the results are summarized here:

Table 1. Performance Data Published by vArmour QA

Enforcement Points as Tested on Inter-hypervisor VMware vSphere	
Concurrent Sessions per EP	100,000
UDP Throughput (Jumbo Frames, 9,018 Bytes)	19.96 Gbps
UDP Throughput (1,518 Byte Frames)	9.75 Gbps
Enforcement Points as Tested on Intra-hypervisor VMware vSphere with TSO/LRO Enabled	
TCP Throughput (1,518 Byte Frames)	18.7 Gbps
TCP Throughput (AppID)	18.7 Gbps
UDP Throughput (Jumbo Frames, 9,000 Bytes)	19.5 Gbps
Fabric Scalability	
Concurrent Sessions	102.4 million
Number of Hypervisors	1024
Number of Workloads Protected	102,400

Source: Enterprise Strategy Group, 2017

It's important to note that these numbers represent approximately 5-10 Gbps of layer-7 traffic inspection and enforcement per vCPU. vArmour rightfully considers this a differentiator, considering that virtualized traditional NGFWs can require up to 16 vCPUs to support 10 Gbps.⁴



Why This Matters

When ESG asked 641 IT professionals and executives to identify the consideration that would be most important in justifying IT investments, improved security and risk management was the most cited response (34%).⁵ As cybersecurity threats increase in frequency and sophistication, IT staffs and security teams must implement numerous security initiatives, many with manual processes, when the business and technical needs change. It's critical for the security system to rapidly adapt to the ever-changing needs of the business. To address these challenges, the security system must be intelligent, automated, and scalable.

ESG Lab validated that vArmour used a single global policy set to inspect traffic throughout all nodes in the distributed system. Policies were enforced correctly regardless of the location. ESG lab also verified that vArmour could rapidly scale the environment from a security perspective to better align to the changing business requirements of the organization. As the environment grows—requiring more compute—and as hypervisors are added, vArmour can easily and automatically provision and deploy EPs to expand the existing vArmour DSS fabric.

ESG Lab validated the scalability and performance of vArmour DSS, confirming support for more than 100,000 concurrent sessions per Enforcement Point and 100 million concurrent sessions system-wide with the ability to handle nearly 20 Gbps of traffic per Enforcement Point.

⁴ Based on examination of data sheets and documentation of multiple vendors' virtual NGFW offerings.

⁵ Source: ESG Research Report, [2017 IT Spending Intentions Survey](#), March 2017.

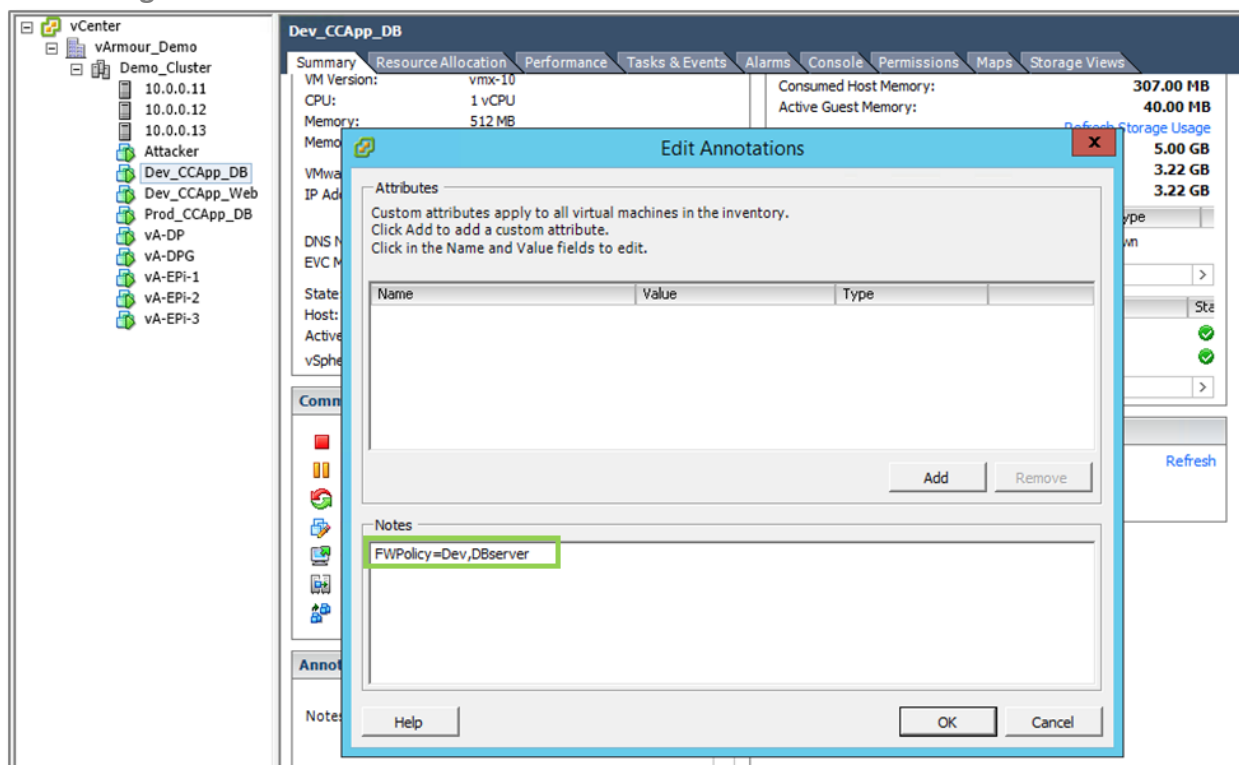
Automated and Extensible Segmentation

vArmour is an all-software, highly programmable platform designed to integrate into Development and Operations (DevOps) workflows for security automation. vArmour is built exclusively on open APIs that enable the platform to integrate into many types of systems of record. For example, ESG Lab looked at vArmour DSS integrations with third-party orchestration and provisioning systems such as vCenter, Cisco ISE, Puppet, and Chef. Likewise, vArmour DSS can integrate with SDNs such as Cisco ACI to provide stateful layer-7 visibility and segmentation, and dynamically consume policies defined in the Cisco Application Policy Infrastructure Controller (APIC). vArmour DSS can also send data to analytic systems such as SIEM tools. The extensibility of the API makes integration with third party tools simple; a customer can create a python script with a few RESTful API calls to vArmour and the other system.

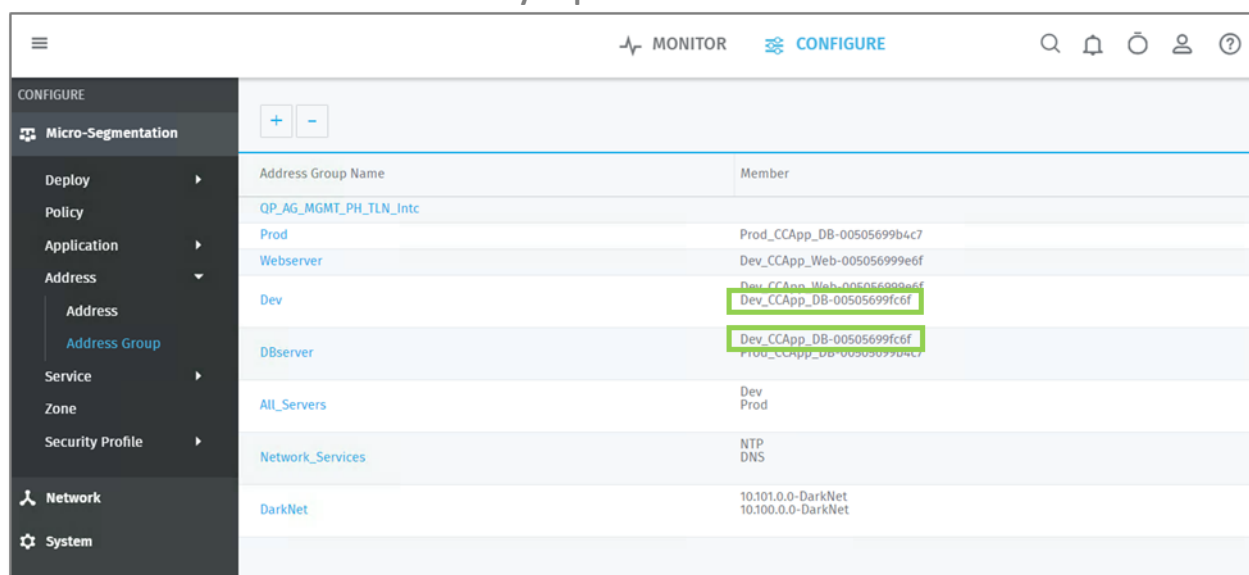
ESG Lab Testing

vArmour can be integrated with any API driven system of record to simplify policy automation. To validate this, we tested automated micro-segmentation and vCenter policy integration. We examined the configuration of a virtual development server for a credit card application called Dev_CCApp_DB. As shown in Figure 10, the **Notes** field contained the string FWPolicy=Dev, DBserver in the **Annotations** section of the vSphere configuration screen for this VM. Through a RESTful API integration these fields are read into the DSS Policy Manager as a development system running a database server. The vArmour Director had a previously configured policy in place—Web2DB—to allow database servers such as Dev_CCApp_DB to connect to web servers. This integration enables a workflow where a new VM can be provisioned in vCenter, automatically micro-segmented, and associated with proper policy without any direct interaction from vArmour administrators to get the workload communicating and protected on the network.

Figure 10. Setting Workload Attributes in vCenter



Next, ESG Lab looked at address groups inside DSS to see how vArmour processes that information. As shown in Figure 11, vArmour DSS automatically recognizes Dev_CCApp_DB as part of the Dev and DBserver groups.

Figure 11. Workload Attributes Automatically Populated into vArmour DSS

Address Group Name	Member
QP_AG_MGMT_PH_TLN_Intc	
Prod	Prod_CCAp_DB-00505699b4c7
Webserver	Dev_CCAp_Web-00505699e6f
Dev	Dev_CCAp_Web-00505699e6f Dev_CCAp_DB-00505699fc6f
DBserver	Dev_CCAp_DB-00505699fc6f Prod_CCAp_DB-00505699b4c7
All_Servers	Dev Prod
Network_Services	NTP DNS
DarkNet	10.101.0.0-DarkNet 10.100.0.0-DarkNet

To change the policy that was applied to *Dev_CCAp_DB*, ESG Lab clicked the **Edit** button for the **Annotations** section on the vCenter management screen, removed *DBserver* from the FWPolicy string (changing it to simply read *FWPolicy=Dev*), and clicked the **OK** button. When the vArmour **Address Group** screen refreshed, *Dev_CCAp_DB* disappeared from the list *DBservers* with no other action required.

vArmour's RESTful APIs enable operators to build security into their automation workflows—examples include interacting with an incident response workflow for quarantining functionality, coordinating with a trouble ticketing system for automated workload provisioning, or integrating into an IP address management solution. ESG Lab also looked at examples of API integrations with orchestration systems and software-defined networks, specifically Cisco Identity Service Engine (ISE) and Cisco Application Centric Infrastructure (ACI). Cisco ISE security groups are automatically imported into vArmour DSS as well as ISE policies. When ESG Lab added a user to Active Directory and included her in an AD group, that user was automatically imported, included in the appropriate address group, and assigned security policies with zero administrator interaction.

ESG looked at how vArmour's integration with Cisco ACI provides scalable, stateful layer-7 segmentation to Cisco ACI. vArmour can consume policy defined in the Cisco APIC to dynamically and automatically integrate operational models while providing layer-7 visibility and control.



Why This Matters

Micro-segmentation enables organizations to granularly protect critical databases, application services like DNS and Active Directory, and compliance-bound workloads like PCI. Segmenting assets with policies that control communication has been in practice for more than a decade. The reason micro-segmentation is much more valuable is because it frees organizations from the constraints of the underlying network and infrastructure. With traditional segmentation, operators can only control traffic based on IP address, port, or VLAN tag. Thus, an organization's architecture and security controls are dependent on their IP addressing and network design. With micro-segmentation, policies are applied at the workload level to every packet that enters or exits that workload, with no dependence on the network topology, the subnet, or the VLAN. This offers both tremendous flexibility and simplicity in terms of policy management and a powerful method of redesigning security controls without network or IP addressing changes.

ESG Lab verified that reassigning a vSphere client to a new segment, and therefore to a new policy, is as easy as changing one field on its management page, without intervention by a vArmour administrator. vArmour can support numerous orchestration and provisioning systems, systems of record, and software-defined networks such as vCenter, Puppet, Chef, and Cisco ISE as well as Cisco ACI.

When administrators include auto micro-segmentation as part of their vArmour configuration, new systems coming online can be automatically brought under management as quickly as they are brought online. This adds value for system administrators, who need not wait for security administrators to approve each system that comes online, and for security teams, who can be confident that appropriate security is being applied to these new systems.

Integrated Deception Security Services

Deception security technologies represent a significant change in approach to network security. Instead of taking a reactive approach to defending a network, deception enables a proactive approach, where attackers and other bad actors are directed away from critical assets and toward virtual assets. An attacker's progress can be slowed, enabling the IT organization to identify the attackers and mitigate before they can reach any real assets.

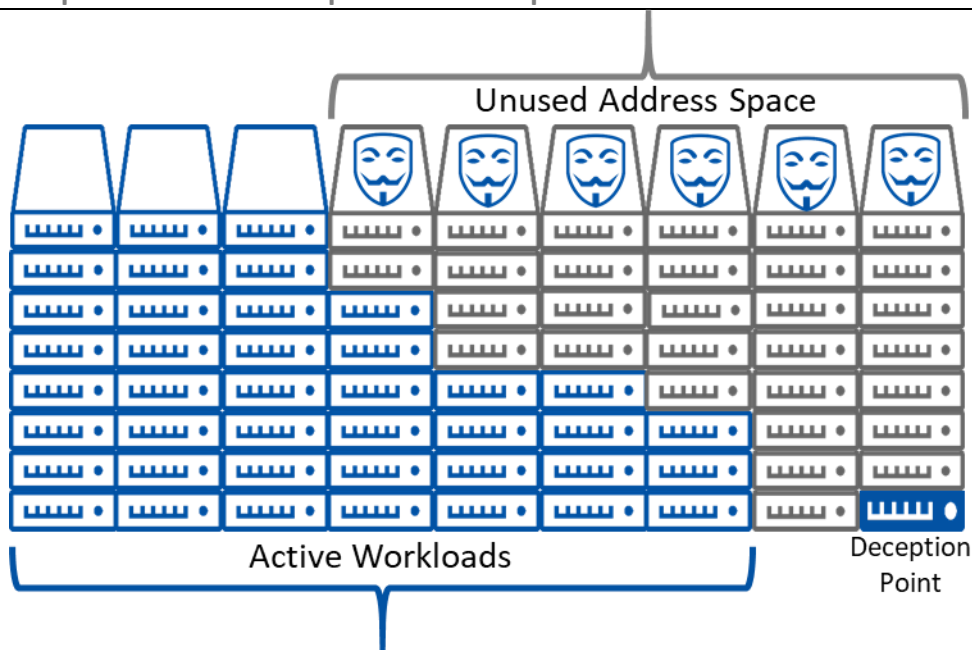
Traditionally, deception is handled through honeypots—systems on the network that look valuable but aren't—and a trail is left by network administrators designed to lead attackers there. Generally, honeypots and their trails require time-consuming work to set up and maintain, and coverage is problematic, since attackers must be lured to them.

vArmour DSS Deception, an integrated security service of the vArmour distributed platform, uses global policies to enable deception. Two key use cases differentiate vArmour DSS deception:

- Unused IP addresses that do not exist that can be leveraged to look like vulnerable workloads by redirecting to a Deception Point.
- Existing real workloads like Active Directory servers or payment applications, where policies can be written to redirect attackers who try to access a real service or protocol that is not allowed to a Deception Point for further analysis about the attacker's intent.

In this way, a single Deception Point can fill the entire unused address space with the appearance of vulnerable workloads, as depicted in Figure 12, and direct attackers to them. The Deception Point itself is secured through vArmour micro-segmentation for added protection.

Figure 12. vArmour-protected Address Space with Deception Enabled



Source: Enterprise Strategy Group, 2017

ESG Lab Testing

ESG Lab began testing vArmour’s deception features by verifying the openness of a test network. Two terminal windows were opened, one running a continuous TCPdump on a server called *critical-asset* on a simulated production network, and the other, on the development network, displaying a shell prompt. First, ESG Lab entered *ping critical-asset* to verify connectivity between the servers; the ICMP requests were shown in the TCPdump session and the *ping* returned successfully. Next, the network security tool *nmap* was invoked to detect ports open and listening on that server. As expected, a list of open ports appeared in the command-line session, and the TCPdump session showed the related server activity. Finally, *ssh critical-asset* opened a command line session to *critical-asset*, and that activity was also reflected in TCPdump.

Next, to begin to protect the network, a darknet was created on the entire 200.0.0.0/8 subnet containing about 16 million IP addresses. A darknet is a range of IP addresses in which no active services or servers reside; the range is used entirely for redirection to a vArmour Deception Point. This is a simple example of the use case defined above to increase the exposed synthetic attack surface. To accomplish this, ESG Lab clicked on the **Create** button on the Policy screen in vArmour Director Policy Manager, and entered the range of IP addresses for which a darknet should be created. Then a policy was created on the same screen so that any traffic originating at any source on the network targeted at the 200.0.0.0/8 subnet would be intercepted by vArmour and redirected to the Deception Point. Once the policy was enabled, the network was created. Thus, the network consisted of about 3,000 real active nodes, and about 16 million synthetic nodes, obscuring valuable systems, workloads, and data from a network scan.

Next, additional policies were added to deny all connection attempts between development and production. In this configuration, a typical layer-7 firewall rule is created in a micro-segmentation environment. Then, ESG Lab re-initiated a *ping critical-asset*, and as that ran, vArmour Director was used to create a policy separating these two networks. Once the policies were in place, the pings began to fail. Network access between development and production was denied.

After proper validation of the normal deny policy, we changed the policy action from deny to redirect—enabling deception. The policies were modified once again, this time to send the once-denied traffic to the Deception Point. As soon as this latest policy change was enabled, the ping picked up right where it had left off, making it appear as though production access had resumed. Running *nmap critical-asset* again returned a perfectly reasonable list of open ports, and *ssh critical-asset* appeared to log into the server. During the *ssh* session, ESG Lab entered *touch ./file* to create a file, followed by the *ls* command to verify that the file had been created. It is worth noting that no TCPdump additional output had been generated since the first policies were enabled. All of this activity took place on the Deception Point, not on *critical-asset*. The real critical asset was protected behind the policy and not receiving any traffic whatsoever.

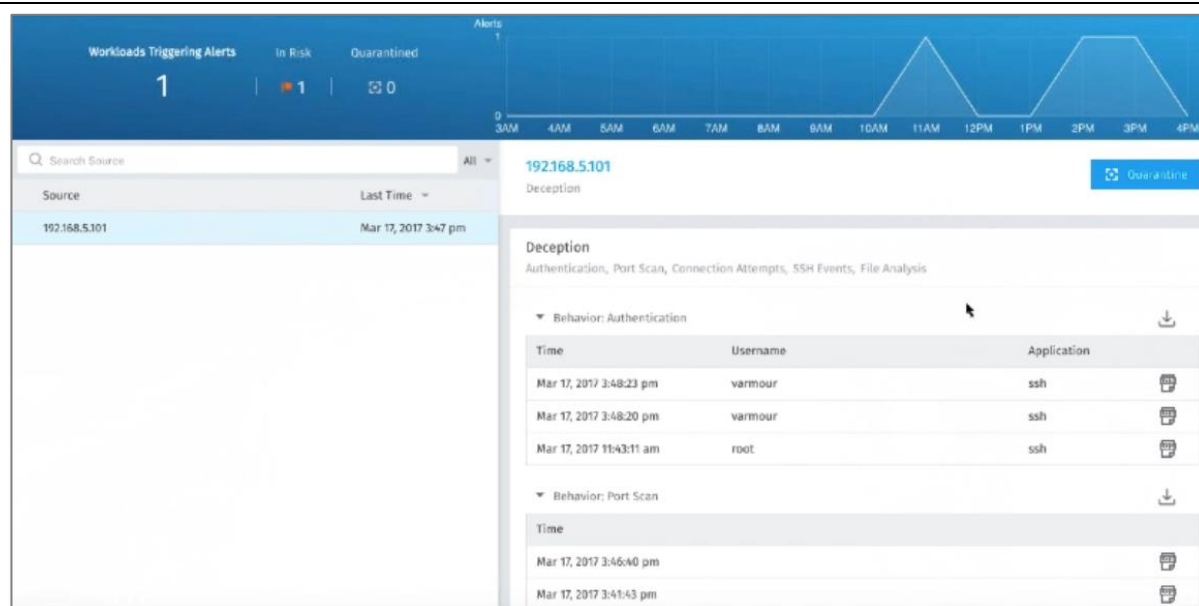
ESG Lab examined vArmour's Deception Manager Dashboard, as shown in Figure 14, to examine the recent Deception Point activity. Clicking on **Analytics** brought up a screen that listed all recent authentication, port-scanning, and *ssh* login attempts. Clicking on the **Log** icon on the far right brought up detailed JSON-formatted log entries for each attempt, as shown in Figure 13. The log entries for the recent *ssh* session included details on the *touch ./file* command, including the full pathname of the file that was created, plus the *ls* command that was run immediately afterward. Finally, ESG Lab clicked the **Quarantine** button on the Deception Manager Dashboard to lock down the system on which the attacker gained access. Once the request was affirmed, that presumably compromised system was immediately cut off from all network contact.

Figure 13. vArmour Deception Event Log

```
Log
{
  "srcport": 46784,
  "sha1": "ad39a3ee5e6b4b0d3255bfe95601890afd807",
  "whitelist": false,
  "filename": "file",
  "sha256": "e3b0c44298fc1c149afb4c8996fb92427ae",
  "sha512": "cf83e1357eefb8bdf1542850d66d8007d620",
  "confidence": 100,
  "full_cmd": "touch file",
  "srcip": "192.168.5.101",
  "time": 1489783750282,
  "cwd": "/home/varmour",
  "username": "dmFybM9lcm==",
  "full_filename": "/home/varmour/file",
  "cmd": "touch",
  "event": "SshCreateFileEvent",
  "workdir": "/home/vadphone/varmour-192.168.5.101-169.254.0.4",
  "md5": "d41d8cd98f00b28d9808998ecf8427e"
}
```

Source: Enterprise Strategy Group, 2017

Figure 14. vArmour DSS Deception Dashboard



Source: Enterprise Strategy Group, 2017



Why This Matters

Deception technology has been in the security administrator's toolbox since the 1990s, helping to slow down attackers, waste their time, and in some cases, give them worthless data. But setup and management of honeypots has always been very complicated, requiring ongoing maintenance of both the honeypot server and of the trail required to lead an attacker there. Thus, despite its potential value, deception tends to be underused in most organizations.

ESG Lab verified that vArmour has made deception much easier and more reliable. vArmour's unique placement of deception technology is distinctly different from legacy deception methods. Instead of requiring a maintained trail of "breadcrumbs" that will hopefully lead an attacker to a honeypot; global policies can be used to transparently redirect attackers to a Deception Point. These servers run a full version of Linux, supporting a variety of standard services, and appear to be a worthwhile target to an attacker. VArmour DSS Deception allows security administrators to truly confuse and fool an attacker, while carefully monitoring progress, offering no data of value, and protecting the real network from further incursions. It's important to note that vArmour's architecture and methodology allows organizations to **cover** an entire network with deception services using a single Deception Point.

The Bigger Truth

In ESG's *2017 IT Spending Intentions Survey*, 39% of organizations that are prioritizing cybersecurity initiatives in 2017 expect to allocate funding to fortifying network security, making it the most cited response. In the same survey, 45% of organizations report a problematic shortage of cybersecurity skills. This threatens their ability to execute on the implementation of these projects. Smart organizations will consider both investing in skills development and seeking products that improve operational efficiency.

vArmour DSS is a distributed platform with integrated security services for the modern cloud and data center. It delivers software-based, application-aware segmentation, micro-segmentation, monitoring, centralized policy modeling, and cyber deception designed to help organizations protect critical applications and workloads. Providing API-driven, distributed, and agent-less security engineered to protect workloads and applications in physical, virtual, cloud, and container environments, vArmour DSS is agnostic to the underlying infrastructure. vArmour's APIs allow integration with a variety of third-party orchestration tools, systems of record, and other custom integrations.

Since ESG's first testing vArmour in 2015, the platform has matured and evolved quite a bit, with numerous new capabilities and enhancements. In this round of testing, ESG Lab validated that vArmour DSS can be installed and providing layer-7 application identification, inspection, and protection of workloads in less than an hour on any combination of physical, virtual, cloud-based, or container-based platforms. ESG Lab also saw vArmour global policy objects protect physical and virtual workloads, providing consistent, automated policy enforcement across heterogeneous environments.

ESG Lab also validated the scalability and performance of vArmour DSS, confirming support for more than 100,000 concurrent sessions per Enforcement Point and 100 million concurrent sessions system-wide with the ability to handle nearly 20 Gbps of traffic per Enforcement Point.

ESG Lab verified that reassigning a vSphere client to a new segment, and therefore to a new policy, is as easy as changing one field on its management page, without intervention by a vArmour administrator. vArmour supports numerous orchestration and provisioning systems including vCenter, Puppet, Chef, and Cisco ISE as well as Cisco ACI.

vArmour has made deception much easier to execute and more reliable too. vArmour DSS can use global policies to transparently redirect attackers to Deception Points where they are presented with interactive services corresponding to the attempted connection, all interactions are captured, and alerts are generated that enable rapid identification and mitigation of attacks.

ESG Lab believes that the vArmour DSS Distributed Security System offers an approach that has already begun to change the way organizations think about protecting their virtual, cloud, and physical assets. vArmour DSS provides simple, scalable, cost-effective security and visualization via automated coarse-grained and micro-segmentation and innovative deception techniques. Organizations working toward simplifying their security operations while improving their network and application controls and their overall security posture would do well to take a close look at vArmour DSS.

Appendix

Table 2. ESG Lab Test Bed

vArmour Fabric Components	Version
vArmour Director	3.1
vArmour Enforcement Point (EP)	3.1
vArmour Deception Point (DP)	3.1
Analytics	Version
vArmour Analytics	3.1

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. 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 The Enterprise Strategy Group, Inc., 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 ESG Client Relations at 508.482.0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

