illumio

Securing High Value Assets in the Federal Sector with Micro-Segmentation

WP201903

Today's federal IT leaders are faced with a broad range of challenges for securing their applications and environments. For example, agencies in the middle of migrating legacy applications to the cloud and/or deploying new cloud-native applications, as part of efforts to modernize government services, are under pressure to keep up with FISMA, DHS, NIST, and OMB guidelines. Agencies are strongly advised to obtain visibility into the open connections in these environments and to segment high value assets (HVAs) to maintain their security posture. This is also often referred to as zero-trust. The talent and resource constraints these agencies face add another dimension to these challenges.

Historically, security investments have largely been focused on prevention and detection. With the adversary always staying one step ahead, NIST asserts they are either already inside or will be in the near future, and that the average dwell time inside perimeter defenses is 80-100 days before detection. As a result, NIST recommends the following posture: "Assume adversary will compromise system."[1] This mindset shifts the emphasis from detection and prevention to containment and remediation, which is often called cyber resiliency, where the focus is to limit bad actors' ability to traverse the internal network and reach HVAs by adopting a zero-trust architecture. Micro-segmentation is a foundational component of this containment approach and is quickly becoming standard good hygiene for any security-conscious enterprise. During the Gartner Security and Risk Summit 2018, Neil MacDonald named "microsegmentation and flow visibility projects" as one of the top 10 critical security projects that CISOs should consider to reduce risk and have high business impact.[2]

Challenges in Securing High Value Assets

OMB, NIST, and DHS are striving to segment and secure every HVA in the federal government. In December 2016, OMB released Memorandum M-17-09 to agency executives advising them to identify their HVAs with

1 "Building Cyber Resilient Systems, A National Security and Economic Imperative" Dr. Ron Ross, May 2018
2 "Top 10 Security Projects for 2018", Neil McDonald, Gartner Security & Risk Summit 2018

the intent of better understanding their level of risk and vulnerability. In September 2017, the ACT released the final version of the IT Modernization report wherein it emphasized the need for federal agencies to prioritize their HVAs, assess their level of risk, and begin taking steps to reduce exposure. More recently, in May of 2018, DHS issued a Binding Operational Directive focused on requirements for federal agencies to protect HVAs through proper access controls, configuration management, vulnerability scanning, and by segmenting them from other network traffic.

In order to effectively secure HVAs, agencies need to be aware of and have a plan for addressing the following challenges:

- Visibility into the application, its behavior, its relationships to other systems, and vulnerability exposure.
- Limitations of using perimeter-centric security inside data center and cloud environments.

Understanding Application Dependencies and Connections

Whether migrating legacy applications to the cloud or segmenting HVAs, cloud and security teams must keep systems operational while achieving these objectives. Most organizations have little idea how their applications actually work; for example, what roles, applications, and application tiers are allowed to communicate with a critical application. This poses obstacles and challenges for cloud migration and security teams to meet segmentation requirements.

Figure 1 is an example of a data center with 15 applications across 80 workloads with thousands of connections (red and green lines). Trying to solve this problem for thousands of workloads across on-premise data centers and public clouds with a full portfolio of HVAs is what the typical federal agency is up against.

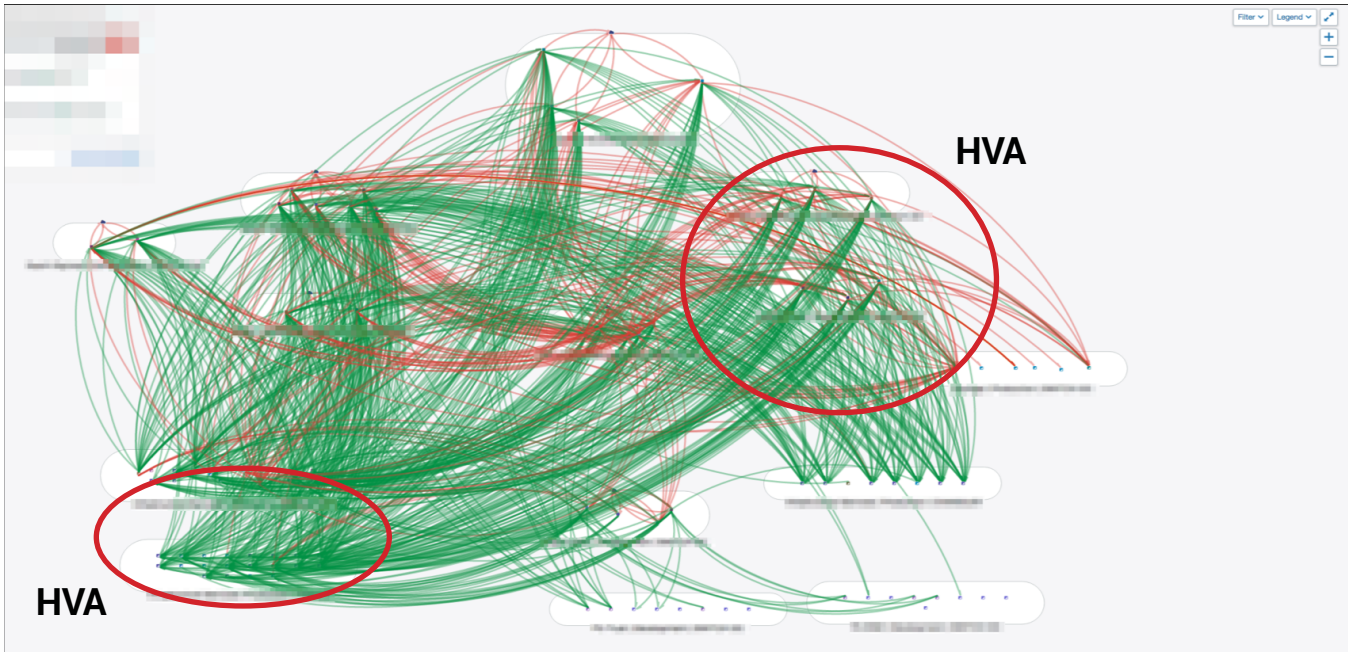

Figure 1: An example of a data center with 15 applications across 80 workloads with thousands of connections.

Visibility First

An important step to addressing this problem and meeting the DHS Continuous Diagnostics and Mitigation (CDM) Phase 3 requirements is building an application dependency map to gain visibility into how applications are connected and communicating. With a real-time application dependency map, teams quickly understand relationships and dependencies between applications and their individual components. This leads to a greater understanding of application groupings, their classification, and upstream and downstream relationships – and ultimately provides the ability to block unnecessary connections without breaking applications. This visibility also provides the impact analysis required to migrate these systems to the cloud. Figure 2 below shows an example of a federal agency's data center environment with micro-segmentation implemented. The red lines show intra-application traffic where there are no existing policies to allow applications to communicate. The green lines indicates traffic that conforms to defined segmentation policies. With this view, permitted connections are easily understood, HVAs are properly secured, and compliance mandates can be met.

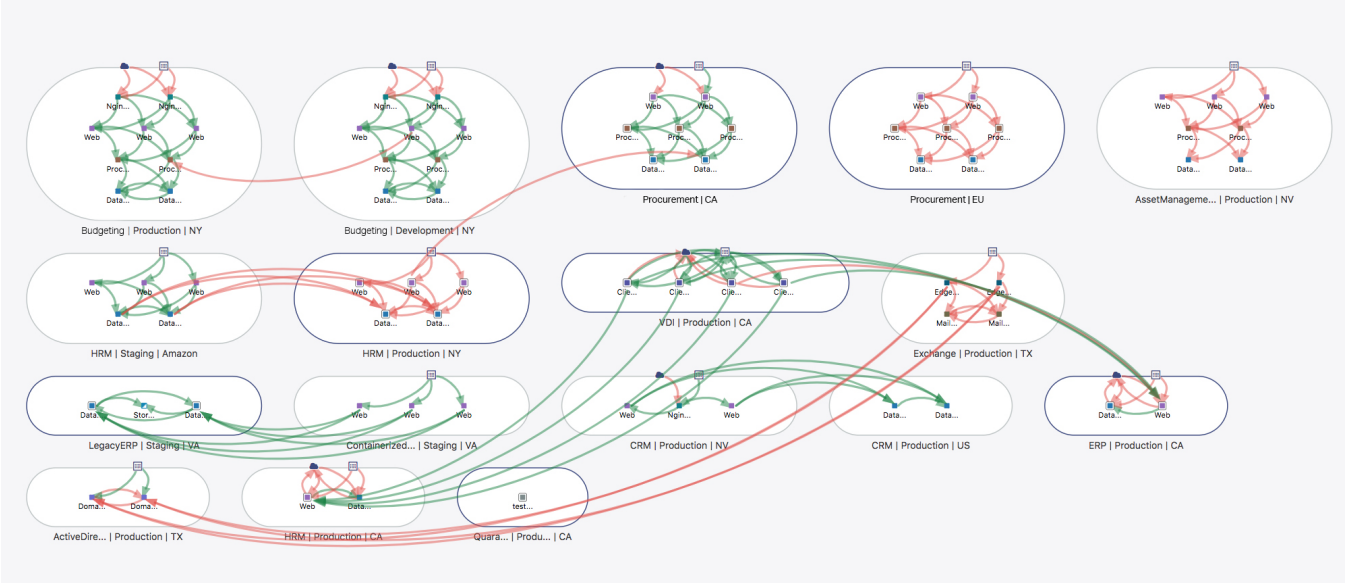

Figure 2: Example of federal data center with micro-segmentation.

Today's federal IT computing environment consists of legacy data centers, cloud environments (GovCloud), multiple hypervisors and computing platforms, bare-metal servers, and emerging technologies such as containers. Gaining visibility across this highly distributed and diverse landscape has historically been unattainable.

To extend the value of this visibility, application dependency maps can be augmented with vulnerability information. Traditionally, security analysts prioritize vulnerability remediation based on the criticality scores the cyber scanning tools calculate. These tools look at each host alone and do not contextualize them into their broader mission (application) in their calculations. Overlaying vulnerability information on top of the application dependency map builds a vulnerability map that enables analysts to prioritize high risk applications and the exposure of vulnerabilities in those applications. If the security team is unable to immediately issue a patch, they could apply the more granular process-based micro-segmentation as a compensating control.

Enforcement Next

Visibility is only one part of the solution. Once the application dependency map is established, IT teams must determine how to enforce policy and

better secure their critical assets. Traditional network-based enforcement points are very expensive, requiring organizations to change their network infrastructure and creating massive amounts of complexity implementing and orchestrating firewalls and thousands of firewall rules. It is now widely accepted that a perimeter-based firewall approach is too complex, costly, and manual, and ultimately is not feasible to meet the visibility and security needs of cloud migrations or to segment federal HVAs.

The Illumio Adaptive Security Platform® (ASP) solves the challenge of delivering visibility and using that visibility to drive segmentation – with no dependency on the network.

Host-Based Micro-Segmentation with Illumio

Micro-segmentation is not intended to replace your perimeter firewalls or any other infrastructure you may already have in place but, as previously mentioned, using perimeter-centric segmentation to control traffic within the data center can become complex and unwieldy. Host-based micro-segmentation will help you get more value out of the existing investments across your infrastructure.

The Illumio Adaptive Security Platform takes a unique host-based approach to greatly simplify the process of visualizing and securing HVAs within distributed, multi-platform computing environments – without having to modify the existing network or infrastructure.

Figure 3 graphically illustrates Illumio ASP's approach to micro-segmentation:

- Illumio ASP is infrastructure agnostic. By focusing on the compute, Illumio enables micro-segmentation across bare-metal, virtual machines, containerized hosts, load balancers, and cloud security groups.
- Illumio ASP is software based. It does not require additional investments in new appliances, rearchitecting of the network, or upgrades to existing infrastructure.

- The Virtual Enforcement Node (VEN), a lightweight agent deployed on workloads, collects and sends telemetry data to the Policy Compute Engine (PCE) and takes segmentation policies from the PCE to program the native stateful Layer 3/Layer 4 firewalls in the host OS.
- The PCE is the "brain" that takes telemetry and traffic information about the hosts to create a real-time application dependency map (Illumination) and calculates the optimal micro-segmentation policy.
- Vulnerability maps integrate vulnerability scan data like Qualys into the application dependency map to generate an East-West exposure score. The East-West exposure score was developed by Illumio to show the number of hosts that can potentially connect into a vulnerability and can potentially exploit that vulnerable host. Security can use this information to prioritize patching or tune micro-segmentation policies as a compensating control when it is not possible to issue a patch immediately.

Note: The Illumio ASP platform is FIPS 140-2 compliant and in evaluation for Common Criteria certification.

Illumio Adaptive Security Platform® Architecture

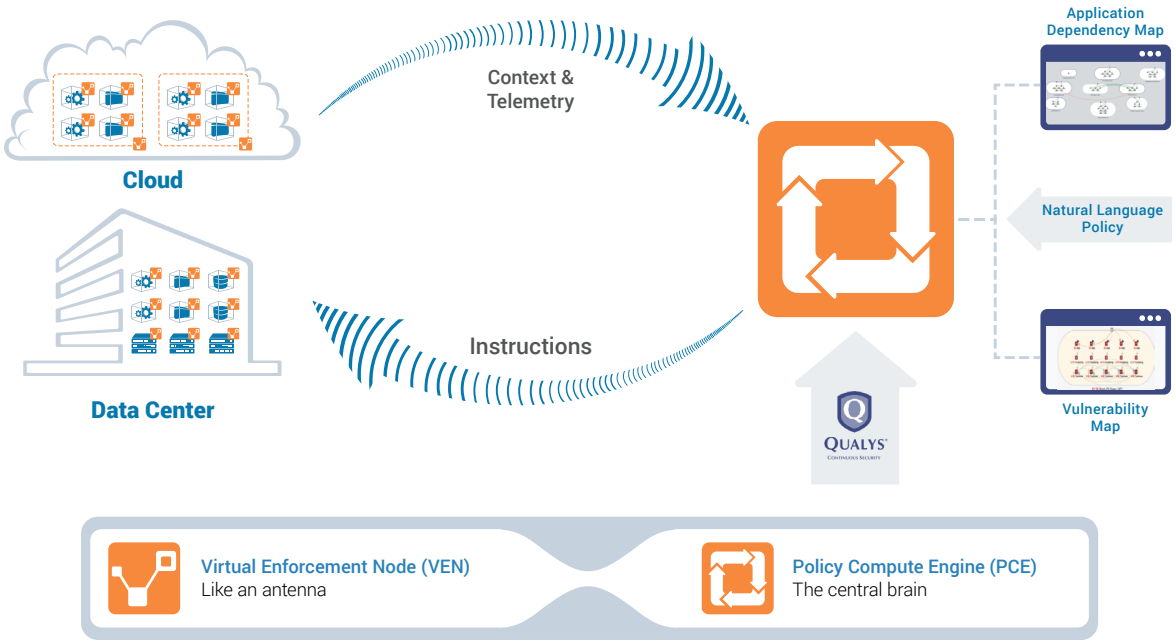

Figure 3: Overview of the Illumio Adaptive Security Platform architecture.

Summary

Federal IT leaders are facing the challenge of modernizing IT infrastructure by migrating to public clouds, improving cyber resiliency, and complying with the impending mandates to secure their high value assets. Micro-segmentation is a proven mitigating strategy to gain visibility across these distributed environments, shut down the attack surface, and reduce the exposure of their most critical assets.

To effectively meet these requirements, a micro-segmentation solution must:

- Provide full visibility of application traffic across a highly distributed computing landscape.
- Be able to secure multi-platform, heterogeneous computing environments.
- Reduce the need to install, configure, and maintain additional firewalls.
- Be able to overlay the application dependency and traffic flow map with vulnerability scan data and use this insight to prioritize patching or update micro-segmentation policies as a compensating control.
- Use natural language to define rules and be able to easily tune policies to miminize the East-West exposure score.
- Apply the right level of granularity to the micro-segmentation policy.
- Be simple to set up and maintain, with minimal required resources.
- Be economically viable.
- Map to the NIST Cybersecurity Framework.

illumio

LEARN MORE

Find out how real-time application dependency and vulnerability maps enable you to visualize the upstream and downstream application relationships, understand the East-West exposure and use this information to effectively secure your high value assets by downloading the following solution briefs.

- Application Dependency Mapping
- Vulnerability Maps

Follow Us

About Illumio

Illumio, the leader in micro-segmentation, prevents the spread of breaches inside data center and cloud environments. Enterprises such as Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite use Illumio to reduce cyber risk and achieve regulatory compliance. The Illumio Adaptive Security Platform® uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with micro-segmentation that works across any data center, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. For more information about Illumio, visit www.illumio.com/what-we-do or follow @Illumio.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085 Tel (669) 800-5000 www.illumio.com