illumio

## BEST PRACTICE GUIDE:

# How to Secure Your Crown Jewel Applications

WP201809

illumio

This guide outlines why and how large enterprises are using application dependency mapping and micro-segmentation in association with the NIST Framework to secure crown jewel applications.

**August 21, 1911:** The most valuable piece of art in the world – the crown jewel of paintings – was stolen from its home in the Louvre Museum in Paris. The morning after the theft, an artist went into the salon to admire the Mona Lisa and saw only four pegs in the wall. In the two years that it was missing there were queues outside the Louvre – not to see the painting, but to see the spot that it formerly occupied.

The ramifications of the loss were staggering. Guards were fired, the Louvre was closed for a week, and the chief of police in Paris was also fired as the theft on his watch was considered a national disaster.

Eventually, the masterpiece was recovered inside the hotel room of a former employee who had pulled off the heist with help from a group of collaborators.

Security around the Mona Lisa changed dramatically after the theft. Instead of being wide open in a salon, it has sensors and barriers, and viewers are limited in how they can enter and exit the part of the museum it occupies. These are countermeasures against theft, but today bulletproof triple-laminated glass also protects her from accidental damage and intentional vandalism.

What's the relevance of this sensational theft to today's cybersecurity landscape? Most organization's crown jewel applications are wide open within their data centers and cloud environments – just like the Mona Lisa of 1911.

Every organization has crown jewels. They may go by names such as toxic assets, high-value assets, critical assets, or mission critical systems. Examples include:

- Customer account information
- Employee information
- Active Directory
- Client data
- Document management system (DMS)
- Personally identifiable information (PII)

- Healthcare records
- Payment systems
- Sensitive designs or intellectual property
- Billing information
- Other financial information

If you are responsible for information security and hope to avoid the fate of the 1911 Parisian chief of police, you should be asking: What are the steps to protect my information crown jewels?

## Step 1: Identify the Crown Jewels

While seemingly obvious, the classification of your high-value assets may be different depending on the stakeholders within an organization. If an organization has not undertaken this effort, the first step is to bring together key stakeholders:

- CISO
- Risk and governance
- Key business stakeholders
- Legal
- Finance

The goal of this team is to map the risk of the assets and applications within the company's infrastructure. A good way of doing this is to look at the NIST Cybersecurity Framework (CSF). A risk assessment should be performed. NIST describes this effort:

**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

**ID.RA-4:** Potential business impacts and likelihoods are identified.

In enterprises, the metric is frequently put in dollar terms (the loss of revenue or cost of post-breach recovery and remediation). For most organizations there is a reputational impact to consider.

For example, if a crown jewel application has all of an organization's customer data, an equation that might be able to describe the business impact of loss of the crown jewels could be:

$ value of each customer (in terms of customer acquisition) + $ cost of breach remediation in customer contracts + $ cost of speaking to the customers about the breach × # of customers

In a business-to-business scenario, if the cost of customer acquisition is $15,000 dollars, the customer has a breach remediation of $50,000 dollars, the cost of dealing with the customer is $15,000 dollars, and the company has 4,000 customers, the total value of the crown jewel would be:

$15,000 Customer value + $50,000 Breach remediation + $15,000 Notification costs × 4,000 # of customers

= $320,000,000

This simplified equation does not include customer revenue and customer churn as a result of the breach. It does not take into account penalties that a customer might pay because of breach of privacy regimes like GDPR.

# Step 2: Determine the Best Protection or Control

There are many layers to protecting a crown jewel application. These include identity and access management (IAM), vulnerability management, and segmentation. Ensuring that your organization has a good identity and access management program that uses two-factor authentication is a good start. Ensuring that vulnerabilities on crown jewels are aggressively managed is another win. However, patching vulnerabilities can be especially difficult because the crown jewels may not be able to be patched for any number of reasons (production freeze, no patch available, or the patch would break applications).

Segmentation is another control that many organizations are turning to that fits into the NIST CSF as follows:

**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

## WHY SEGMENTATION FOR CROWN JEWEL APPLICATIONS?

Segmentation ensures that crown jewels can only be accessed from authorized devices and those devices only have access to specific business processes on the critical applications.

The remainder of this document will focus on segmentation and micro-segmentation (sometimes referred to as "ring-fencing"), an area that yields big wins in protecting crown jewels. Many organizations are using it to protect their most valuable applications and assets and here's why.

While traditional firewall solutions protect network perimeters, the valuable applications, databases, and communication pathways between devices on the network are wide open. We know that perimeter firewalls are often breached, allowing threat actors to roam relatively unimpeded to conduct

reconnaissance across the network. The benefit of using segmentation to protect crown jewels is that organizations control the devices that can connect to the crown jewels. A very common technique that bad actors employ to compromise an application is to move from a low-value application or asset to a high-value asset. Segmentation ensures that you are creating secure enclaves within which crown jewels can run. This dramatically reduces risk. If an organization's crown jewels fall within a compliance regimen such as SWIFT or PCI, segmentation is absolutely required.

While the benefits of being able to apply specific restrictions to important assets within an otherwise open network should be obvious, exactly how to achieve it is a stumbling block for many organizations. The rest of this guide lays out steps to get to that happy, secure state.

## Step 3: Identify Potential Solutions

Determining a set of solutions to address the segmentation problem begins with identifying key stakeholders that may be called upon at different points in the journey. Following are some of the titles that will likely be needed along with why:

| Title | Role in determining micro-segmentation solution |
|---|---|
| Security Engineering | Provide insight into integration with full security stack; key stakeholders in engineering the final solution. |
| Network Engineering | Many of the solutions in the segmentation space are attached to the network; therefore, they may ultimately own the solution. |
| Application Teams | Because they are the teams that own the applications and understand how they operate and run, they will need to be consulted on normal 'baseline' behavior and rules. (More information provided below.) |
| Server Platform Teams | Much like network engineering, depending on the solution that is ultimately chosen, they may have a part to play in the final solution selection. |
| Security Operations Center | The solution to protect crown jewels will need to be integrated into the overall security operations center (e.g., threat intelligence, vulnerabilities management, and security event monitoring and investigations.) |

The team should get together to look at the solutions that are available in the market. It is highly recommended that the team look at different approaches from different vendors. It is important to remember that segmentation is an emerging market. Traditionally, organizations just used firewalls, subnet, and zones to protect applications, but because the threat landscape has changed and compute has evolved, new solutions have evolved to solve the problem of segmenting applications (crown jewels) sitting in existing data centers and public clouds.

**A high-level overview** of the different approaches are as follows:

- **Network based** – This requires using traditional firewalls, and may require changing IP addresses, subnet, zones, and VLANs.
- **Hypervisor based** – These solutions use the virtual switch within the hypervisor as the enforcement point.
- **Host based** – These solutions use the native stateful firewall within the host for enforcement.

It is highly recommended that the team looking at solutions bring in at least one vendor for each category.

At this point, the organization has a list of what assets need to be protected and an idea of the different approaches.

# Step 4: Important Considerations

It is important to remember that the goal of the project is to protect the crown jewels sitting within the data center and/or public cloud. Segmentation, as a technology, first identifies and isolates crown jewel applications and maps the normal flow of traffic into and out of them. Once this baseline is established, the solution provides capabilities to filter traffic to reduce the exposure of the crown jewels to bad actors.

## BUILDING AN APPLICATION DEPENDENCY MAP

The crown jewels are the most important applications running in an organization. Protecting the crown jewels should not result in breaking them. Determining how those applications work through mapping normal

workflow traffic (i.e., establishing baselines of acceptable traffic) will ensure that when segmentation is enforced, it doesn't break the application. This is where involving application teams to define what is normal is so important. Ideally, the solution has capabilities that will enable a wide range of application SMEs across your organization to be able to easily use the tool to review and lock in normal traffic patterns they are observing.

As an added bonus, determine if the application dependency map also includes integration with vulnerability management. This will allow you to measure the risk and exposure of unpatched vulnerabilities – thereby bringing segmentation and vulnerability management together.

## INTEGRATING INTO WORKFLOWS

There is an end state to protecting the crown jewels at which point policy violations should be sent to the SIEM and will be acted upon by the security operations center (SOC). SOC teams want to ensure that they will not be inundated with false-positive indication of compromise alerts due to overly-restrictive rules on what turns out to be normal traffic flows. Again, this is why it is crucial that your solution allows application SMEs to do thorough analysis to map baseline flows. Ideally, your solution will allow traffic restriction rules to be run in production, but initially in a test mode that would expose volume of alerts and allow adjustments to be made as necessary.

## MINIMIZING DISRUPTION

While all solutions have the ability to solve the crown jewels problem, don't lose sight of a solution forcing an organization to change underlying infrastructure. You must remember that the goal is to protect the crown jewels, but not disrupt them. For that reason, the team must evaluate the disruption caused by security. Often security throws the hammer down insisting on "needing" something. In this  case, throw away the hammer – the application dependency map will allow a scalpel to be applied that does not disrupt the crown jewel.

## METADATA

All micro-segmentation solutions work on some form of label metadata. This is because static IP address policies are brittle and break when an application changes IP addresses. Generally more robust policies can be written when using some form of tagging, labelling, or metadata. The question is how does the solution use these labels, tags, or metadata – how does this fit into an organization's operations? This is an important consideration.


# Step 5: The Bake-Off

Determine the requirements for the solution, map those requirements into a test plan, and bring in at least one solution from each category for testing. Why? Because each solution will have its puts and takes, and only by looking comprehensively can an organization measure the cost, impact, and capabilities of each solution.

After the bake-off, look at the broader impact on the organization. How many full-time employees will it take to deploy and then run?

Insist on talking to other organizations that have the same size deployment and are fully enforced. Learn about the time it took to get to a fully-enforced infrastructure protection solution operationalized. If asked, peers in other organizations will tend to tell you about their struggles. Vendors will likely direct you to their customers they know will give "glowing" references, so if possible talk to industry analysts or try to find others that have adopted the solution but were not suggested by the vendor you are investigating.

# Step 6: Get Bids

Insist on getting bids from each financially viable vendor who is able to solve the problem. Clear and objective metrics against a framework like NIST CSF controls are important.

Ensure that the team has looked at the scope of the deployment and ask for a bid that fully addresses the solution from each vendor.

Get an estimate on time-to-implement from each vendor and ensure that all stakeholders have buy-in on the time and cost to implement and then operationalize.

## Step 7: Evaluating the Cost of Protection

Protecting a crown jewel asset is not free. Protecting the asset will likely require some form of investment in technology, but there will also be a cost in people and process. Sometimes the total cost of protecting the crown jewels is higher than the anticipated business impact of a successful attack against them.

Organizations should measure (in dollars) the business impact in terms of people and process change, in addition to supporting technology costs. If the total implementation costs of a micro-segmentation solution exceed the estimated loss from a successful attack, it will be hard to get approval. As such, you'll want a solution that includes sophisticated cost-saving usability features in addition to effective protection functionality.

A classic example of this is data loss prevention (DLP). For highly complex organizations, doing a full DLP implementation is very expensive in terms of people and process, and a risk team may determine that the cost of the DLP control is more expensive than the loss of the data itself.

Once the crown jewels have been identified and the size and scale have been identified, it is important to look at the cost of the segmentation implementation. A simple way of making an assessment is to ensure that the cost of protection is far less than the potential business loss or risk so that the following equation holds:

**$ Risk – $ Cost of Control > 0**

(includes people, process change, and cost of technology)

## A THOUGHT ON HOST-BASED SOLUTIONS

Classic infrastructure vendors have come to realize that their customers are decoupling from their infrastructure (i.e., network and hypervisors). The move to public and private cloud has made this an inevitable part of the future. Most organizations have some type of public cloud initiative – and those initiatives force an organization to decouple from micro-segmentation that's based on hypervisors or switch ports. For instance, if an organization's entire micro-segmentation strategy is focused on network-based enforcement, they may have to rethink that strategy should they move to public cloud in the future.

That's why it is important that every infrastructure vendor now has a host-based solution for micro-segmentation.

# Conclusion

Protecting an organization's most valuable assets or crown jewels is essential to protecting the organization from adverse monetary, reputational, and business continuity impact.

One of the best ways to look at protecting the crown jewels is through the NIST Cybersecurity Framework, which provides a clear, prescriptive, and risk-based approach.

It's also important to take a methodical, open, and collaborative approach to looking at potential solutions to protecting crown jewels. The analysis should begin with defining the estimated cost of a successful attack against your organization. This value serves as the comparison point against which the total cost of any micro-segmentation protection solution must be compared. Only through a fully thought-out, risk-based process can an organization achieve success.

# Why Illumio?

Illumio has developed real-time application dependency mapping and micro-segmentation technology that prevents the spread of breaches inside any data center and cloud.

## WHAT DOES ILLUMIO GIVE YOU?

### BEYOND NETWORK VISIBILITY: SEE YOUR CROWN JEWEL APPLICATIONS IN REAL-TIME

Many vendors in the security industry offer greater "visibility" to your network. Illumio uniquely provides real-time application dependency and vulnerability maps across all your data center and cloud environments showing traffic flows, and which applications are connecting to vulnerable ports. This real-time visibility provides a foundation for creating the ideal micro-segmentation strategy.

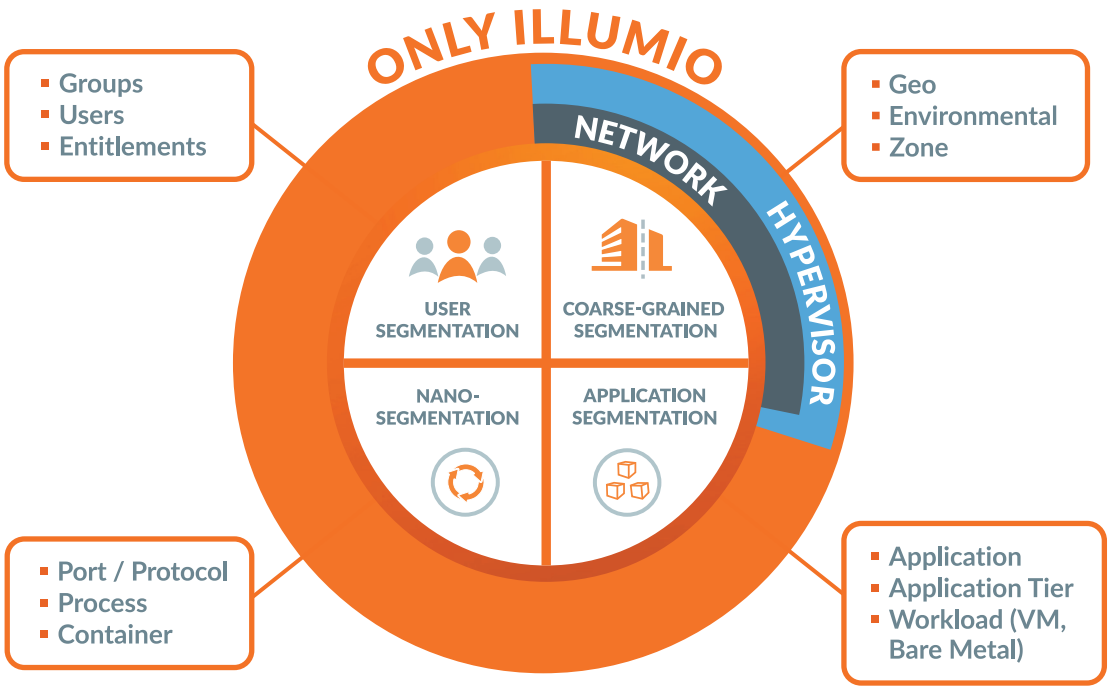
- See a real-time map showing how applications are communicating across all your data centers and cloud environments, and which applications are connecting to vulnerable ports.
- Get an East-West exposure score that's calculated based on how many upstream workloads can potentially exploit the vulnerabilities on a given workload.
- Understand application behavior and common service dependencies (e.g., Active Directory, Exchange, DNS).
- Model security policy and receive real-time visual feedback to eliminate risk of breaking applications with new enforcement policies.

### MICRO-SEGMENTATION WITHOUT ANY NEW HARDWARE AND INDEPENDENT OF THE NETWORK

Imagine that a firewall already exists in front of every server, virtual machine, container, or network port in your data center and you could manage all of them simply and automatically at scale – Illumio turns them all into sensors (see what's communicating) and enforcement points (control what's communicating).

Illumio's micro-segmentation technology lets you choose the level of segmentation that is right for your environment to protect your crown jewel applications. We offer the widest range of segmentation options available without all the manual work normally associated with traditional segmentation.

- Get control of lateral (East-West) traffic by turning every host into a sensor that detects unauthorized traffic and an enforcement point that prevents the spread of breaches.
- Know your optimal enforcement policies using Policy Generator, which recommends micro-segmentation policies based on vulnerability data paired with application traffic.
- Securely connect within and between cloud environments and private data centers with the only policy-based IPsec encryption.



# GET STARTED WITH ILLUMIO

1. Take a guided tour of the Illumio Adaptive Security Platform®.
2. Try it out with a 30-day free trial.
3. Get a custom technical demo from a micro-segmentation expert.

Go to: illumio.com/testdrive

## About Illumio

**Follow Us**

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. 160 San Gabriel Drive, Sunnyvale, California 94086 Tel (669) 800-5000 www.illumio.com