illumio

Illumio for IT

By Justin Warren

ST201702

About the Author

Justin Warren is Chief Analyst and Managing Director of PivotNine, a firm that advises vendors on positioning and marketing, and customers on how to evaluate and use technology to solve business problems.

He is a regular contributor at Forbes.com, CRN Australia, and iTNews, and provides expert commentary to other media organizations. He writes and speaks extensively about the IT business and tries to help customers and vendors alike to navigate the often bewildering landscape.

Justin holds an MBA from Melbourne Business School, where he received commendations for Brand Management and Marketing Strategy, and an Award of Distinction for academic excellence. He is a graduate member of the Australian Institute of Company Directors.

illumio

Table of Contents

Why Illumio?

Before the firewall era, servers connected directly to each other and controlled access to services using host-based methods, like iptables or IPFilter. These host-based firewalls were complex to manage at scale because every change required updating the configuration on each affected server by hand. Instead of having to maintain a multitude of host-based firewalls, the firewall function was moved into a dedicated device (a perimeter firewall), and the firewall era was born.

Since then, the dominant approach to controlling activity and protecting the data center has been with perimeter firewalls and in the network with VLANs and Access Control Lists (ACLs). Instead of manually updating configuration on a dynamic and ever-growing fleet of servers, configuration could now be managed across a handful of firewalls at the perimeter and switches across the network.

The benefits of the concentration of controls also came with a cost. The servers on the protected 'inside' now had few defenses against attacks, and became reliant on a strong firewall. Pass the firewall, and suddenly an attacker could have access to move latterly across the entire internal network.

To solve this new problem, internal networks were segmented and more firewalls were added to help protect servers from each other. An attacker attempting to traverse from a web server to the database server – known as lateral movement – now had to cross multiple, internal firewalls.

Increasingly, firewalls and controls in the network policed what traffic was allowed, and what wasn't, using complex ACLs, traffic inspection, and filtering techniques. Unfortunately, configuring firewalls and architecting networks with a complex set of ACLs and VLANs is a complex business.

Firewall policies and ACLs are difficult to craft by hand, and the multitude of services that require data access across these borders has made them long and complex.

The arrival of virtualization made the problem worse. Instead of crossing a physical network device – a firewall – to move from one server to another, virtual servers all lived inside the same physical environment. Virtual firewalls helped a little, but now figuring out which server was in which segment became more challenging, and the number of firewall devices, each needing separate configuration, became unmanageable.

We now find ourselves back at the beginning: complex network architectures, a multitude of devices acting as choke points, each requiring separate management and a complex list of policies. As application environments have become more dynamic and demand more agility, this rigid approach to security has started to break down.

What if we could have the added protection of host-based firewalls without complex networks and the administration headache? What if we could complement our perimeter devices with a distributed network of adaptive firewalls that live inside the hosts, monitoring and responding to changes and threats in real time?

What if we could have the best of both worlds?

What is Illumio?

Illumio Adaptive Security Platform (ASP)™ is a distributed security platform that provides continuous control and protection of your application environment through adaptive segmentation. Illumio ASP combines live application visibility and a centralized policy engine with distributed enforcement that makes use of the existing capabilities of Linux and Windows servers. The Illumio Policy Compute Engine (PCE) at the heart of the Illumio solution takes easy-to-understand, declarative security policies and converts them into instructions that are enforced using the standard host-based firewalls that already exist inside Linux and Windows servers.

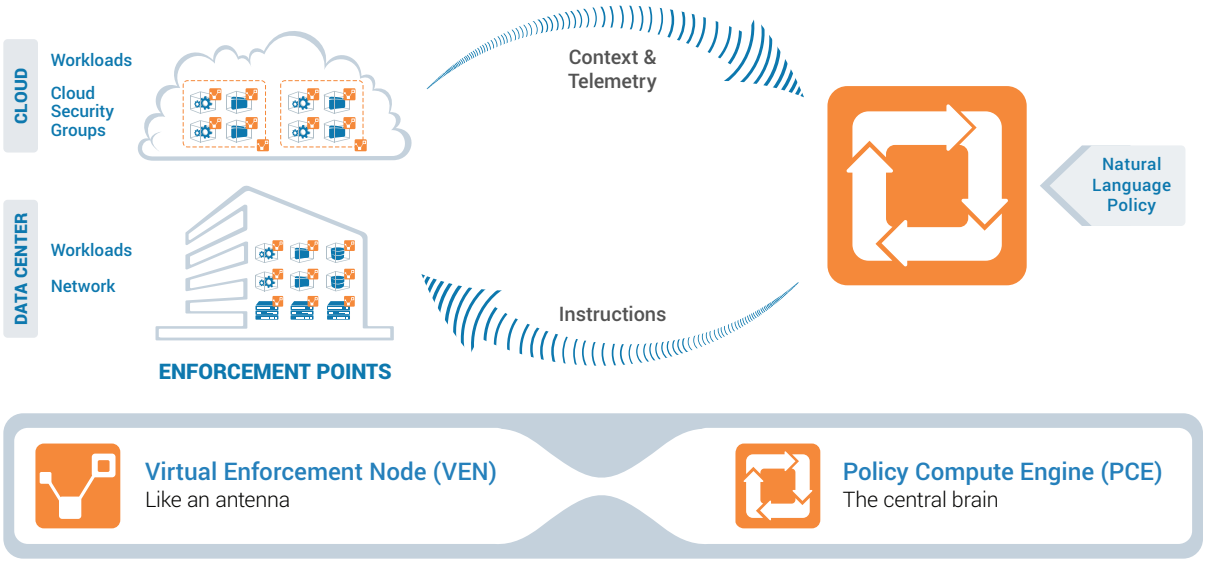
Illumio ASP enables adaptive segmentation so if the topology of the application environment changes, or the policy rules change, the PCE automatically recomputes the required policy and applies the changes on all of the hosts that need updates – no more depending on manually updated firewall policies. Launching a new application? No more sitting through countless meetings, opening multiple tickets, and waiting weeks for the right policies to be defined and implemented. If the application lives within the existing policy, simply adding it to the Illumio protected environment will automatically configure policy appropriately.

Illumio's Illumination view – a live, visual display of applications, how workloads are connected and communications across environments – clearly shows the data flows that the security policy allows, and those it doesn't. Illumination makes it easy to find a server that's misconfigured and is operating out of policy. Changes that place a workload in breach of security policy can be quickly found and fixed.

The PCE monitors telemetry information sent back from the VEN on hosts to detect threats inside your application environment, not just attempted breaches at the perimeter. Once again, the Illumination view makes it easy to find potential breaches and to take action. Attacks can be contained and servers can be automatically quarantined to allow security teams to perform forensics and gather intel on the attackers or perform remediation.

Illumio frees up perimeter devices to concentrate on aggregated traffic flows, rather than trying to police each and every small flow across its interfaces. Illumio complements a true defense-in-depth approach to information security.

How It Works



Illumio ASP is a software solution that is comprised of two pieces:

- Virtual Enforcement Node (VEN) - a lightweight agent that is installed in the operating system (OS) running on a bare metal, virtualized, or containerized host in a private data center or in the cloud. The VEN acts as an antenna with the ability to send and receive information from the PCE.
- Policy Compute Engine (PCE) – the central brain of the Illumio ASP solution – is continually collecting and aggregating information from all the VENs to build a live map of the application environment. The PCE also takes admin-generated policy created in simple, declarative language, and translates it into instructions that are pushed back to the VEN and understood by the host-based firewalls.

The VEN collects context about the host (e.g., OS, IP addresses, protocols, and processes) and sends this information to the PCE. The PCE collects this detail from all the VENs and uses this information to build a live map of the application environment for the Illumination view.

The Illumination view provides live visibility of the application environment with details on how application workloads are connected and communicating. Illumination provides context and feedback to help during the policy planning and creation process.

Policies are created by an administrator in the Illumio console using natural language that is easy to understand. The PCE takes this natural language policy and translates it into instructions that the host-based firewalls will be able to understand.

Instructions are sent from the PCE to the VEN and the VEN uses these instructions to configure the host-based firewall (iptables in Linux and Windows Filtering Platform in Windows Server) where policy is enforced.

The communication between the VENs and PCE is continuous so any change, like a move or added workloads, will result in an updated view and recalculated policy for the environment.

With Illumio, you'll finally feel like you understand and are in control of your application environment.

ILLUMIO FOR

DevOps

Security is often a painful part of the fast-paced world of modern software development. Defining the right security policy for an application using traditional methods can be slow and difficult. With the Illumio ASP, it gets a lot easier.

Security is defined as easy-to-understand, declarative policy in the language of the application, so developers don't need to become experts in network topology or arcane firewall configuration syntax. The Illumio Illumination view provides a clear and simple visual display of the application environment to help with policy creation, and to show how policy will be enforced in the live environment. You can easily model policies and see what will happen with new policy before choosing to enforce new rules.

The robust Role Based Access Control (RBAC) and multi-tenant nature of Illumio means you can configure and test your rules before enforcing them, independently of others, with no risk of breaking your application or anyone else's. The security policy for an application can be defined by that application owner, while global security policy stays with the security team. Each group can focus on its own needs without stepping on each other's toes.

Illumio has a fully self-describing REST-API for integration with your choice of orchestration framework. Changes to security policy no longer depends on network changes, and can be as automated as your continuous integration tool-chain allows. No more waiting for other teams to burn firewall rules or reconfigure network devices.

Scaling an application is simple. Policies are associated with Illumio labels, and new workloads added with that label inherit the appropriate security policy. Illumio's PCE takes care of working out the details of how enforcement is configured on each host, so you don't have to worry about hand-crafting lengthy lists of rules. Just add a new host with the appropriate label and Illumio will take care of the rest.

Enforcement of policy on the server uses Linux iptables or Windows Filtering Platform, depending on the operating system, so you can see the effects of Illumio policy on your servers if you prefer. It's not

hidden off in the corner of the data center on a special network device, so debugging errors with security policy doesn't need coordination with multiple teams. Using the native OS controls means Illumio gets all the benefits of an in-kernel implementation of firewall rules, and if you really want to, you can check the implementation yourself using standard admin tools.

The Illumio Illumination view graphically displays all workloads and application data flows into and out of your applications, so you can see what's really going on. If something isn't configured correctly, you can quickly locate the problem and correct it, even in the most complex environments. Segmentation can be as simple or as granular as each application requires, ensuring that you have the level of detail you need to be informed about what your applications are doing at all times.

The native REST-API and use of standard host-based enforcement means Illumio works well with your existing environment. You don't need to throw out the tool-chain you've spent so long investing time and effort in building. Illumio plugs right in and complements your existing environment, adding extra capability, and simplifying the overall management of the system.

Integrating robust security controls into your application doesn't need to be painful and time-consuming. With Illumio, security becomes just another part of the automated deployment system you use every day.

Security and rapid innovation work hand-in-hand – the way they're supposed to.

ILLUMIO FOR

Enterprise Architects

Information security is now a Board and C-level discussion. Relying purely on outdated techniques like perimeter firewalls and antivirus to keep an organization protected from modern threats is simply not enough. The agile and fast-moving enterprise needs tools and techniques that can work with the organization to securely achieve its goals, not a department of "no" that slows everyone down.

The Illumio ASP provides a policy-driven approach combined with automated, distributed enforcement that protects against external and internal threats, including lateral movement within the enterprise. Illumio combines an easy-to-understand, declarative policy view of security with intuitive visualization – Illumination – that graphically displays application topology and live application flows.

Illumination provides immediate visual feedback for modeling policy while providing a tool to confirm compliance and identify potentially compromised workloads. Showing the value of security has never been so easy.

Application owners often choose to 'accept' security risks rather than slow down or delay implementations, placing the entire organization at risk. Making it easier to do the right thing provides the right incentives to ensure that security isn't merely an afterthought. Micro-segmentation isolates applications from each other, insulating them from decisions made elsewhere. Putting the control of security in the hands of the application owner can encourage them to take responsibility for the decisions they make, and segmentation protects the rest of the organization should some of those choices prove incorrect.

Security controls can be aligned with applications and business groups, matching organizational structure rather than the infrastructure. The technical designs can then be decoupled from security policies, freeing

up the infrastructure to be designed to facilitate information flow, rather than as a series of security control points. Applications can span bare-metal servers, cloud services, hyper-converged appliances, whatever best suits the application, and Illumio works just the same. Illumio is not dependent on platforms or underlying infrastructure; it automatically adapts the policy implementation to match the environment, even as it changes.

For example, in a hybrid- or multi-cloud environment where an application spans multiple sites, some in a cloud environment and some on-site, the application security boundaries don't have to align with physical network devices like perimeter firewalls. Simple rules can be configured at physical boundaries while logical flow control is managed at the endpoints. Network devices can then be free to manage data in the aggregate, such as securing all flows from one site to another, while per-application segmentation can control what data is allowed to be accessed, from where, and by whom.

Security policy decisions don't need to have immediate infrastructure impacts. Deciding where to place a workload need not be constrained by physical segmentation decisions and the limitations of vendor hardware. Instead, workloads can be placed and moved wherever they need to be and Illumio will adapt the implementation details accordingly, automatically. Manage security at a high level, not down in the weeds with lines of ACLs.

And with Illumio's Illumination view, you can see your security policies working in real time as live telemetry data is fed back from the distributed enforcement nodes. You can prove that systems are operating securely, and have confidence that threats are being detected and managed.

Risk is contained within the appropriate domain, even down to a specific host, and those responsible for the security of their application will bear the impact of breaches without endangering the rest of the organization, aligning incentives to encourage the right behavior.

Security can become an enabler of innovation instead of just another procedural speed bump.

ILLUMIO FOR

Solution Architects

Many applications need to be re-designed or re-implemented from time to time. But when that time comes, the required documentation is often incomplete or just plain wrong. Finding out what's really going on is time-consuming and frustrating.

Illumio's Illumination view gives you a clear picture of how an application works by providing visibility into its workloads and flows. When you're able to see how workloads are connected, you can see how data flows through an application, and to which other applications it connects. You can see all the services it uses, including those it may be trying to use but shouldn't be.

Instead of breaking applications and then waiting to see who complains, Illumio can help you understand why data is flowing the way it is. It can provide you with a window into what's really happening in your application environment, right now, in a way that's simple to understand. What might look like a breach of security policy might be happening for a good reason.

You can determine that a web application uses the main Active Directory system for identifying information, but uses a custom-built one as well for some reason. You can find all the obscure, one-off decisions that made sense at the time, but that no one can remember what the reasons were. You can get to the bottom of complex systems designs quickly, and with confidence that the information you have is correct, because it's taken from the real system.

Security controls can be designed to be added at the right level of abstraction; organizational rules live with the central policy, and application-level rules can be defined within the application environment. No need to be concerned with the complex interactions of firewall rules or hundreds of lines of network ACLs.

You can adapt segmentation to match the business need. Where coarse-grained segmentation is sufficient, say to separate a development environment from production, Illumio enables this

with a simple policy for quick results. If more granular micro-segmentation is appropriate, Illumio offers the detailed, granular policy you need with the same familiar interface. As your segmentation journey evolves, Illumio is there with you every step of the way.

Illumio implements security policy at the OS level using in-built host-based firewalls, which keeps compatibility issues to a minimum. The centralized control makes it easy to keep a consistent, enterprise view of policy while enforcement happens closer to the edge, keeping unwanted traffic off the network. Changes to application security policy don't need to affect perimeter firewall or network configurations, minimizing cross-team conflicts and speeding up changes and the pace of project approvals.

Illumio works with your current security environment, complementing existing perimeter firewalls and segmentation devices. It is particularly strong in virtualized environments where it's more difficult to insert a perimeter device between virtual machines. With Illumio, workloads can be segmented within the same virtual cluster without needing dedicated firewall devices or expensive overlay software.

Finally, you can quickly and easily add a visual representation of a planned implementation using Illumio's Illumination view. A visual display of the proposed effect is a powerful tool in gaining the required approvals for a design to move forward through formal enterprise processes. With Illumio's ability to test policy on real flow data before enforcement, you can have confidence that the implementation will match the design.

Illumio helps you ensure solutions are secure without security becoming a project roadblock. Get more done, faster.

ILLUMIO FOR

Network Professionals

With the Illumio ASP, the responsibility for application-level security is moved out of the network and into the application where it belongs. Instead of maintaining hundreds of ACLs, trying to fix conflicts between different group requirements, and being blamed for the complexity of a centralized approach to security, network operators can focus on making the network operate smoothly.

The Illumio PCE takes easy-to-understand, declarative security policy descriptions and converts them into specific host-based firewall instructions. Illumio's lightweight VEN software on Linux and Windows then implements this host-specific configuration using the in-built iptables or Windows Filtering Platform.

By moving security enforcement off the network and onto the hosts, perimeter firewalls can concentrate on bulk flows of North-South traffic while leaving finer-grained control of East-West traffic to Illumio. With the rise in virtualization, using dedicated firewall devices to regulate VM-to-VM data flows makes for extremely complex and tricky-to-manage network topologies. With Illumio, global network policy can use simpler rules without compromising security, and previously endless ACLs become simpler and easier to manage.

Illumio also reduces unnecessary traffic on the network, removing load from perimeter devices. Packets that shouldn't enter the network are stopped at the host, as the Illumio VEN configures the host-based firewall to prevent forbidden traffic from leaving in the first place. Gateway devices and firewalls can concentrate on higher-level aggregated rules that implement global network policy, not dozens of application level exceptions.

No more responding to urgent requests for network changes so an application can go live just because someone 'forgot' a specific port needed to be open. No more firewalls with Swiss cheese rule sets operating as expensive routers or switches.

With Illumio, the network infrastructure and topology are decoupled from the applications, so upgrading a firewall no longer requires dozens of approvals from application teams. Complex, inefficient network flows can be simplified, and application performance issues can be easily traced to the real root cause.

Illumio's Illumination view shows simply and clearly how data flows between applications. You can see exactly which flows are being blocked and why. If the flow really does need to happen, allowing it is simple. No more tedious tracing of how the ACLs actually function to find the specific line causing problems, or accidentally allowing insecure traffic through because of non-intuitive rule interactions.

The hard work of orchestrating a distributed network of firewall rules is left to the Illumio PCE, which automatically figures out the right rules for each device based on the simple-to-understand, declarative policy description. No more laborious, hand-crafting of ACLs. Even better, when applications need to change, the network doesn't have to change with them. Illumio automatically updates the implementation to match the current policy configuration.

Best of all, Illumio's robust RBAC and multi-tenant functionality means that application owners can take responsibility for the mistakes they make without risking the rest of the network. Gain micro-segmentation of the network without having to teach VMware administrators about the intricacies of network topology.

Whatever your existing security approach, Illumio is complementary. It doesn't require a full rip-and-replace of your existing infrastructure; instead, it might save you a major upgrade to firewalls that are capacity constrained. You can gradually add functionality as you become more familiar with the possibilities.

Focus your existing security controls on what they're best at, and leave the complex automated capabilities to Illumio.

ILLUMIO FOR

Operations

Keeping your organization's information secure is becoming harder as the number of threats mount and the sophistication of the attackers increases. Perimeter firewall policy and network-based ACLs grow longer and more complex while the pressure to move faster, be it Agile or DevOps, never goes away. The old ways of doing security just aren't coping any more.

The Illumio ASP simplifies things by taking easy-to-understand, declarative security policy descriptions and converting them into specific host-based firewall instructions automatically. Illumio moves the complexity of security configuration out of network devices like perimeter firewalls and load balancers, and puts it close to the applications where it belongs.

The Illumio PCE turns simple policy into the detailed rules that host-level firewalls require, eliminating the tedious work of hand-configuring access control lists. You can leave the detailed configuration to Illumio.

The implementation itself uses the existing and familiar host-based firewalls built in to Linux and Windows, not some arcane proprietary software. You can see exactly what Illumio has done using existing system administration tools. Illumio interoperates well with other host-based tools, such as fail2ban, and complements existing approaches to security.

The Illumio Illumination view provides a clear and simple application display of the workloads and data flowing across your organization. Real-time telemetry data is collected from hosts by the Illumio VEN on each host that is connected to the central Illumio controller to implement policy. The data feeds into the Illumio controller to provide a real-time view of what's really happening in the systems. See which applications are talking to each other, where data is leaving your organization, and where it's coming in.

You can see all the application flows—those that are supposed to be there, and any that aren't. If someone has changed their application configuration and is now in breach of security policy, you can detect it and fix it quickly. Keep anxious project managers at bay by showing them exactly what's wrong with their application with an easy-to-understand diagram.

For something more serious, like an attempted breach, Illumio can quickly show you where the traffic is flowing from, and to, and can easily plug in to your preferred approach to incident response. You can quickly detect the attempt and immediately see which systems are at risk on the Illumination view.

Illumio's policy implementation is always default-deny, so any unauthorized flows are stopped in their tracks. But what if you want to do something more complex, like making the server completely inaccessible to the attacker and isolating it from the rest of the environment? Or maybe you want to observe and gather data to be used for forensics? It's as easy as a few clicks. Drag-and-drop the affected systems into a quarantine zone for observation and data collection, but keep the rest of the applications safe and operating.

A powerful REST API and support for third party SIEM solutions makes integrating Illumio into existing orchestration and monitoring systems easy. Keep using your existing tools and add integration where it makes sense. Illumio works in combination with your existing tools and processes; a wholesale change to your organization isn't required to start getting the benefits of the Illumio approach.

Illumio is ready to be plugged into your modern approach to operations. It automates the tedium, and helps operators to understand what's going on at all times, allowing them to quickly fix and keep applications secure and online.

When changes are needed, Illumio makes them safe and fast, helping operations contribute to the faster time-to-market demanded by businesses today without breaking things in the process.

ILLUMIO FOR

Security Professionals

Balancing security with the need for a rapid, agile response is a complex challenge. There is no single tool that can solve all problems, but it's clear that the heavily manual methods of the past are no longer sufficient. The modern security professional needs tools that can quickly adapt with a changing threat landscape, while helping you meet the needs of your organization.

The Illumio ASP combines the power of a distributed network of firewalls, one in each host, with the control of a centralized policy engine. Add the ability to define domains of responsibility with robust role-based access control, and security policy can match the organization—not just the technology.

Segmentation based on physical devices like perimeter firewalls is too rigid for a world where lateral movement within a segment is a real threat. Illumio complements your existing approach by supporting granular micro-segmentation that matches your organization's needs.

The complexity of managing individual firewall policy and lengthy ACLs by hand invites disaster from a single human error. Illumio's PCE takes easy-to-understand, declarative security policy descriptions and generates the enforcement instructions automatically, making human error less likely.

Designing quality security policies is simple with Illumio's intuitive interface, and the clear visualization of Illumio's Illumination view makes modeling and troubleshooting policy easy. Design policy in build and test mode to see its potential impact, then move it to enforcement mode when you're happy with the set of security controls you've designed. Enforcement then becomes as simple as clicking a button.

Security policy can be tightly aligned to the goals of an application or a business unit without impacting the network topology. Responsibility for ensuring that the appropriate controls exist can be aligned with taking the risk if something goes wrong. The entire organization isn't at risk if one group decides to deploy without the right security controls, and any problems can be quickly corrected once detected.

Network design can look at technical and performance considerations while security deals with higher-level policy concepts that are easy to enforce. In a world where 'assume breach' has profound implications for network design, Illumio helps to simplify things where firewall devices live inside hosts, not just in specialized devices at carefully designed choke points.

The clear display of security boundaries aligned with the organization makes showing the value of robust security controls easy to demonstrate. The Illumio Illumination view can show what's happening in real time, with live telemetry data from the VEN operating on each host. You can show what's working, not just what breaks.

Respond to threats with a few clicks. Illumio uses a default-deny approach to security to ensure each host is well protected. But perhaps you want to observe a potential attack before taking further action? Simply drag-and-drop affected systems into a quarantine zone, keeping other systems protected while you determine the best response to the potential threat.

With the Illumio ASP, security can get out of the way of innovation, setting simple and easy-to-accept policies for the organization as a whole, and leaving small details to the individual business units that should be making them. Security professionals can concentrate on looking for big-picture gains, not picking through ACLs line-by-line.

Illumio helps make secure-by-design a core part of your enterprise's approach to security.

Contact Illumio

www.illumio.com

+1-669-800-5000

Illumio Adaptive Security Platform and Illumio ASP are trademarks of Illumio, Inc. All rights reserved.