Palo Alto Networks and Illumio

Simplify and Automate Workload Security for Microsegmentation and Zero Trust

Benefits of the Integration

Together, Palo Alto Networks and Illumio provide:

- **Comprehensive application and workload visibility**
  - » See everything across your application flows and workloads
  - » Use a single source of truth to enable intelligent policy management for dynamic workloads
- **Effective microsegmentation and Zero Trust**
  - » Reduce the attack surface across east-west traffic at the network level
  - » Automate policy definition, testing/modeling, provisioning, and enforcement for effective workload segmentation
- **Dynamic security for workloads**
  - » Streamline PAN-OS policy changes across Dynamic Address Groups whenever dynamic workloads move
  - » Reduce complexity by pushing workload telemetry (IPs, labels, etc.) from the Illumio PCE via XML/JSON API into Panorama and Palo Alto Networks NGFWs

The Challenge

Today's data center and cloud environments are becoming more dynamic and complex to securely deliver workloads across on-premises data centers and multiple public, private, and hybrid clouds. The underlying architecture is evolving to enable businesses to move more quickly. In addition, the threat landscape is growing, with an expanding attack surface that has given rise to an influx of security breaches and threats. Organizations need a simpler approach to hybrid cloud security that helps reduce risk as well as minimize business disruption and data loss for effective Zero Trust.

Illumio

Illumio built a new way, pioneering microsegmentation for applications and workloads across data centers and multi-cloud environments. This vision gave way to a segmentation platform that gives you 20/20 application visibility and 24/7 control to stop lateral movement, preventing the spread of breaches across any data center or cloud on bare metal, virtual machines, and containers. Illumio helps you solve the lateral movement problem that occurs in every single breach. It all starts with a map that gives you complete visibility into any application environment, no matter how complex it is, and brings to light what's communicating and what shouldn't be. Use that map to simply create east-west segmentation policies. With Illumio, visibility begets simplicity. This is why customers rely on Illumio to keep lateral movement in check and reduce their cyber risk.

Palo Alto Networks

Palo Alto Networks ML-Powered Next-Generation Firewalls (NGFWs) inspect all traffic at Layer 7 and offer a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere.

ML-Powered NGFWs inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. The application, and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies as well as write rules that are easy to understand and maintain.

Palo Alto Networks and Illumio

Together, Palo Alto Networks and Illumio help organizations automate dynamic security changes by making their PAN-OS® firewall policies workload aware to eliminate manual effort and risk of service disruption as the applications change or workloads move. Integration via XML/JSON API enables Illumio Policy Compute Engine (PCE) to send real-time context of workloads and labels that are mapped to IP address and tags within Dynamic Address Groups (DAGs) in Panorama™ network security management or PAN-OS firewalls (PA-7000, PA-5200, PA-3200, VM-Series). Enterprises can take advantage of best-in-class network- and host-based segmentation (via PAN-OS firewalls and Illumio Virtual Enforcement Node [VEN] and PCE software, respectively) for robust security across the network as well as on hosts in the data center or multi-cloud environments.

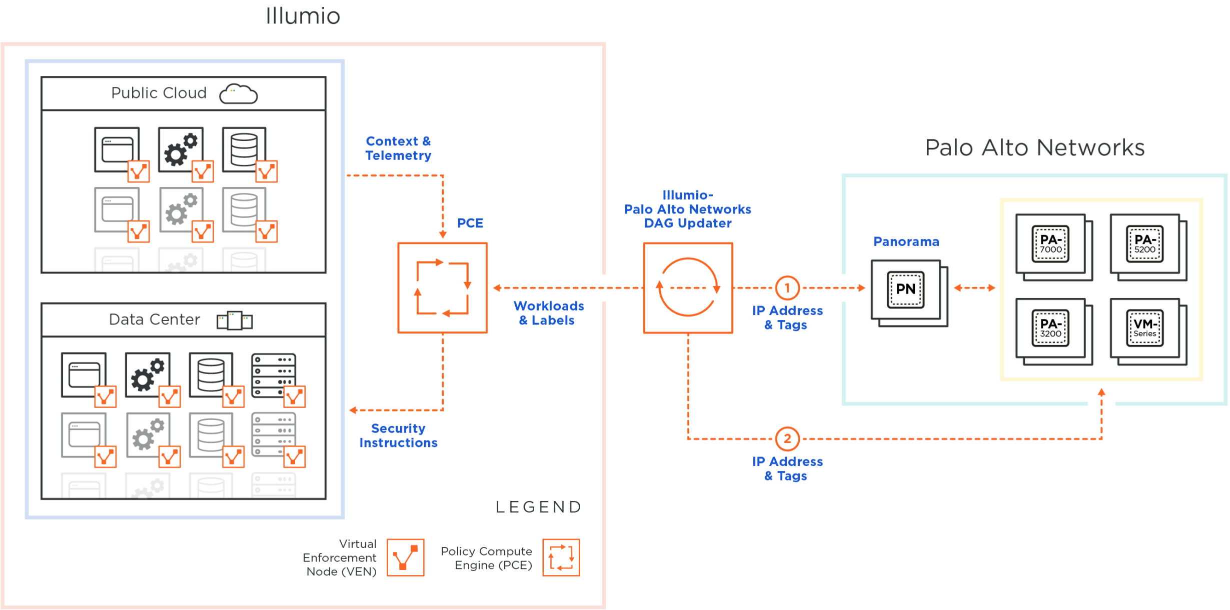

Figure 1: Integration between Palo Alto Networks NGFWs and Illumio

Use Case No. 1: Update Workload Context Continuously and Automatically

Challenge

Continually tracking and automating security for dynamic workloads is complex as well as difficult to manage and deploy. IP addresses can change for workloads as they move (live migrate) inside or across data centers and clouds. On-demand workloads can spin up or down, and dynamic changes to workload policies can be cumbersome to administer using dynamic addressing.

Solution

Illumio helps you intelligently tag and push real-time context across workloads into Panorama to quickly define effective segmentation policies for Palo Alto Networks NGFWs across east-west traffic. You can automate DAG policy changes to reduce risk from blocking legitimate application flows and implement real-time workload controls (microperimeters) without business impact using Palo Alto Networks NGFWs.

Use Case No. 2: Limit Threats from Spreading Laterally

Challenge

Ransomware, malware, and other security threats can quickly spread across east-west traffic. Increasing cyberthreat risk is difficult to see and stop inside the data center or across clouds. Breaches are bad for business and result in business disruption and data loss.

Solution

Quickly detect, block, and isolate threats across the network via PAN-OS firewalls (PA-7000, PA-5200, PA-3200, VM-Series), and on endpoints via Illumio software agents, to prevent hackers from stealing data or disrupting operations.

About Illumio

Illumio enables organizations to realize a future without high-profile breaches by preventing the lateral movement of attackers across any organization. Founded on the principle of least privilege in 2013, Illumio provides visibility and segmentation for endpoints, data centers or clouds. The world's leading organizations, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit https://www.illumio.com/what-we-do and engage us on LinkedIn and Twitter.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com