illumio

TECHNICAL BRIEF

Illumio vs. Traditional Firewalls

Security Through Workload Segmentation

Illumio outperforms traditional firewalls in defeating malware, thanks to workload-based segmentation that isolates servers, applications and data

Traditional Firewalls Can't Isolate Inevitable Attacks

The impact of cyberattacks, including via ransomware, have increased dramatically in the 2020s. Attackers deploy an arsenal of sophisticated tools to gain entry to servers and access sensitive data, hold it for ransom, threaten companies with exposure, or steal it for monetary or competitive gain. In this environment, it's often not a matter of if a breach will occur but when.

In the past, organizations have depended on physical or virtual firewalls to keep bad actors out and valuable IT assets safe. However, traditional firewalls become increasingly complex to manage for smaller groups of users, limiting their effectiveness for security.

In short, proliferating networks, cloud-based workloads, the internet of things, and an explosion of ransomware and other attacks mean organizations need a new approach to security.

Workload-Based Segmentation Isolates Breaches

Workload-based segmentation allows systems administrators to quickly visualize, define, and segment servers, devices, workloads, and even geographies in any way they see fit.

For example, it lets them preemptively disable problem areas such as little-used but vulnerable ports that attackers often exploit. Administrators can quickly identify vulnerable workloads and automatically isolate them in case of attack.

Workload-based segmentation provides a level of micro-segmentation unavailable with traditional firewalls. You can think of it as an abstraction layer on top of typically much more difficult to manage firewall setups, providing unprecedented control over data flows and tighter security. And because it frees staff from manually configuring firewalls in response to threats, letting them focus on higher-level tasks, it also helps organizations maximize limited IT resources.

Workload Segmentation Helps You Take Control

Get control over workloads and vulnerabilities and respond to threats more quickly without draining IT resources

Greater Visibility
Illumio abstracts layers of complexity to let IT professionals visualize workloads and vulnerabilities across servers, devices, applications, geographies, and more.

Faster Configuration
Unlike traditional firewalls, Illumio allows administrators to quickly apply micro-segmentation across the IT environment, proactively or in response to threats.

Lower Cost
Illumio lets organizations deploy smaller firewalls, reducing infrastructure costs. Easier management also reduces person-hours required to keep up with evolving threats

How Illumio Enables Workload-Based Segmentation

Map Application Communications

Illumio takes in your entire IT environment, whether in the cloud, on-premises, or hybrid configurations. For example, it gathers object metadata and flow telemetry from across cloud accounts.

From there, it builds real-time visualizations of workloads and connected environments. These maps show application dependencies across clouds, on-premises, and hybrid environments based on what's happening now and in recent history.

Illumio also makes sense of complexity. Rather than displaying a confusing mass of connections across all workloads, Illumio breaks up visualizations into maps that adapt to the role of individual users. For example, it can show assets and data flows by geography or cloud service, depending on what a given user needs to see.

> "One of the benefits of the Illumio solution is that we don't have the hindrance of traditional hardware support, maintenance and cost. We've got an investment that we can rely on for years to come."
>
> **Andrew Dell**
> **CISO at QBE Insurance**
>
> Source: https://www.illumio.com/resource-center/video/QBE-Zero-Trust-CISO

With Illumio, you can:

- Track data flows by geography.
- Visualize data in cloud services such as AWS, Azure, or Google.
- Identify policy violations and suspicious communications between servers and devices.

Segment Workflows

Armed with visualizations of what's happening with your data, you can use Illumio to easily segment workflows right within the application, rather than having to configure external firewalls and manually rewrite complex rules.

Illumio gives IT teams the speed, flexibility, and responsiveness they need to meet today's threats cost-effectively, wherever they appear.

Learn more about how Illumio improves on traditional firewalls for segmentation.

Visit:
illumio.com/solutions/micro-segmentation

About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model.

Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.