illumio

SOLUTION BRIEF

Reduce Vulnerability Risk With Illumio

Use Zero Trust Segmentation to limit the risk of exploitation and stay ahead of evolving cyber threats

Security gaps are inevitable in today's complex networks

The surge in sophisticated cyberattacks shows that too many vulnerability gaps remain unnoticed or unpatched. These gaps are created by an increasingly complex network infrastructure, fragmented visibility, and outdated network architectures – and threat actors are constantly finding new vulnerabilities to exploit.

Outdated services and missing patches are notorious for inviting cyber threats in. And even if organizations patched every vulnerability, it still takes time for issues to be found and patches to be rolled out.

In fact, according to Verizon's 2023 Data Breach Investigations Report, the roll out of critical patches takes a median of 49 days, leaving exposed workloads vulnerable for far too long.

While vulnerability scanners do a great job at pinpointing where security gaps are, it's nearly impossible to address every vulnerability. It's essential to prioritize securing the most at-risk workloads first, but without complete visibility into network flows, it's impossible to know what workloads pose the most risk at any given time.

Breaches are inevitable – and a proactive cybersecurity approach is imperative. Organizations must evolve and keep pace with the complex dynamics of today's threat landscape to avoid exposing themselves to unnecessary risk.

This risk can be reduced by being able to mitigate emerging vulnerabilities before they can be exploited.

> "The map grew legs when we overlaid vulnerability data from our scanner software. This allows us to see what applications are connecting to vulnerable ports, then make a business decision and a cyber decision to determine what needs to be closed."
>
> **– Nick Venn**
> Global Collaboration & Cyber Infrastructure Manager
> QBE

The solution: Illumio Zero Trust Segmentation

Illumio's application dependency map helps reveal systems or applications with excessive, unnecessary, or non-compliant communication. It can even combine this information with data from vulnerability scanners.

Using this insight, teams set granular, flexible segmentation policies to reduce vulnerability exposure and stop the spread of inevitable breaches.

By understanding context and exposure, workloads can be secured quickly before a patch is rolled out.

Quantify risk

In the face of emerging threats, it's crucial to not only identify but also quantify potential vulnerabilities within your network.

Illumio shows network weak points so that teams can implement proactive measures precisely where most needed.

This insight arms cross-functional teams with actionable insights, fostering data-driven decision-making and enhancing risk mitigation strategies across the entire environment.

Proactive vulnerability defense

Model, test, and deploy granular segmentation of high-risk assets as a compensation control, effectively shielding critical systems when patching isn't feasible or will introduce unacceptable operational complexity.

Awareness is key. If traffic connects to a port with a known vulnerability, the security operations center (SOC) gets alerted of the violation, including the vulnerability and severity context with data provided by Illumio.

Integrate seamlessly

Ingest vulnerability data and formulate mitigating policies at an unprecedented scale.

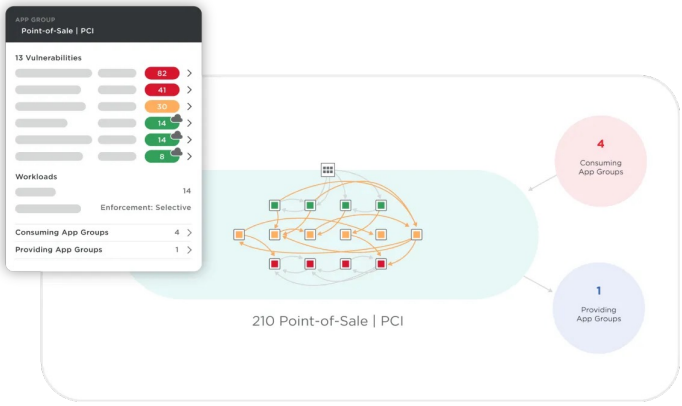
Illumio effortlessly combines Common Vulnerability Scoring System (CVSS) data from industry-leading third-party scanners like Qualys, Rapid7, and Tenable. This data is then combined with Illumio's real-time application dependency map to optimize response strategies and enhance the granularity of network traffic insights.

By enriching CVSS data with traffic insights, security teams can know the actual risk score of each system and quickly decide if systems need to be virtually patched through segmentation before an actual fix is available.

Illumio's Vulnerability Exposure Score

Vulnerability management solutions typically use industry-standard Common Vulnerability Scoring System (CVSS) scores. While valuable, these scores don't consider a workload's connectivity relative to other workloads in the environment.

Illumio combine CVSS scoring with information on how many workloads can potentially connect with a vulnerable workload to calculate a Vulnerability Exposure Score (VES). Security and IT operations teams can better prioritize mitigation strategies based on exposure scores and implement Illumio Zero Trust Segmentation to mitigate risk if patching is not an option.



Learn more about closing security gaps with Illumio

Visit:
illumio.com/solutions/vulnerability-risk-reduction

About Illumio

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.