SOLUTION BRIEF

# Strengthening Zero Trust with Integrated Breach Containment and Continuous Compromise Assessment®

## EXECUTIVE SUMMARY

Enterprises today face a relentless barrage of sophisticated cyberattacks that bypass traditional perimeter defenses. Once inside, attackers move laterally across the network, escalating privileges and exfiltrating data, often undetected for weeks or months. To combat this, organizations are adopting a Zero Trust security model, which assumes that no user or system is inherently trustworthy. The integration of **Illumio Zero Trust Segmentation (ZTS)** and **Lumu Continuous Compromise Assessment®** provides a powerful, automated solution to operationalize Zero Trust, contain breaches, and minimize the impact of cyberattacks.

This joint solution combines Illumio's industry-leading microsegmentation and breach containment capabilities with Lumu's real-time threat detection and response. By sharing rich contextual data and automating response actions, Illumio and Lumu empower security teams to proactively identify and contain threats, preventing lateral movement and stopping ransomware in its tracks.

## THE CHALLENGE: PERVASIVE THREATS AND THE POROUS PERIMETER

In today's hybrid, multi-cloud world, the traditional network perimeter has dissolved. The rise of remote work, cloud adoption, and interconnected applications has created a vast and complex attack surface. Attackers who successfully breach the perimeter can move laterally with ease, exploiting the "flat" internal networks that lack sufficient east-west traffic controls. This reality has led to a surge in devastating ransomware attacks and data breaches, highlighting the urgent need for a new security paradigm.

**Key challenges include:**

### Lack of Visibility

Security teams often lack a clear understanding of how applications and workloads communicate, making it difficult to identify and stop lateral movement.

### Slow Threat Response

Manual incident response processes are too slow to keep pace with automated attacks, allowing attackers to dwell in the network and cause significant damage.

### Operational Complexity

Managing a patchwork of disparate security tools creates operational silos and increases the risk of misconfigurations and security gaps.

## THE SOLUTION: INTEGRATED DEFENSE FOR PROACTIVE BREACH CONTAINMENT

The integration of Illumio and Lumu delivers a closed-loop security solution that automates threat detection, response, and containment. This powerful combination enables organizations to:

### See and Understand Risk

Gain real-time visibility into all network communications and continuously assess the level of compromise across the entire hybrid environment.

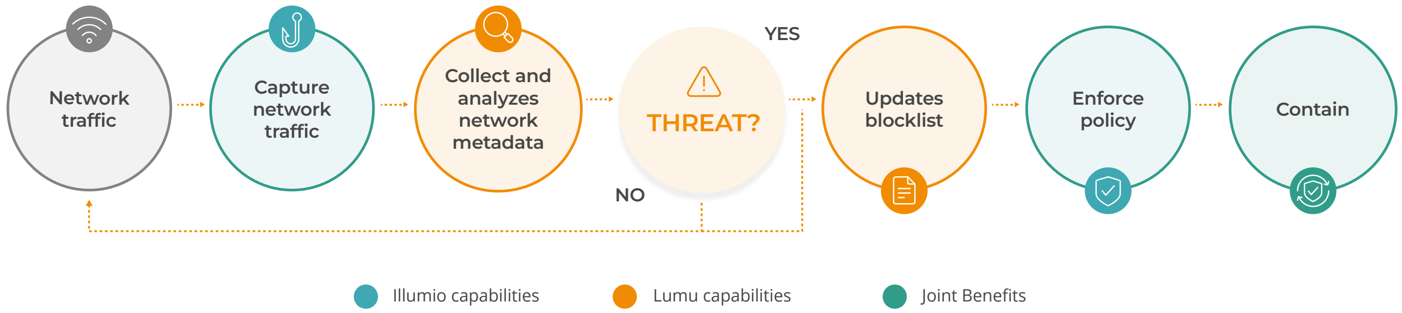
### Contain Threats Automatically

Proactively contain threats by automatically updating segmentation policies based on real-time threat intelligence from Lumu.

### Strengthen Zero Trust

Implement a robust Zero Trust architecture that assumes breach and continuously verifies all network activity.

## AUTOMATED THREAT RESPONSE WORKFLOW



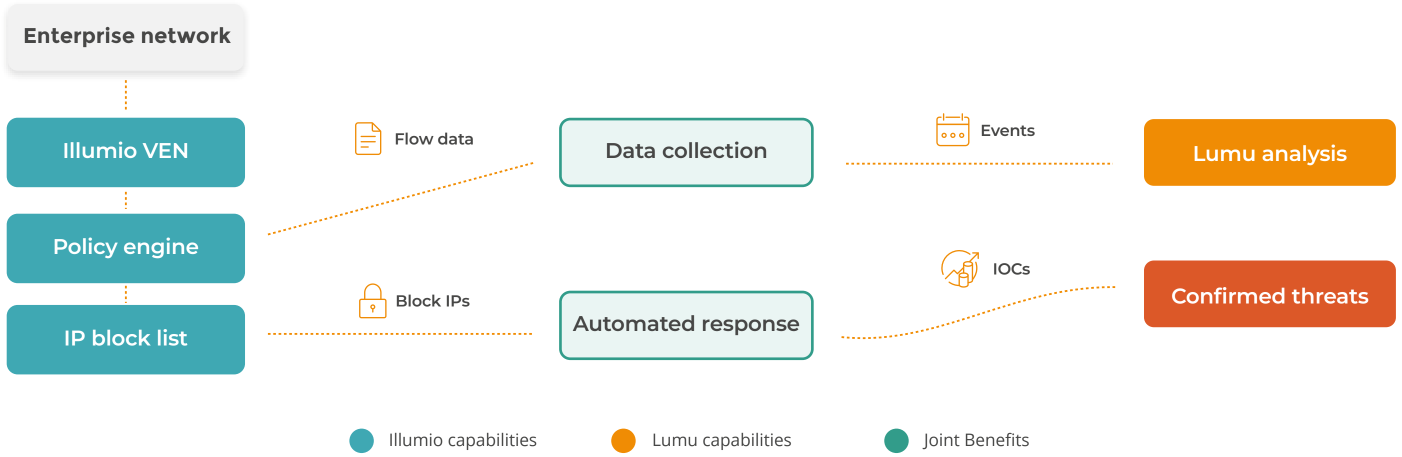
## HOW IT WORKS: A TWO-WAY INTEGRATION

### Data Collection (Illumio to Lumu)

Lumu's integration collects rich network flow metadata from the Illumio platform. This data is then analyzed by Lumu's Illumination Process to detect confirmed compromises in real-time.

### Automated Response (Lumu to Illumio)

When Lumu confirms a threat, it feeds the associated Indicators of Compromise (IOCs) to Illumio. Illumio then automatically updates its IP block lists and enforces segmentation policies to isolate the compromised hosts, preventing any further communication with malicious infrastructure.



## KEY BENEFITS OF THE JOINT SOLUTION

| BENEFIT | DESCRIPTION |
|---|---|
| **Automated Breach Containment** | Instantly isolate compromised systems to prevent the spread of ransomware and other advanced threats, dramatically reducing the potential impact of a breach. |
| **Accelerated Threat Response** | Eliminate manual intervention and slash response times from days or hours to minutes or seconds, freeing up security teams to focus on strategic initiatives. |
| **Enhanced Visibility and Context** | Gain a unified view of your security posture with real-time application dependency mapping from Illumio and continuous compromise assessment from Lumu. |
| **Strengthened Zero Trust** | Operationalize your Zero Trust strategy with a solution that continuously verifies all network activity and enforces least-privilege access at scale. |
| **Reduced Attacker Dwell Time** | By providing continuous, real-time monitoring of the entire network, the joint solution significantly reduces the time attackers can remain undetected in your environment. |

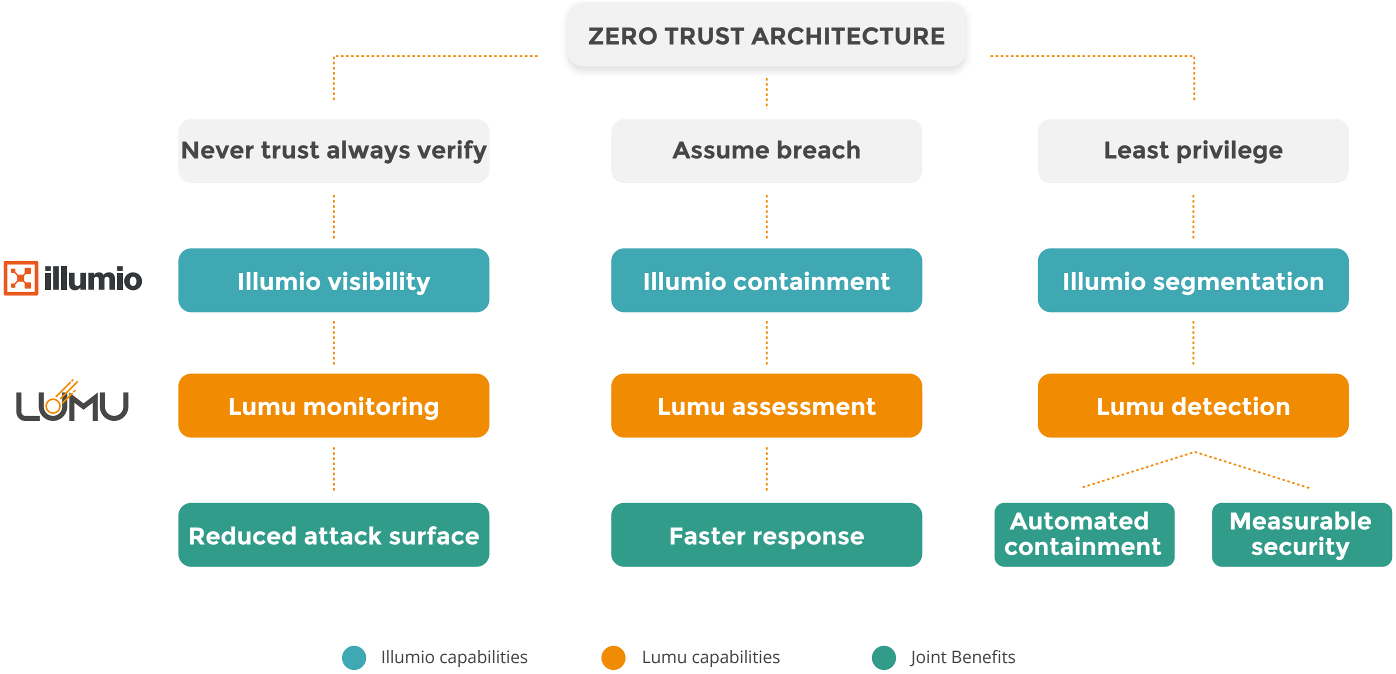
## USE CASES

### Ransomware Containment

The Illumio and Lumu integration provides a powerful defense against ransomware. When Lumu detects the initial signs of a ransomware attack, such as communication with a known command-and-control (C2) server, it immediately notifies Illumio to isolate the infected endpoint. This automated containment prevents the ransomware from spreading to other systems, effectively stopping the attack in its tracks.

### Strengthening Zero Trust Implementation

Zero Trust is a journey, not a destination. The Illumio and Lumu integration provides a practical and effective way to implement and enforce Zero Trust principles across your hybrid environment. By combining Illumio's microsegmentation with Lumu's Continuous Compromise Assessment®, you can build a security architecture that is both resilient and adaptable.



ZERO TRUST ARCHITECTURE

Never trust always verify

Assume breach

Least privilege

illumio

Illumio visibility

Illumio containment

Illumio segmentation

LUMU

Lumu monitoring

Lumu assessment

Lumu detection

Reduced attack surface

Faster response

Automated containment

Measurable security

● Illumio capabilities ● Lumu capabilities ● Joint Benefits

### About Illumio

Illumio, the Zero Trust Segmentation company, prevents breaches from spreading and turning into cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology.

→ For more information, visit www.illumio.com

### About Lumu

Lumu is a cybersecurity company that helps organizations measure and understand compromise in real time. Lumu's Continuous Compromise Assessment® model enables organizations to identify and respond to threats as they happen.

→ For more information, visit www.lumu.io