illumio

Anatomy of Successful attacks and how stop attacks from spreading

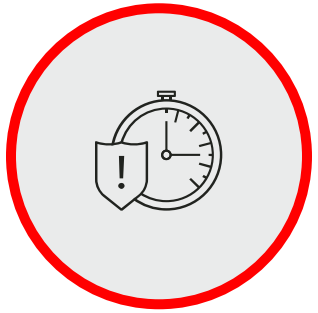
Assume breach. Minimize impact. Increase resilience.

Wassim Daghash (Principal Systems Eng, APAC)

Attacks are becoming more costly and more destructive

$4.45M USD

The average cost
of a data breach



277 days

The average time it takes to
identify and contain a breach

25%

A quarter of malicious
attacks halt system operations

IBM Cost of a Data Breach Report 2023

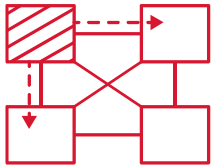
Attackers use a variety of tools to traverse your environment and then pivot and leverage vulnerabilities to move laterally.

Verizon 2023 Data Breach Investigations Report

Why are attacks successful?

Prevention and detection fails

- Undetected + unauthorized intrusion
- Attackers lurk for months – dwell time



Attack spreads

- Lateral movement allows attackers full network access
- Flat networks with no segmentation are defenseless

Critical assets compromised

- Malware locks systems and demands ransom
- Risk of exfiltrated data and regulatory violations

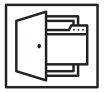
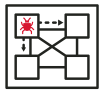
In a hyperconnected, hybrid, multi-cloud world, lateral movement is THE biggest risk

Anatomy of attacks: When detection is not possible/fails

ZTS is the difference between devastation and containment

Initial Entry	Network Discovery	Establish Backdoors	Lateral Movement	Defense Evasion	Data Collection	Exfiltration
Purchase stolen High-Level Credentials	Lack of effective segmentation enables Recon: looking for data stores	Establish backdoors	Uncontrolled attack surface: Laterally move and collect data from middleware across environments.	**Detection is moot** – no tools/malware deployed, no need to evade.	Compile custom tools whilst inside, to collect data from other different parts of the business	exfiltrate data before being detected while triggering a decoy – EDR is abused by attackers.



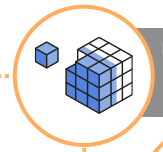

Illumio ZTS platform prevents recon by attackers.

Illumio ZTS platform significantly reduces the ability to move laterally and collect data

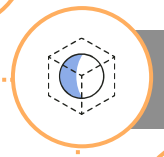
Illumio Outcomes

1 PRE-ATTACK

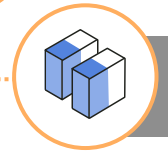
Visibility and SEGMENTATION

A 

Understand the environment through a risk-based and business context application dependency maps – across data-centres and public clouds

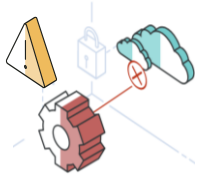
B 

Measurably Reduce Attack Surface by generating policies to segment environments, and ring-fence high value applications. Measure the segmentation efficacy through the reduction of exposure to vulnerabilities.

C 

Confidently Demonstrate segmentation outcomes through application dependency mapping and detailed reporting with segmentation policy results overlay.

2 INVESTIGATION & DETECTION



Accelerate detection by co-leveraging Illumio events and SIEM

When the ransomware's first lateral movement attempts are initiated, denied, and/or detected and logged by Illumio, investigation can be triggered sooner, and detection achieved more rapidly – thus reducing attackers dwell time

3 AUTOMATED RESPONSE

Automatically generate containment policies in real-time

Auto-generate policy to mitigate exposure to live vulnerability risk. Rapidly identify ports being used by the ransomware to confidently activate selective port-blocking, isolation or quarantine policies for infections.

4 ERADICATION & RECOVERY

Use Illumio for visibility of both known and potential infected nodes, and to control fine-grained access to all such nodes by the eradication crew only. Easily and confidently migrate cleansed nodes back onto the clean network.

Lion Hops From a Ransomware Attack to a Resilient Security Infrastructure With Illumio: Online Case Study.

> Regardless of which industry you're in, technology is essential to business growth. And to grow quickly and responsibly, leadership must be able to trust that the organization's technology and data is secure. Illumio makes not only our technology team, but also our entire business confident that our operations are secure and resilient to inevitable cyberattacks now and as we scale.

Jamie Rossato
Chief Information Security Officer at Lion

illumio

Demo

illumio

Thank you