illumio

SOLUTION BRIEF

Faster Incident Response and Recovery With Illumio

Respond to breaches and restore environments securely with Zero Trust Segmentation

Breaches are inevitable

Despite record spending on cybersecurity, organizations continue to be breached at great financial and reputational cost.

- The average cost of a data breach reached **$4.45 million** in 2023, an all-time high.
- It takes organizations an average of **277 days** to uncover, identify, and contain a breach in 2023.
- Speed matters. Organizations spend nearly **23% less** when breaches are identified and contained in less than 200 days compared to when they take longer.

Incident response planning is critical

The response to incidents can never be fast enough. That's why a proper incident response plan — the steps used to prepare for, detect, contain, and recover from a breach — is fundamental cybersecurity hygiene.

When you're breached, one of the first calls is often to your cyber insurance carrier. Your carrier will typically assign a Digital Forensics and Incident Response firm (DFIR) or a recovery firm to stop the attack, perform remediation to get you back online, and conduct forensics.

But these firms are going into networks they don't know almost completely blind and working against the clock to limit a breach's impact and damage.

Whether you are working with an IR firm or handling the restoration yourself, it's critical to minimize the impact of the breach immediately. The more an attack spreads, the more devices are compromised — and that means more time and money you spend to secure and recover them.

> “The Illumio Zero Trust Segmentation Platform has already helped us to stop dozens of attacks from spreading mid-breach and has proven to be a valuable addition for our response teams.”
>
> **– Matt Baruch**
> Senior Director
> MOXFIVE

Zero Trust Segmentation stops and contains breaches

Shorter breach lifecycles mean lower breach costs. Use Illumio Zero Trust Segmentation (ZTS) for incident response and recovery to:

- Proactively prepare for breaches with complete network visibility and granular policy to isolate high-value assets
- Stop the spread of a breach and isolate compromised systems during an active attack
- Enhance the effectiveness of your response by prioritizing your most critical business functions, even when the attacker is still in the environment

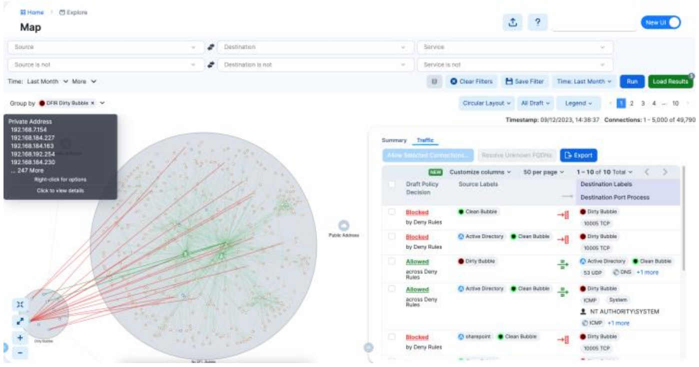
Zero Trust Segmentation can significantly reduce the time, money, and effort you spend on recovering from a cyber incident.

Reduce the impact of breaches at every stage

Prepare for inevitable cyberattacks

With Illumio, get immediate network visibility to see your environment and understand the potential impact of a breach. Use these insights to reduce your attack surface by limiting high-risk or administrative ports and outbound connections to the Internet.

Then, ringfence your critical assets to limit traffic in and out of devices, allowing you to quickly isolate them during a breach. This enhances your existing security tools, like endpoint detection and response (EDR), by giving them more time to detect and identify threats.



Timestamp: 09/12/2023, 14:38:37 Connections: 1 - 5,000 of 49,790

Draft Policy Decision	Source Labels	Destination Labels Destination Port Process
Blocked by Deny Rules	Clean Bubble	Dirty Bubble 10005 TCP
Blocked by Deny Rules	Active Directory, Clean Bubble	Dirty Bubble 10005 TCP
Allowed across Deny Rules	Dirty Bubble	Active Directory, Clean Bubble 53 UDP, DNS +1 more
Allowed across Deny Rules	Active Directory, Clean Bubble	Dirty Bubble ICMP, System NT AUTHORITY\SYSTEM ICMP +1 more
Blocked by Deny Rules	sharepoint, Clean Bubble	Dirty Bubble 10005 TCP

Respond quickly to an active breach

During an active breach, Illumio's application dependency map helps you see where the attack is occurring in real time. This allows you to quickly implement segmentation rules to block known infection paths and stop the attack from spreading further into your environment. Illumio can then quarantine infected systems with ringfencing so that breaches can't spread to other machines.

Even if the attacker is still active in your environment, you can bring critical business systems online with Illumio by creating separate "bubbles" for clean and dirty devices.

Recover securely and prevent reinfection

Post-breach, Illumio helps to ensure compromised assets are completely isolated during the recovery process, helping to prevent reinfection that would disrupt business operations again. Further protect your high-value assets by blocking traffic across ports and protocols where the incident moved.

For forensic work, use Illumio's historical analysis of connections and traffic to gain an understanding of the incident's origins.

Illumio ZTS strengthens any incident response plan

Incident response planning and testing has proven to be a highly effective tactic for containing the cost and impact of a breach. Illumio ZTS gives security teams and responders a set of tools to make IR faster and safer.

Feel confident that you can prepare your organization for inevitable breaches and get back online faster post-breach with Illumio.

Learn more about incident response and recovery with Illumio

Visit:
illumio.com/solutions/incident-response-and-recovery

About Illumio

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.