illumio

SOLUTION BRIEF

Better Together: Illumio Endpoint and EDR

Combine breach containment with the power of your preferred endpoint security solution

Don’t pay the price for delayed detection

The “assume breach” mindset

As threat actors devise new methods to attack organizations, the importance of Endpoint Detection and Response (EDR) has never been greater.

Sophisticated threat actors leverage a combination of zero-day exploits, supply chain attacks, and social engineering tactics to launch their attacks, making them notoriously challenging to detect.

Modern security tools rely on AI and ML to quickly adapt to new attack patterns, but it still takes time to adapt to new zero-day exploits – time you might not have.

Best case scenario, detection takes seconds or minutes, but in reality, it can take days, weeks, and even months. According to a recent IBM report, the average time to identify and contain a data breach is a stunning 277 days.

Even with constant improvement in detection capabilities, attackers still find new ways around them. At any time, a breach can circumvent these defenses. The main question at this point is, what is the impact of that breach?

Faster detection reduces this risk, but it can be challenging to accomplish. Instead, better results can be achieved by combining detection capabilities with breach containment.

By stopping the spread of breaches, your EDR has the time it needs to detect and respond to attacks.

Combining Zero Trust Segmentation (ZTS) with EDR

Stop ransomware spread

Stop all endpoint-to-endpoint attacker spread instantly without breaking any applications.

Protect against zero-days

Increase available time for detecting attacks by preventing breach spread.

Control endpoint to server traffic

Use identity for granular access to the data center (e.g., only Finance users can access the application).

Manage admin access

Prevent non-admin endpoints from performing risky outbound connections like RDP, SSH, and WMI.

Contain breaches as they happen

Pre-build emergency containment policies that can be triggered by a SOAR for increased response speed.

Protect agentless devices

Prevent users from reaching SAN, NAS, Switch, Firewall, ESXI, HyperV, OT, and IOT instantly.

Why segmentation is essential for modern endpoint security

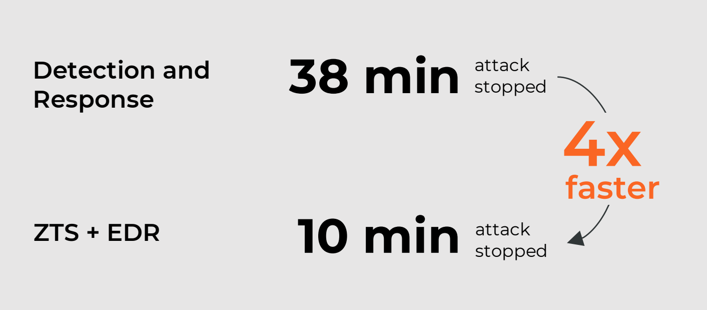
Attack-agnostic protection

Illumio Endpoint takes a proactive approach to stopping attackers from spreading by only allowing essential traffic to flow to and from endpoints.

Illumio Endpoint makes it easy to create allowlists for the right traffic while blocking risky traffic (eg., RDP, SMB, etc.) when there is no need for it – without the need for cumbersome GPOs or manual firewall rule writing.

By stopping spread, EDR and other detection tools have time to detect an incident before that compromised device grows into a full-blown disaster.

By enabling segmentation, attackers are forced to be noisier when trying to propagate, resulting in an attack being stopped 4 times faster compared to EDR alone.



Detection and Response

38 min attack stopped

4x faster

ZTS + EDR

10 min attack stopped

Bishop Fox, Ransomware Scenario Emulation 2022

Segmentation built for the hybrid world

Hybrid work environments are significantly more costly, averaging around $600,000 more than the global average, says IBM. As such, ensuring attackers can't move from any location is becoming increasingly crucial.

Illumio Endpoint addresses this challenge by enabling policies that travel with the user whether they are domain-joined in the office or non-domain joined at home or on the go. Illumio Endpoint enable segmentation policies to be rolled out based on the user's location, bolstering security without disrupting local connections.

Illumio Zero Trust Segmentation (ZTS)

With ZTS from Illumio, operators can proactively stop attacks before they can spread and cause significant harm.

Illumio achieves this in the datacenter, the cloud, and on endpoints by restricting traffic movement, effectively preventing the spread of ransomware, and blocking attackers from infiltrating deeper into the network.

No matter where devices are located, Illumio offers a traffic visibility that provides a comprehensive overview of potential risks, open ports, or misconfigurations.

Critically, Illumio limits the access users have to the data center. By leveraging user identity to only allow defined users access to the right workloads over a limited set of ports the datacenter is secured from one of your most vulnerable devices.

Want to learn more?

Read about Illumio ZTS at:

illumio.com/products/what-is-zero-trust-segmentation

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.