Key Findings From Bishop Fox Ransomware Emulation

Illumio Core stops ransomware attacks from spreading in less than 10 minutes

Stopping Breaches in a Dynamic, Hybrid World

Digital transformation and the accelerated sprint to the cloud has dramatically expanded the modern attack surface. Where IT was traditionally a walled in, on-premises environment, today, modern IT architecture is increasingly a hybrid mix of data centers, public clouds, multi-clouds and endpoint devices.

Over the past few years, new levels of hyperconnectivity have emerged as even more of our world has become remote and digital. Manufacturing operations are mostly automated, a trip to the hospital is now nearly an end-to-end digital experience, and you can enter and leave a retail or bank branch without interacting with a single human being.

This shift has created a substantial new set of attack vectors and opportunities for cybercriminals.

Putting Illumio Core to the Test

To measure the effectiveness of Illumio Core in detecting and responding to an active ransomware threat, Bishop Fox, a leader of offensive security and penetration testing, conducted a series of attack emulations. Each test measured whether the attack could be stopped, how long that would take, how many hosts were infected, and how many tactics, techniques and procedures (TTPs) were executed.

The red team (attackers) used a well-established set of TTPs from the MITRE ATT&CK and PRE-ATT&CK frameworks to attempt to infect hosts. The blue team (defenders) used detection and response technologies combined with Zero Trust Segmentation to measure the efficacy of ransomware containment.

The attack scenarios included:

- Detection alone
- Detection and Zero Trust Segmentation for incident response
- Detection and Zero Trust Segmentation, proactively blocking well-known ports used by ransomware
- Detection and Zero Trust Segmentation, proactively implementing full application ring-fencing

Illumio Core Stops Ransomware in Minutes

Bishop Fox's emulation proved that Zero Trust Segmentation stops attacks from spreading in 10 minutes, nearly 4 times faster than detection and response capabilities alone. Additionally, the report found that:

EDR should be paired with Zero Trust Segmentation to be most effective against ransomware and other cyberattacks.

The stricter the Zero Trust Segmentation policy and enforcement modes, the faster teams can detect and stop an ongoing attack.

Illumio Core can proactively limit the attack surface, reducing movement throughout the network following an initial attack.

The Results

The first infected host is also the last infected host with proactive Zero Trust Segmentation

SCENARIO 1 — Detection alone

Attack successful
All hosts compromised

This scenario was devoid of any Zero Trust Segmentation capabilities and resulted in complete success for the red team. They were able to execute all TTPs and infected all hosts after 2 hours and 28 minutes.

SCENARIO 2 — Detection and Zero Trust Segmentation for incident response

Attack stopped: 38 minutes
2 hosts compromised

This model had Illumio deployed in visibility mode, feeding alerts to the SIEM system, which was also collecting event data from EDR, Active Directory, Sysmon, etc. Upon detection of anomalous activity, the blue team deployed a containment policy. The attack was stopped in 38 minutes.

SCENARIO 3 — Detection and Zero Trust Segmentation proactively blocking well-known ports used by ransomware

Attack stopped: 24 minutes
2 hosts compromised

In this scenario, common ports that ransomware uses were blocked by Illumio to reduce lateral movement. The attack was stopped after 24 minutes with only two hosts compromised.

SCENARIO 4 — Detection and Zero Trust Segmentation proactively implemented with full application ring-fencing

Attack stopped: 10 minutes
1 host compromised

Full application ring-fencing was deployed, resulting in no spread of the ransomware. The attack was stopped within 10 minutes, contained to the first infected host. This result was four times faster than reactive deployment.

The difference between what an attacker can do in 10 minutes vs. 40 or 150 minutes is dramatic. That's why it's critical to pair perimeter security and detection and response strategies with Zero Trust Segmentation to stop the spread of a breach.

By adopting the Zero Trust mindset of "assume breach" and deploying Zero Trust Segmentation alongside EDR, modern enterprises can drastically improve their protection against ransomware — which can mean the difference between being able to operate during a cyberattack and major business failure.

Segment to Stop the Spread

Read the full Bishop Fox assessment report, Ransomware Scenario Emulation 2022.

Learn more about Illumio Core.

About Illumio

Illumio, the Zero Trust Segmentation Company, stops breaches 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.