illumio

CUSTOMER STORY

Lessons from a Digital Giant

How eBay achieved cyber resilience segmenting 3,000 servers and never breaking an app

From support desk to security lead

Serving 134 million active buyers in over 190 markets requires a complex infrastructure spanning thousands of workloads.

To stay resilient, eBay needed more than just traditional perimeter defenses. The company needed a new security model built for hybrid environments, dynamic workloads, and constant change.

That model was Zero Trust. And that's where Brian Hansen — now a senior systems admin at the online retailer— comes in.

"I started out answering phones in customer service," Hansen recalls. "Twenty-three years later, I'm leading a large-scale Illumio deployment protecting over 3,000 servers. Not because I started out as a security expert, but because I said yes."

When his direct manager spearheaded eBay's push into microsegmentation, a key pillar of Zero Trust, Hansen stepped up despite having no formal background in security.

"I had zero security experience. I knew what a firewall was, but that was it," he says. "But we had the mandate —and the tools — to do it right."

THE CHALLENGE

Complexity at cloud speed

With more than 3,000 Windows and Linux servers supporting around 250 unique applications — and about 350 total environments when dev and QA are included — traditional perimeter firewalls were no longer enough. The team needed:

- **Visibility into how applications actually talked**
- **Control to contain threats, even post-breach**
- **A rollout that wouldn't break anything**
- **Speed and scale without adding complexity**

"We used to play whack-a-mole trying to block every threat," Hansen says. "We had to flip the model to 'proactively contain and control.' "

Solution: Illumio Segmentation

Industry: Technology / E-commerce

Challenge: Stopping lateral movement and enforcing least-privilege access across a hybrid cloud infrastructure

Use cases:

- Ransomware containment
- Critical asset protection
- Asset mapping and visibility

Location: Global

Key benefits:

- Segmented over 3,000 servers across 250+ applications
- Zero application downtime during rollout
- Automated, scalable deployment with dynamic labeling
- Enhanced visibility, reduced noise, faster incident response

FROM VISIBILITY TO ENFORCEMENT

eBay's playbook

The journey began with visibility, operating Illumio in observation mode.

"For the first few months, we were focused on visibility," Hansen explains. "That helped us build confidence. When we saw what traffic was flowing — and what shouldn't be — we could act without fear."

Armed with real-time traffic maps, the team moved to policy enforcement in stages. Grouping servers by app and environment, it created rules in small batches, validated them, then scaled up.

"We didn't try to boil the ocean. We built one solid rule set at a time," Hansen says.

> We had to flip the model to proactively contain and control.

Automation that scales

Using Microsoft Endpoint Manager and PowerShell scripts, the team automated deployment and dynamic labeling. Nearly every new workload comes online labeled and in full enforcement.

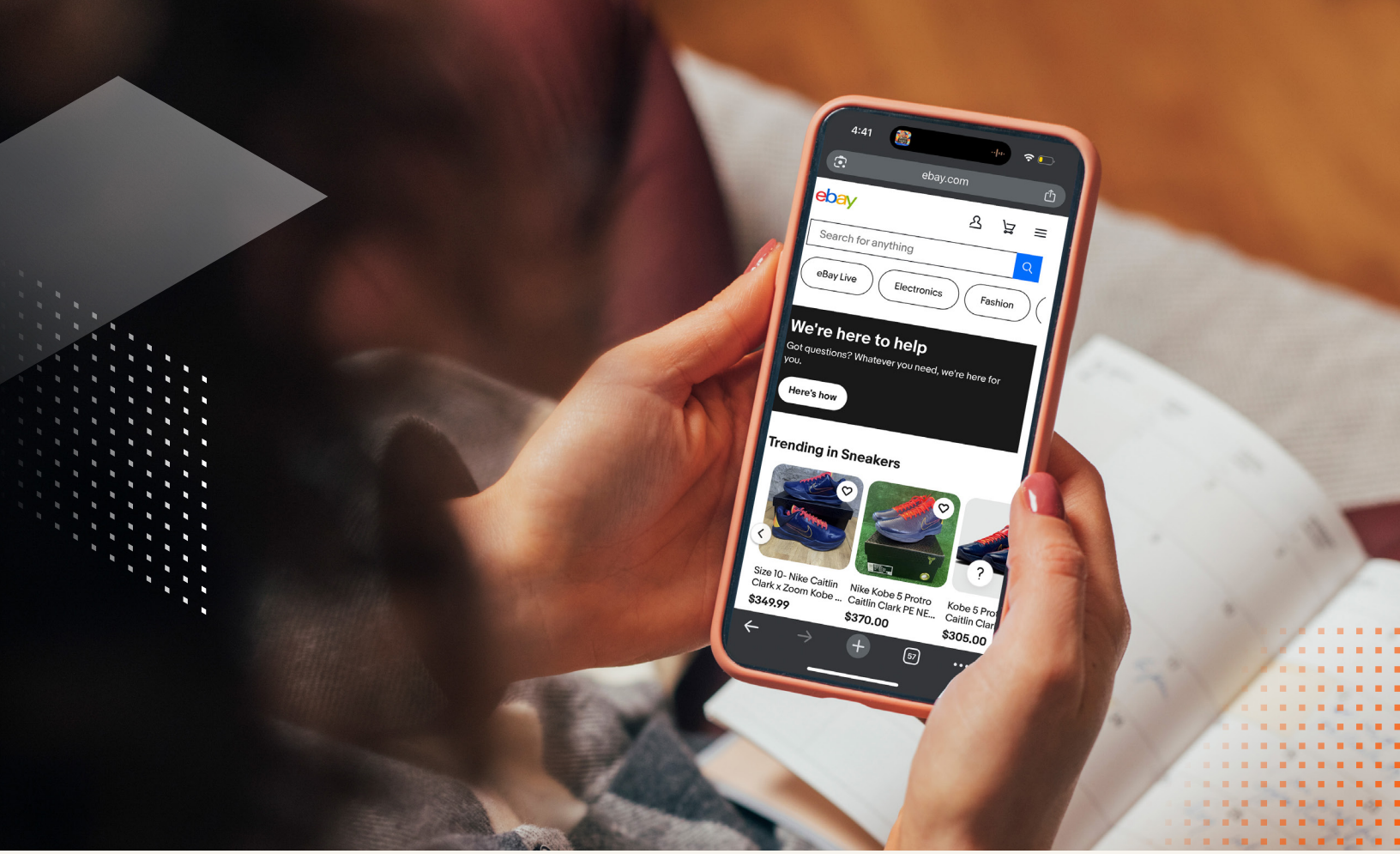
The team built the labels in advance, so as soon as a workload comes online and gets that label, the policy is already there.

Clean-up crew for unwanted traffic

Illumio didn't just stop threats. It surfaced unknown and unwanted traffic.

Hansen and his team discovered old load balancer health checks still running, misrouted app calls, and open ports that no one was using. Illumio helped them shut it all down.

Even app owners were surprised. As Hansen recalls, "They'd say, 'Wait, we're still using that port?' And we'd show them the data."



“Illumio let us build a resilient core first.

Critical first: Protect what matters most

The team started by locking down the most critical assets — DNS, domain controllers, identity systems — then moved outward.

“If those go down, everything else does,” Hansen says. “Illumio, let us build a resilient core first.”

Cross-team wins, company-wide confidence

The success wasn’t just technical. It was organizational.

“We worked with networking, infrastructure, and app teams. Everyone played a part. That’s what made it successful,” Hansen says. “When something breaks, app teams now come to us to check Illumio first. We can usually spot the issue in minutes.”

Results that matter

Zero downtime.
"We didn't break a single app during rollout.".

Faster troubleshooting.
"We can resolve issues in minutes — not hours."

Cleaner environments.
"We removed legacy flows, outdated configs, and noisy traffic."

Segmentation that never stands still

For Hansen, Illumio isn't just a one-time project. It's a living part of eBay's Zero Trust security strategy.

Hansen says the team regularly refines policies and monitors for anomalies to continually improve security.

And his advice for others?

"Don't wait until you've got it all figured out," he says. "Anything you do with Illumio makes you more secure than you were yesterday."

Breaches are inevitable.
Disasters are optional.

Visit illumio.com/illumio-platform