illumio

INDUSTRY BRIEF

Illumio for Supermarket Cybersecurity

With Illumio, you can contain ransomware and cyberattacks to keep your digital operations fully operational and protected

Cyber Threats Grow for Supermarkets

Retailers operating grocery stores and supermarkets cannot afford a moment of downtime in their sales or supply chain systems.

But criminal cyber gangs have gone beyond stealing credit cards and customer information. They are now seeking to seize control of key aspects of a retailer's operations to extort payments and cause harm.

For many supermarket organizations, these cyberattacks can disrupt supply chains and create severe financial and reputational damage.

Beyond crippling retail businesses, such disruptions can have a profound societal impact by causing shortages of essential goods that lead to hardships and put lives at risk.

The growing number of cyberattacks from ransomware and global hacker gangs are now a national digital security issue as they pose serious threats to the delivery of essential supermarket products, such as food and healthcare supplies.

Technical Challenges Facing Supermarkets

As their dependency on technology has grown, so too has grocery retailers' cybersecurity exposure.

- **New point-of-sale (POS) systems** that include self-scan and payment systems integrated with smartphone apps open up another pathway for cyberattacks and complicate PCI compliance
- **New e-commerce models** for pre-ordering items and having them delivered or reserved for collection in-store often include third-party organizations and cloud-based applications that can be difficult to secure
- **Rapidly and continuously developed applications** for new services and products need protection throughout their lifecycle to safeguard against the introduction of malicious code
- **Pharmacy services** require greater oversight and control to comply with privacy and healthcare laws while ensuring customer safety
- **Highly integrated supply chains** created for greater efficiency and speed expose retailers to cyberattacks via a compromised vendor, such as a processor, shipper or food supplier

Stop the Lateral Movement of Cyberattacks

Illumio helps supermarket operators address essential digital security needs to segment and isolate critical computing resources

Identify Areas of Risk
By visualizing the connectivity among devices and applications, supermarket retailers can understand their cyber exposure to know what is talking to what.

Contain Ransomware
Easily segment systems and applications. Quickly ring-fence critical computing resources and instantly shut down pathways during an incident response.

Build Long-Term Protection
With Zero Trust Segmentation, supermarket chains can contain breaches at the point of attack, preventing threats from advancing to cause damage.

Ensuring Business Continuity: Stop Cyberattacks in Their Tracks

Zero Trust Segmentation isolates breaches to prevent the spread of a cyberattack across a supermarket's digital infrastructure.

Though traditional hackers have looked to acquire and sell customer and credit card data, new attacks focus on compromising POS systems or logistics infrastructures to disrupt or gain control of business operations.

Whether looking to steal or disrupt, cybercriminals want access to as many systems as possible to reach the highest value assets (system controls, financial data, customer info, etc.).

To do so, they need to move through networks, data centers, clouds and devices to reach critical applications and their data. The greater number of computing assets compromised, the more damaging the attack.

> "The challenge with Zero Trust security for retailers has been in isolating legacy environments and applications. Illumio addresses this issue by providing a unified, real-time view into communications flows and a straightforward way to safely implement microsegmentation by application."
>
> **Jon-Michael Lacek**
> **IT Operations Manager**
> **Wegmans**

Unchecked, ransomware and other cyberattacks can cause increasingly serious financial and reputational harm to supermarket retailers.

Illumio Zero Trust Segmentation

By using Zero Trust Segmentation from Illumio, supermarket operators can stop cyberattacks before they spread to cause significant damage.

Illumio restricts the movement of traffic to only verified sources using allowed protocols. This prevents ransomware from stowing away on communication pathways to move across hybrid computing environments.

Illumio provides a crystal-clear map of the communication between your systems and application, offering a detailed view of any potential risks, open ports, or firewall misconfigurations.

Critically, Illumio can map and segment traffic among traditional data centers and clouds, as well as devices on IoT and OT networks, such as sales systems, freezers, alarms, etc. With this information, simple security policies can be applied with a click of the mouse.

With Zero Trust policies enforced by Illumio down to the workload level, supermarket operators can contain breaches and prevent malware from spreading to critical systems, ensuring business resilience and operational continuity.

Zero Trust Segmentation for Modern Cybersecurity Protection

Learn more about how Illumio can help supermarkets and other retailers better defend against ransomware and other cyberattacks.

Please email our team of experts at AMS-Channel@illumio.com.

About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.