SYMMETRY

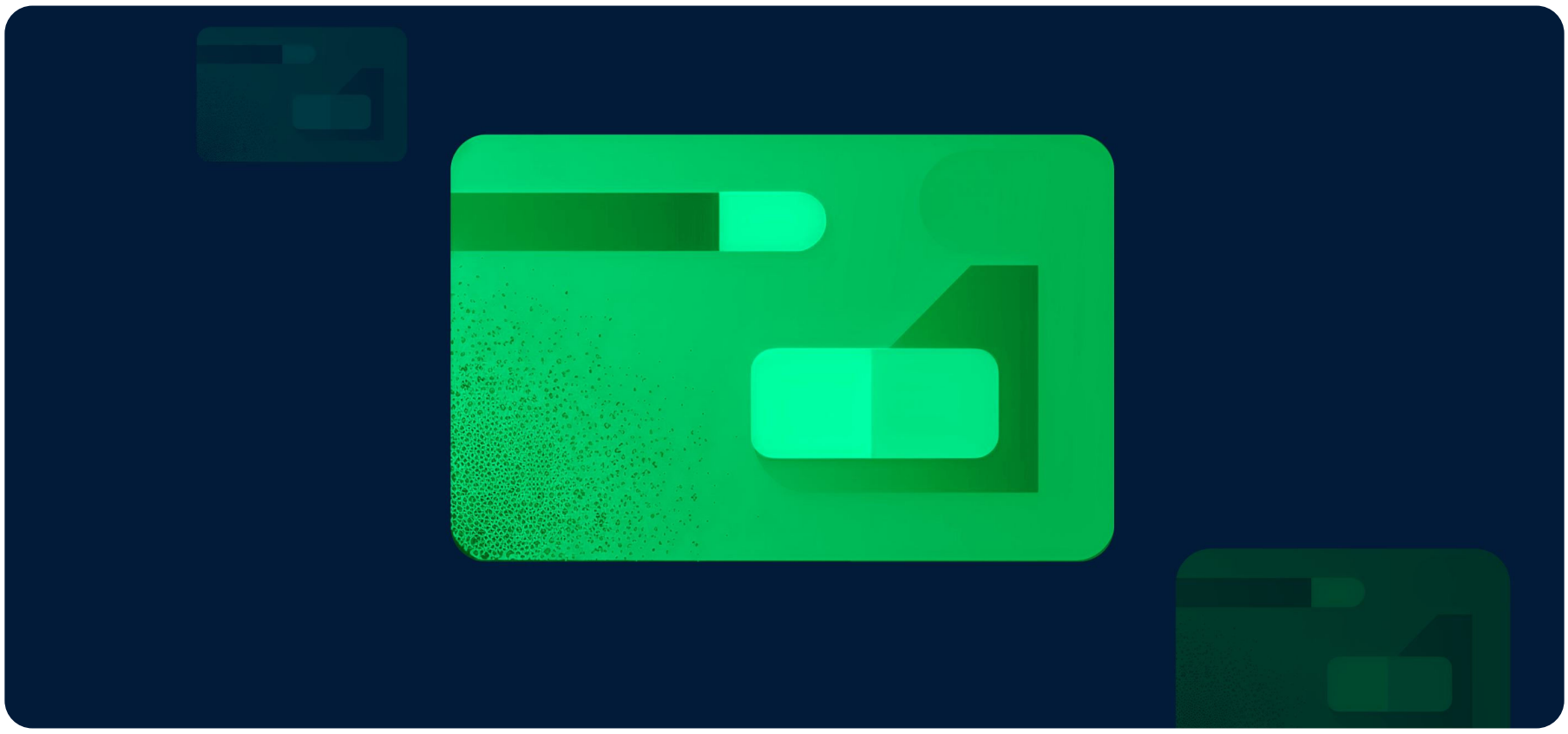
WHITE PAPER

Retail & Ecommerce

Retail and ecommerce businesses have been all over the news on account of being the victims of a plethora of cyber attacks. Ecrime is one probably the most active attack vector to date. Be it ransomware, point-of-sale system compromises, eskimming, phishing, or other attacks, ecommerce cybersecurity teams have had to fight harder than most to keep their businesses safe from threat actors.

With customer data at stake, a cyberattack places retail and e-commerce and their supply chain partners at significant risk for cyber attacks. Obtaining private identifiable information (PII), credit card data, and business data is a lucrative goal for threat actors. Credit card information, as an example, can fetch an average of $500 per card on the dark web. Most cybersecurity technologies and processes were designed to defend the businesses security perimeter, not the data the malicious hackers want to attain. Retail & ecommerce industry cybersecurity teams need to evolve from securing the perimeter and endpoints, to establishing data security practices to protect customer data and their businesses brand.

The Retail & E-commerce Data Security Challenge: Protecting Customers and Brand



COMPLIANCE AND DATA PRIVACY

In order to conduct digital business, customer information is collected by retailers in droves. Also, most retail and e-commerce organizations operate across multiple jurisdictions and borders, and are challenged to maintain pace and compliance with various evolving privacy law requirements – GDPR, CCPA, PCI, and more.

CUSTOMER DATA PROTECTION

It has been reported 69% of consumers would be less inclined to do business with a breached organization.
The Verizon Data Breach Investigations Report (DBIR) outlined that 61% of attacks targeted payment card data. Retailers must secure their environment with Payment Card Industry Data Security Standards (PCI DSS) compliance requirements, or they will be subject to fines. In order to protect customer data, you need to know where it is stored, who has access to it, and what is being done with that data.

Data Security Best Practices with Cloud Adoption

Comply with PCI, GDPR, CCPA and other regulations by establishing cybersecurity practices from the data out.

Minimize potential data risks and exposure with visibility into the enterprise data across cloud environments.

Automate data management and security tasks on a single console for the hybrid cloud.

Symmetry Systems DataGuard

Symmetry's platform is engineered specifically to address modern data security and privacy challenges at scale from the data out, providing organizations the ability to innovate with confidence. With total visibility into what data you have, where it lives, who can access it, and how it's being used, Symmetry safeguards your organization's data from misuse, insider threats, and cybercriminals, as well as unintended exposure of sensitive IP and personal information through use of generative AI technologies.

WHAT WE DO

Symmetry offers comprehensive visibility and control over your data, addressing all aspects of your data security requirements, including the full spectrum of functions outlined in the NIST Cybersecurity Framework.

Identify

Discovers, classifies, maps, and monitors sensitive data across cloud, on-prem, and hybrid environments.

Detect

Identifies and creates alerts for abnormal data behaviors and data policy violations in real-time.

Protect

Discovers, classifies, maps, and monitors sensitive data across cloud, on-prem, and hybrid environments.

Respond & Recover

Contain the security and business impact of compromised identities and impacted data with speed and precision.

INTEGRATION INTO YOUR MODERN DATA+AI SECURITY STACK

Cloud Storage

On Premise

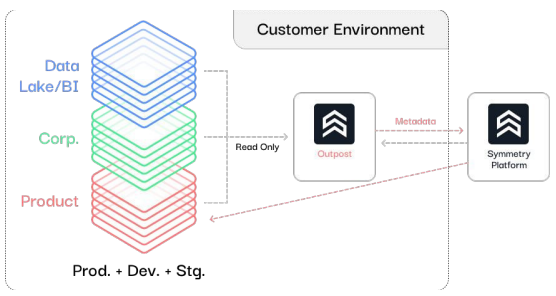
SaaS Storage

Data Governance

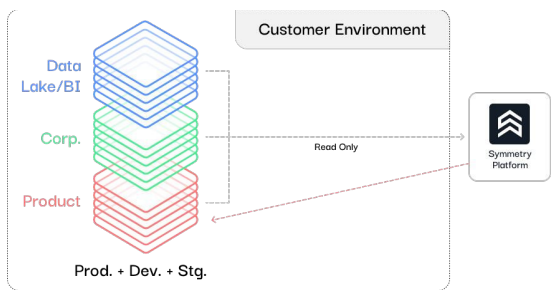
FLEXIBLE DEPLOYMENT MODEL FOR YOUR ENVIRONMENT

Our deployment model is tailored to your operational needs and risk appetite. Whether it's air-gapped, fully in your cloud, traditional SaaS, or hybrid-cloud – we have done it.

SaaS Model



Outpost Model



Air-Gapped/In-Your-Cloud Model*