

# Building Greater Security, Compliance, and Control for Retailers

As retail data breaches continue, smart businesses are seeking a proactive approach to protect their customers and their brands.

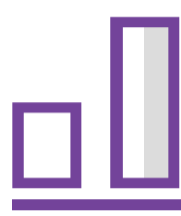


## Retail Landscape



**60%**

of non-ecommerce retailer breaches were skimmers installed in gas pump terminals and ATMs.<sup>1</sup>



**Top 10**

Retail is one of the top 10 targeted cybercrime sectors.<sup>2</sup>



**3.2**

PCI DSS 3.2 added new security requirements for retail.<sup>3</sup>

## Real-World Breach



Attacker phishes a 3rd-party contractor.



Attacker uses stolen credential to access company's network.



Attacker uses malware to infect vulnerable servers leading to POS access.



Malware scrapes RAM for clear text mag strip data.



Malware stores credit card data on an internal server.



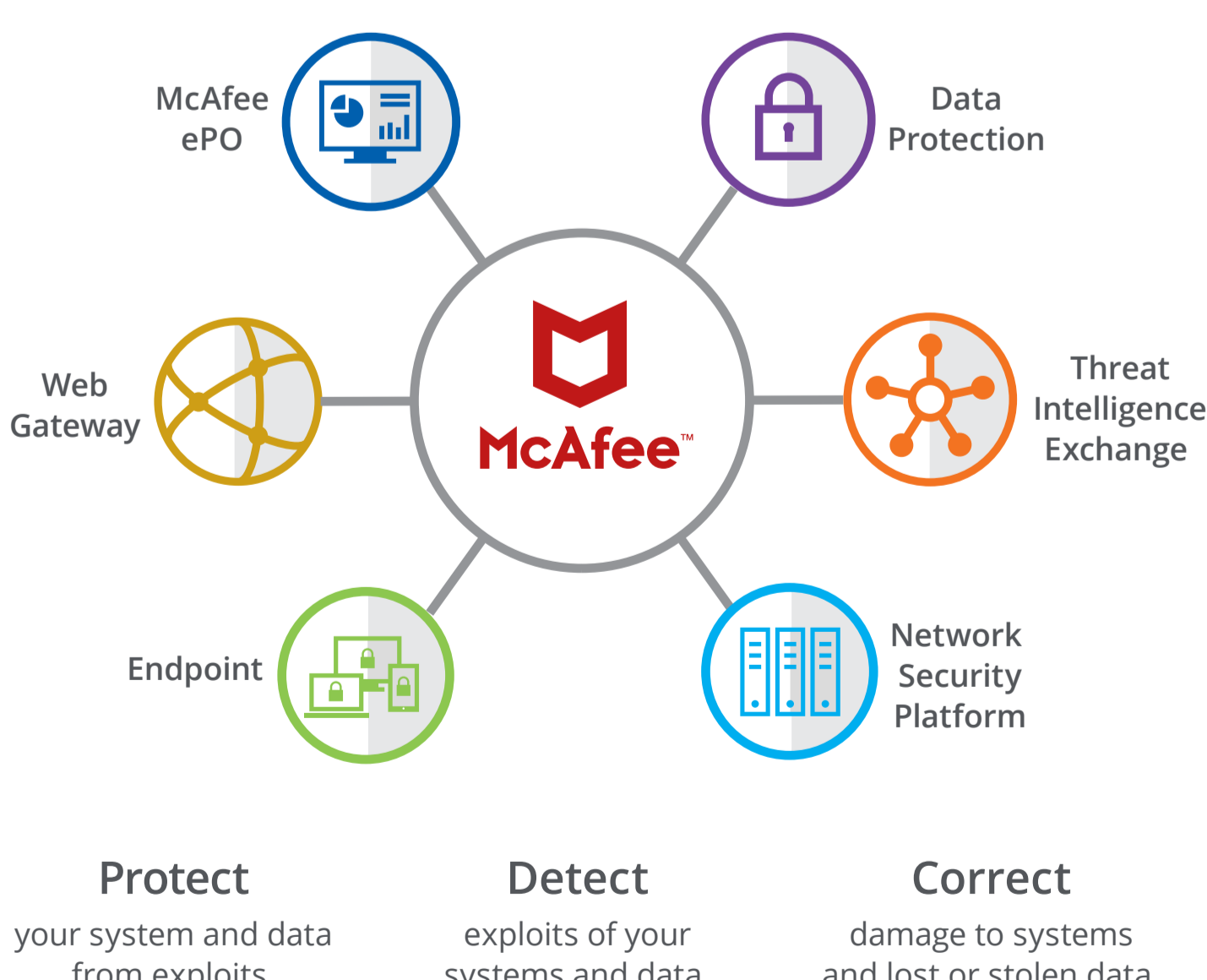
Stolen data exfiltrated and sent to attacker FTP servers.



Millions of credit card accounts' information compromised.

## Security by Design

Protect ATMs, registers, point-of-sale systems, kiosks, networked devices, digital signage, and more.



Learn more: [www.mcafee.com/embedded](http://www.mcafee.com/embedded)

1. Verizon 2017 Data Breach Investigations Report  
<https://www.mcafee.com/us/security-awareness/articles/verizon-2017-dbir.aspx>

2. McAfee Labs Threat Report  
<https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-jun-2017.pdf>

3. [https://www.pcisecuritystandards.org/security\\_standards/](https://www.pcisecuritystandards.org/security_standards/)