Global Security Report 2011

Charles Henderson
Director of Application Security Services
Trustwave's SpiderLabs

Agenda

- Introduction
- Incident Response Investigations
- Malware Statistics
- Attack Vector Evolution
- Strategic Initiatives
- Global Conclusions
- Questions?

Introduction

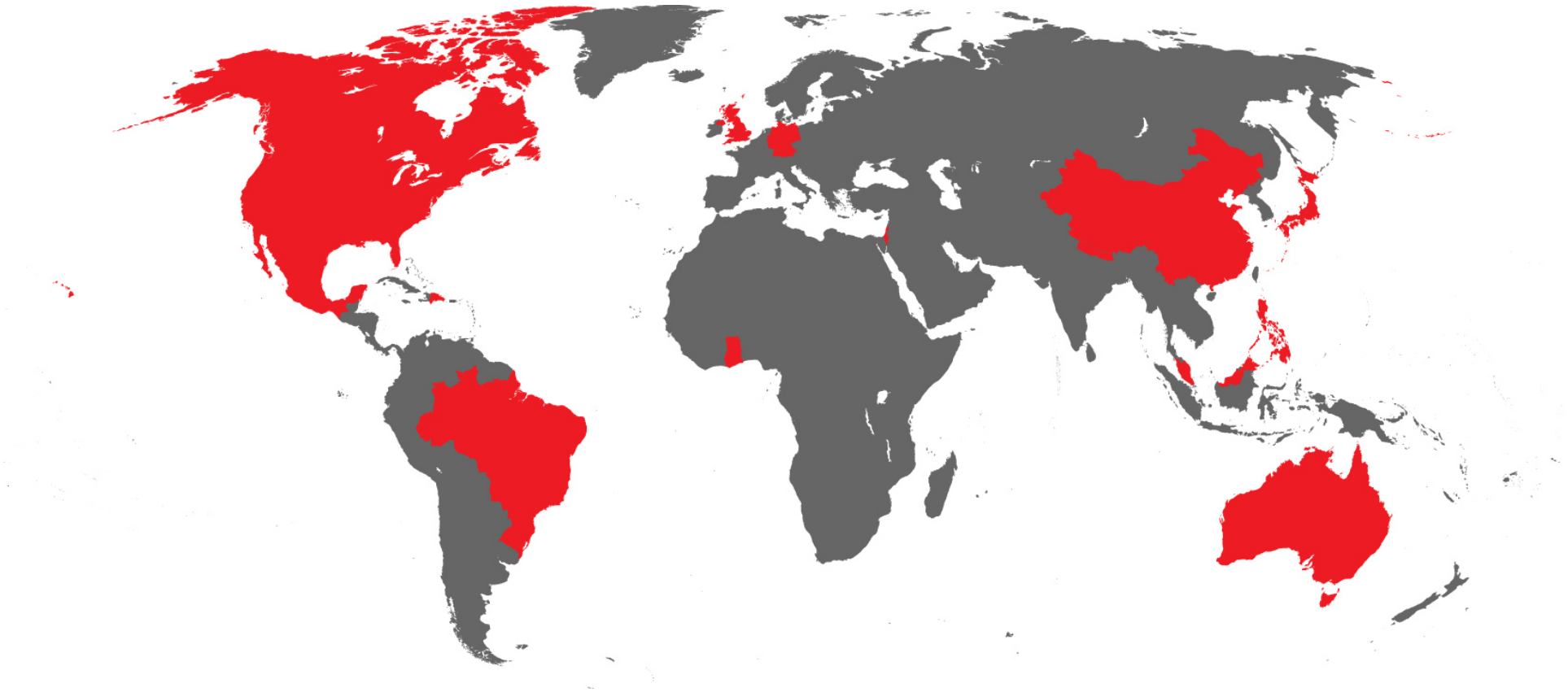
About Trustwave's Global Security Report:

- Issued annually
- Based on findings and evidence from work conducted by Trustwave's SpiderLabs in 2010
- Serves as a tool to educate and assist in planning business security strategy
- More than 200 investigations and 2,000 penetration test results contributed to the analysis and conclusions
  - Data gathered from Top 20 GDP countries
- Download the report for free: https://www.trustwave.com/GSR

Trustwave

Incident Response Investigations

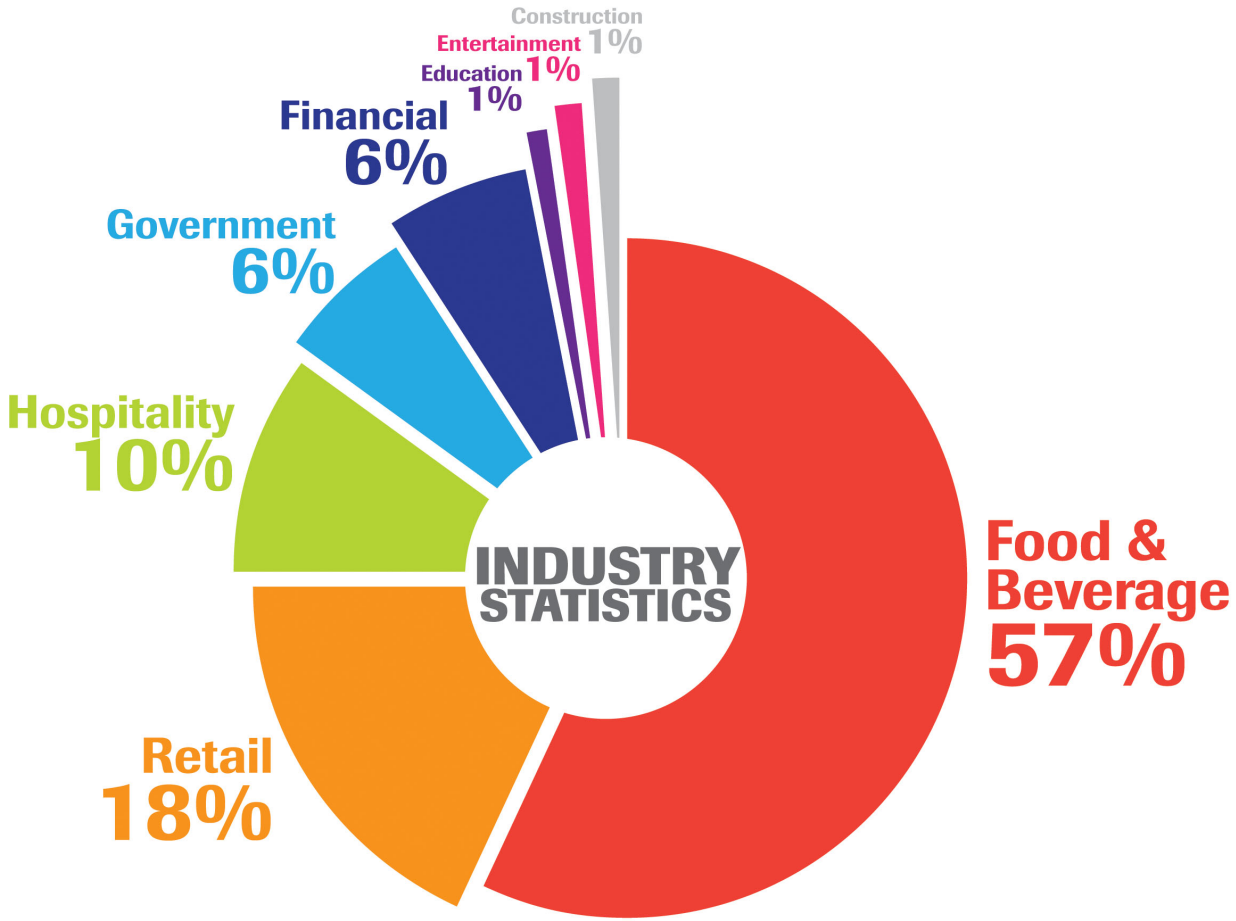
- Countries Represented



Trustwave®

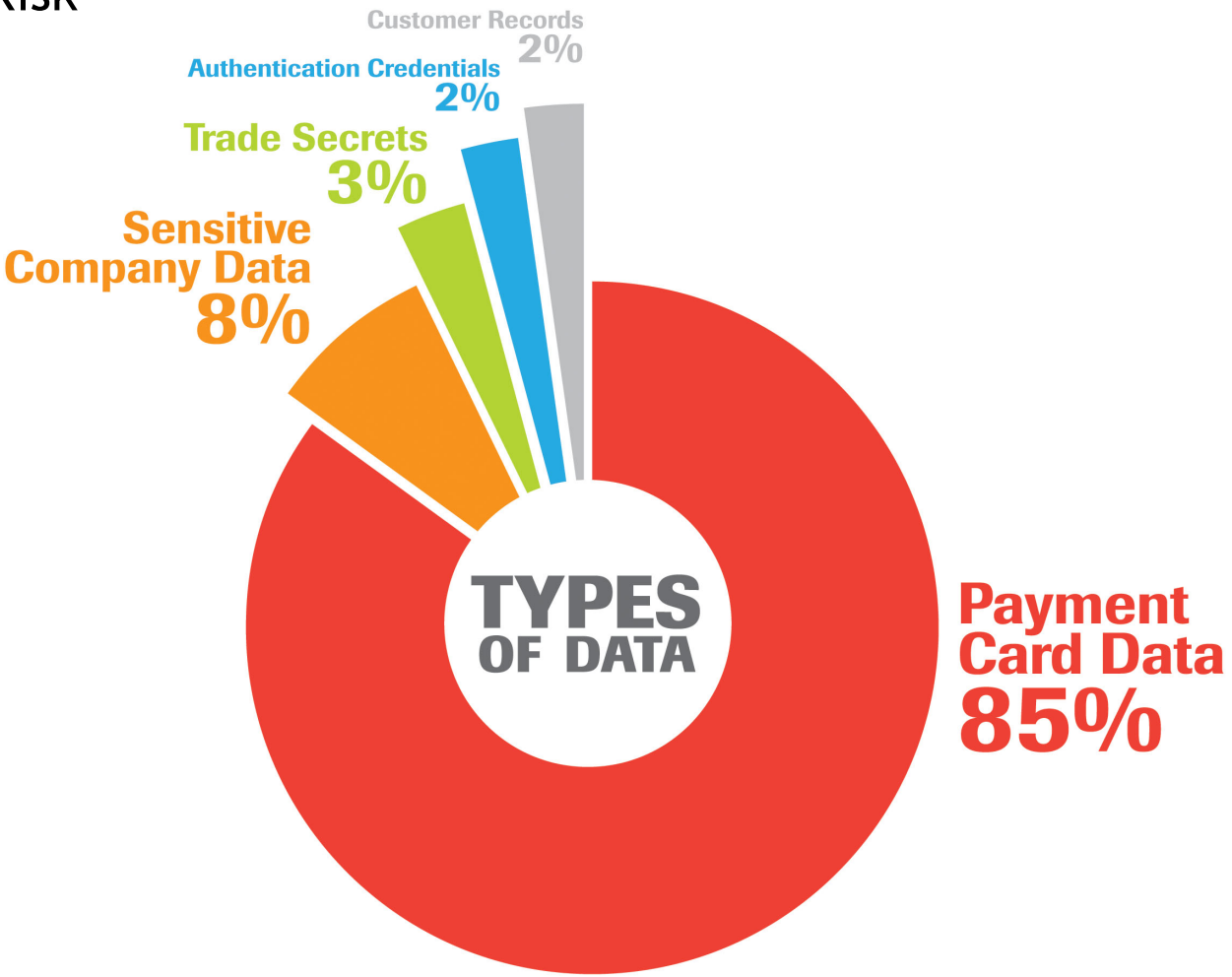
Incident Response Investigations

- Industries Represented



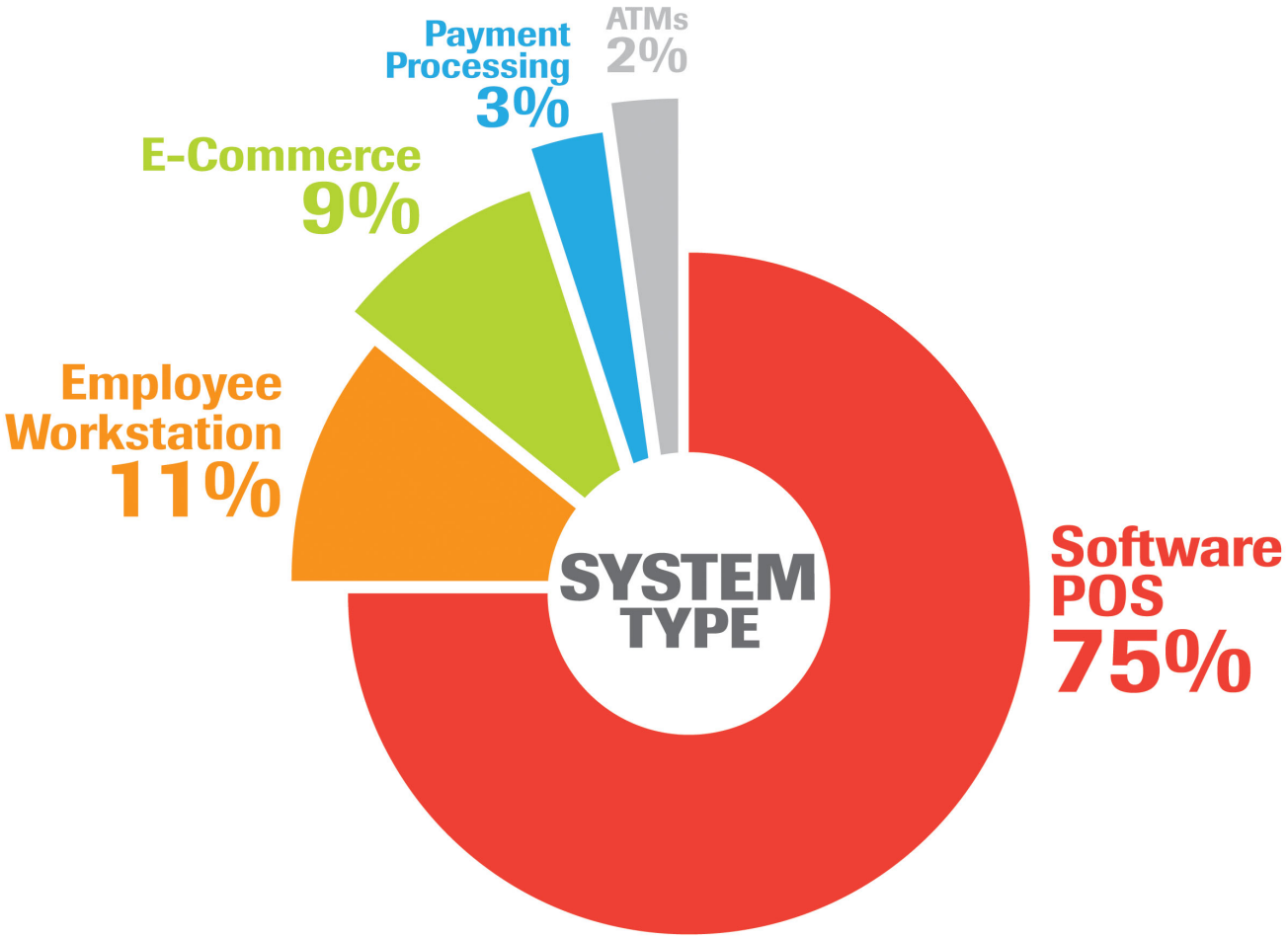
Incident Response Investigations

- Data at Risk



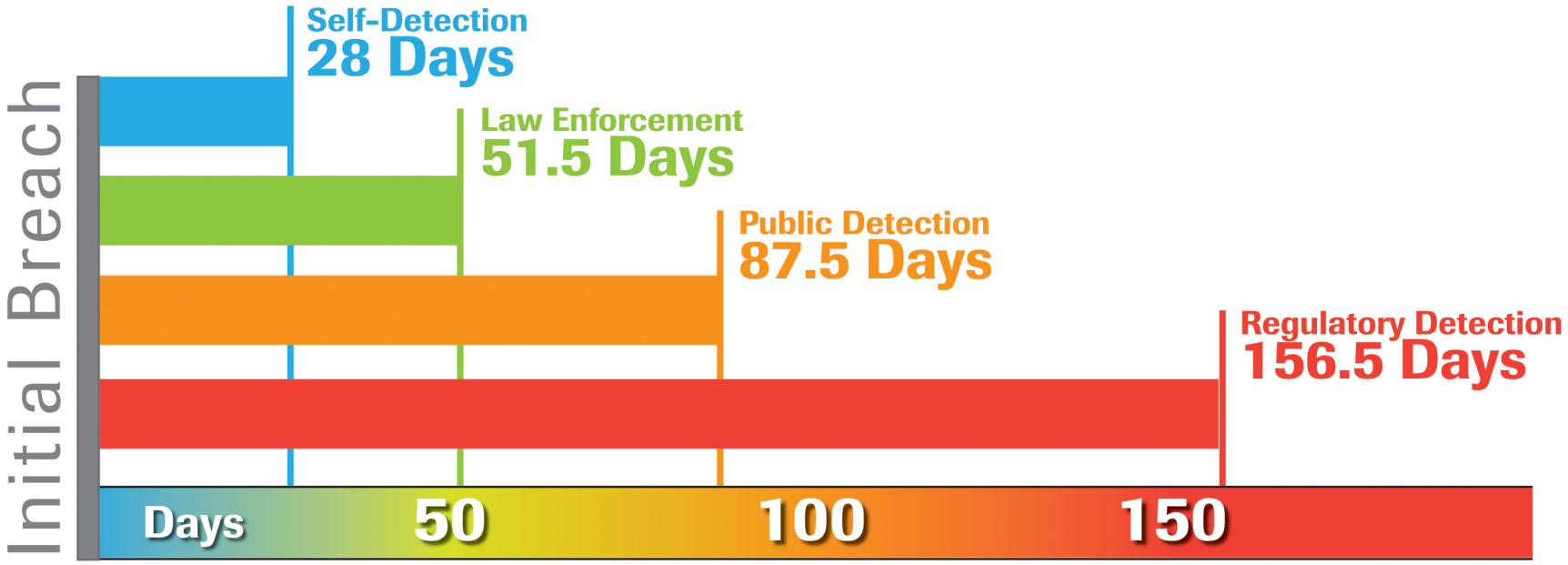
Incident Response Investigations

- Target Assets



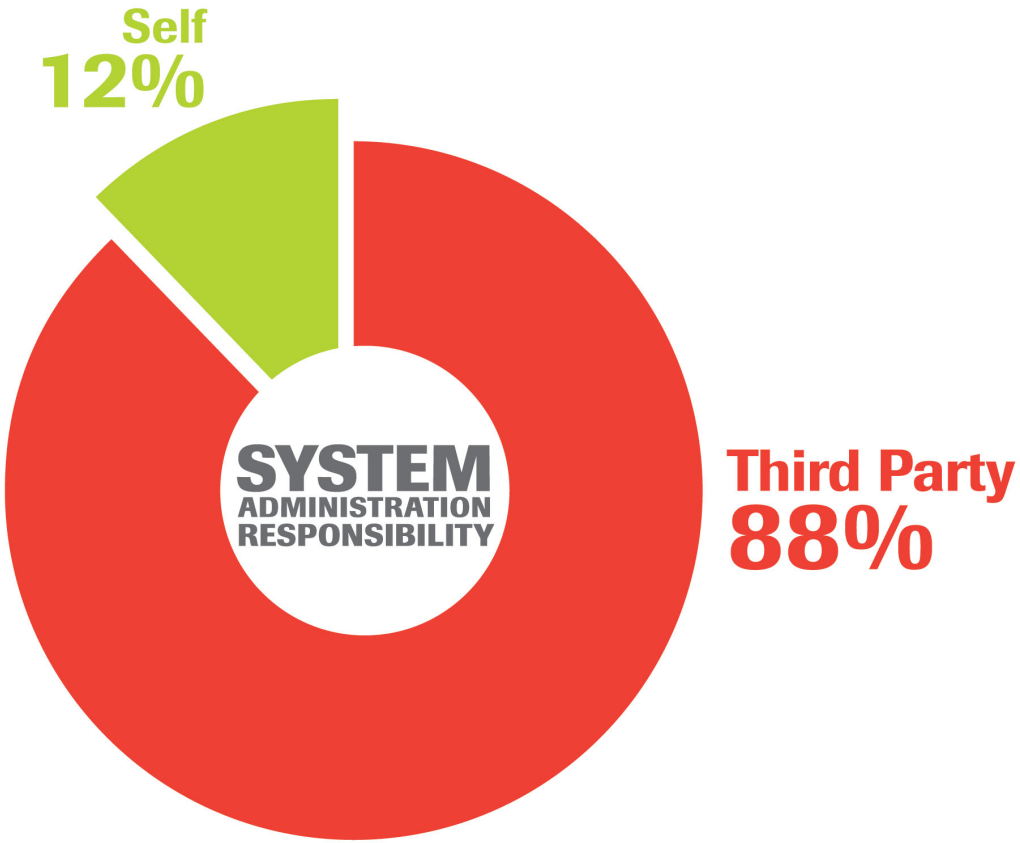
Incident Response Investigations

- Detection Methods vs. Time



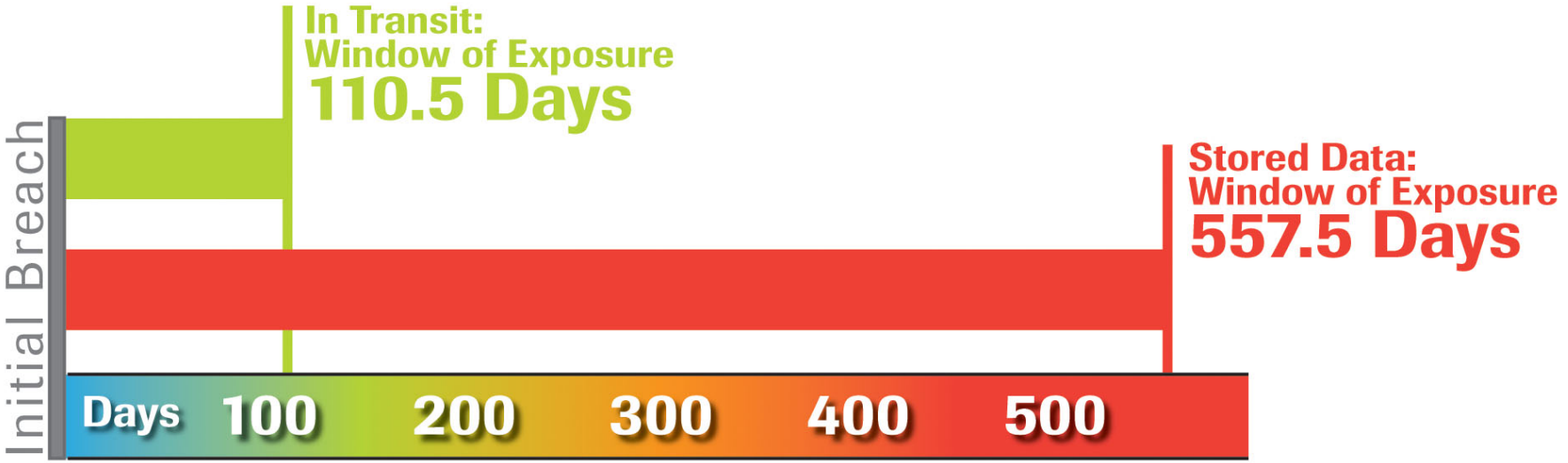
Incident Response Investigations

- Administration Responsibility



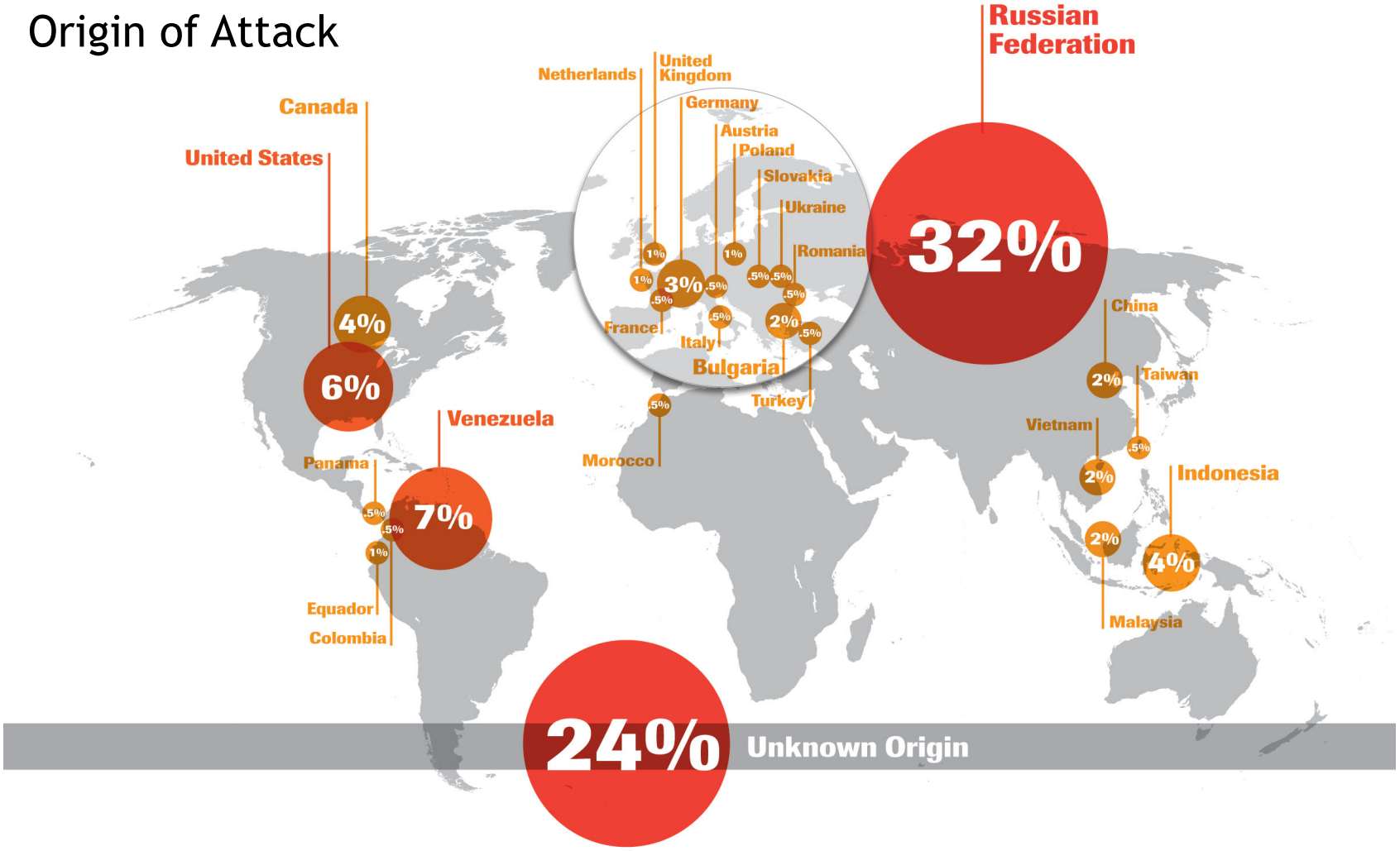
Incident Response Investigations

- Window of Data Exposure



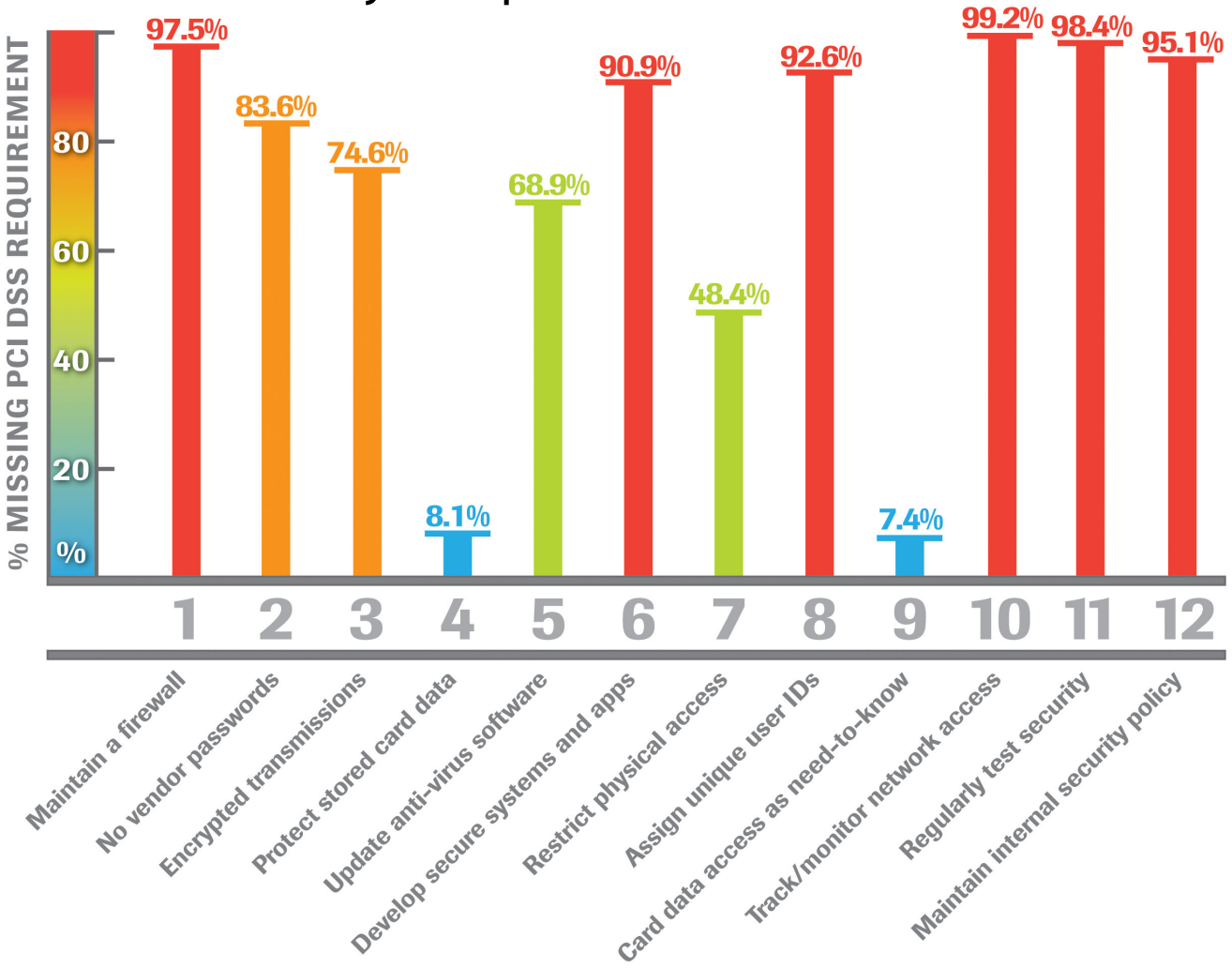
Incident Response Investigations

- Origin of Attack



Incident Response Investigations

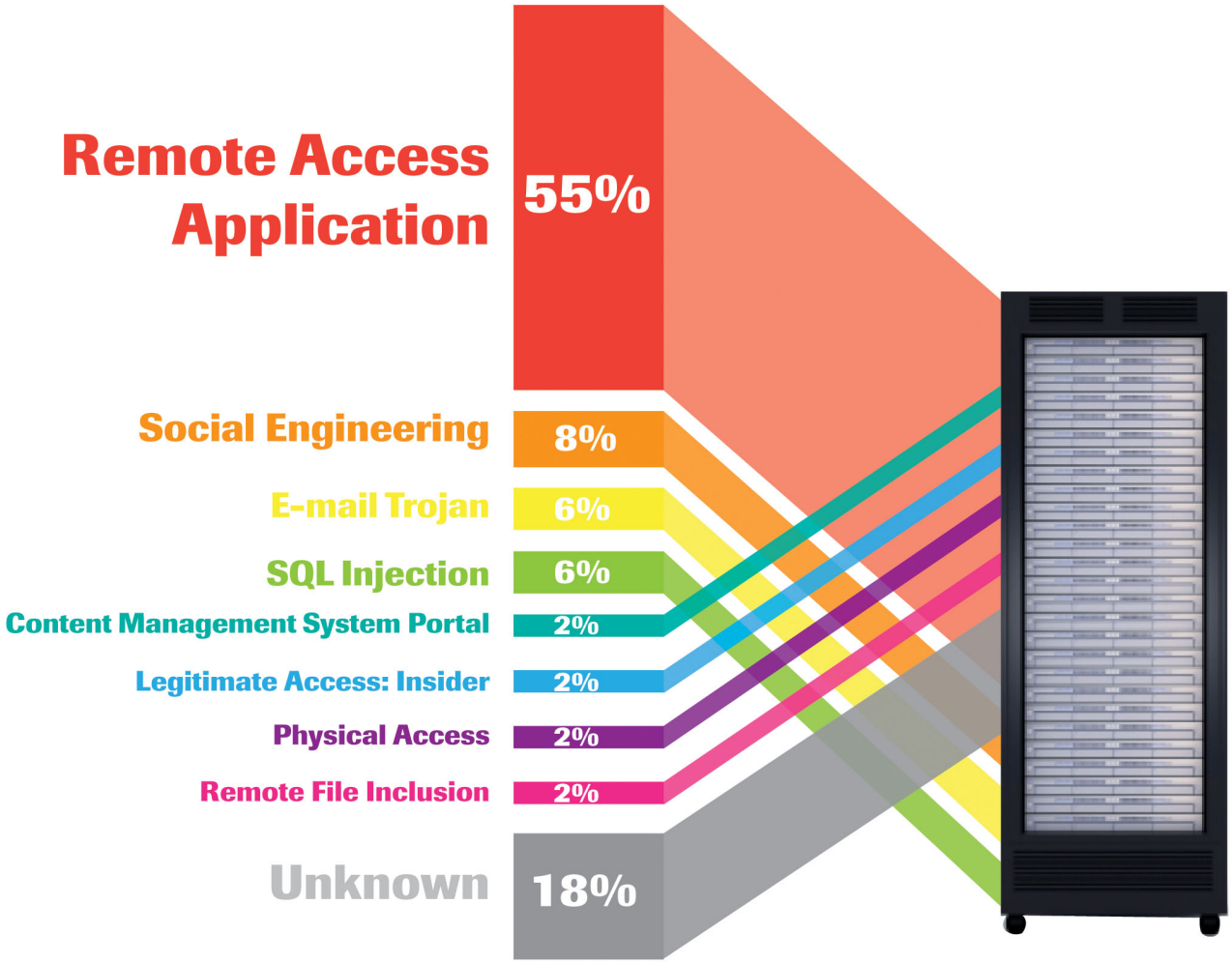
- Payment Card Industry Compliance



Trustwave®

Breach Triad – Infiltration, Aggregation, Exfiltration

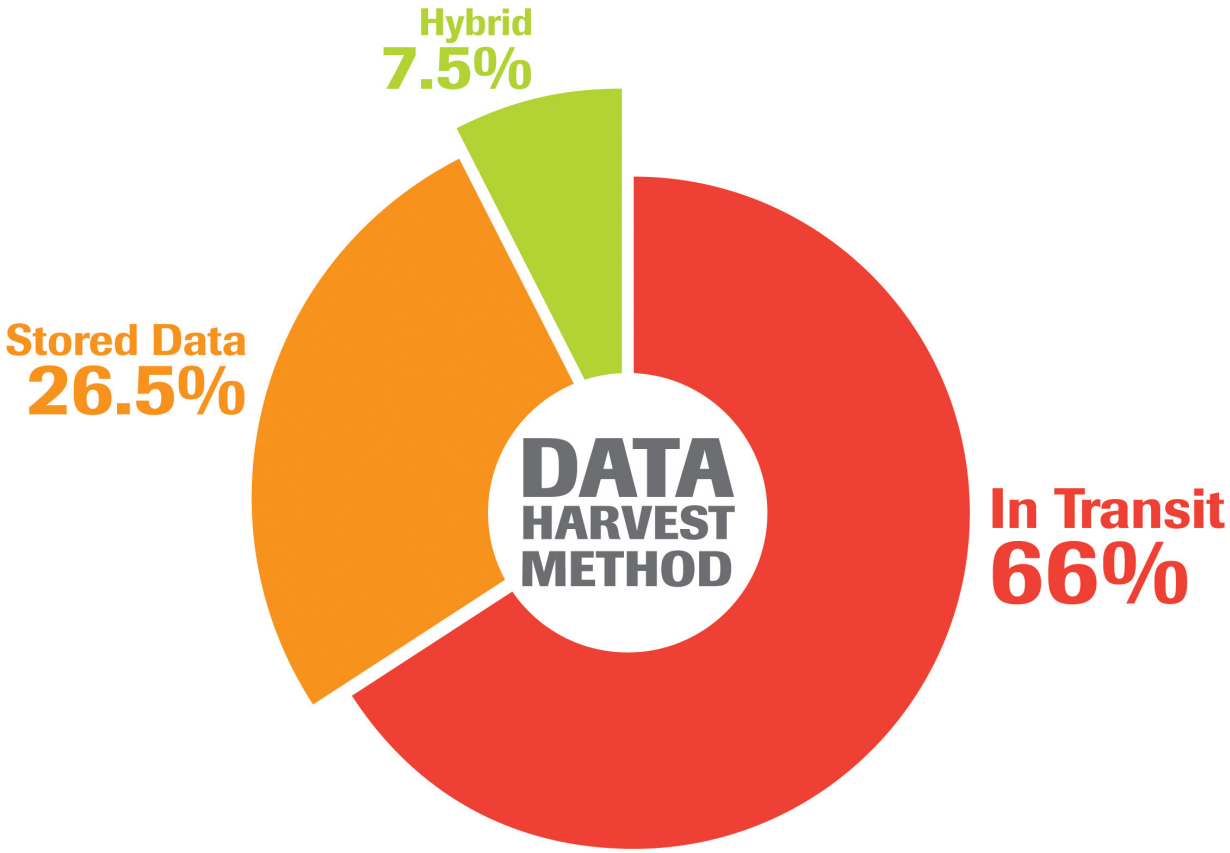
- Infiltration



Trustwave®

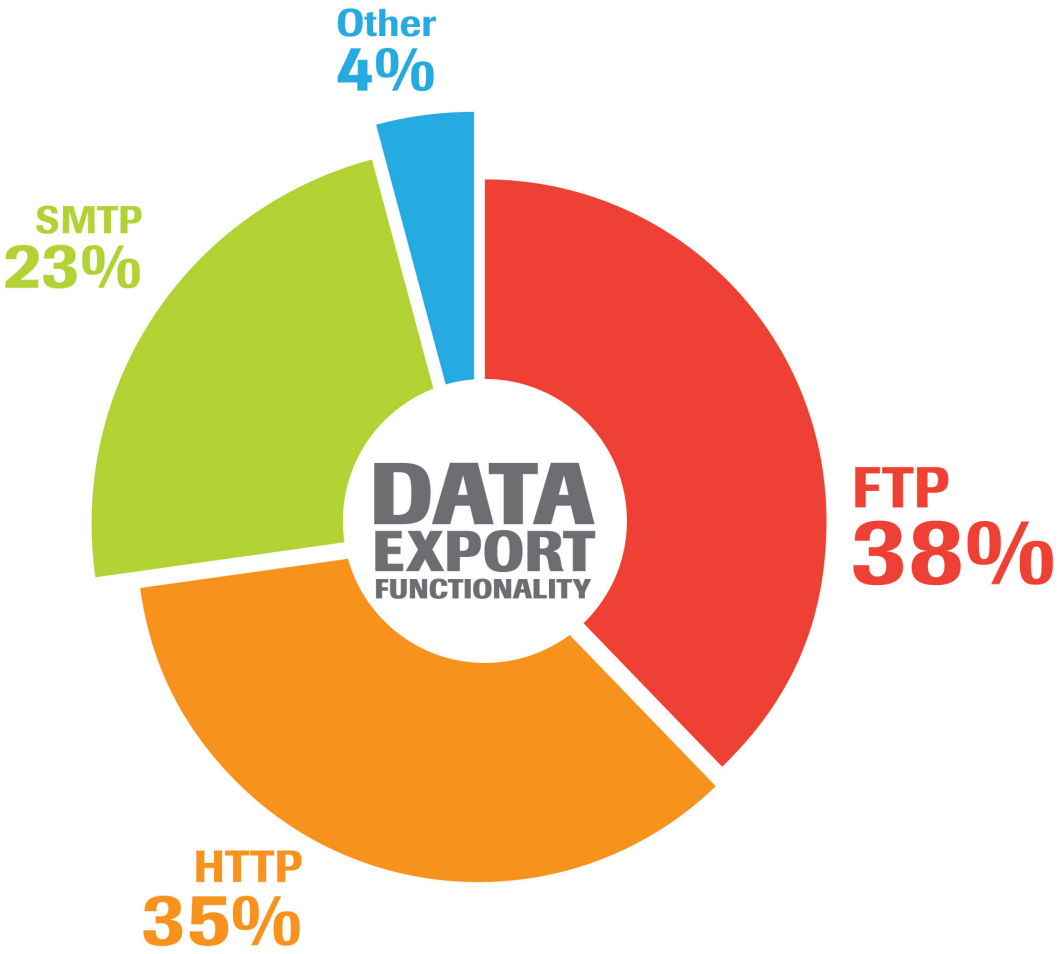
Breach Triad – Infiltration, Aggregation, Exfiltration

- Aggregation



Breach Triad – Infiltration, Aggregation, Exfiltration

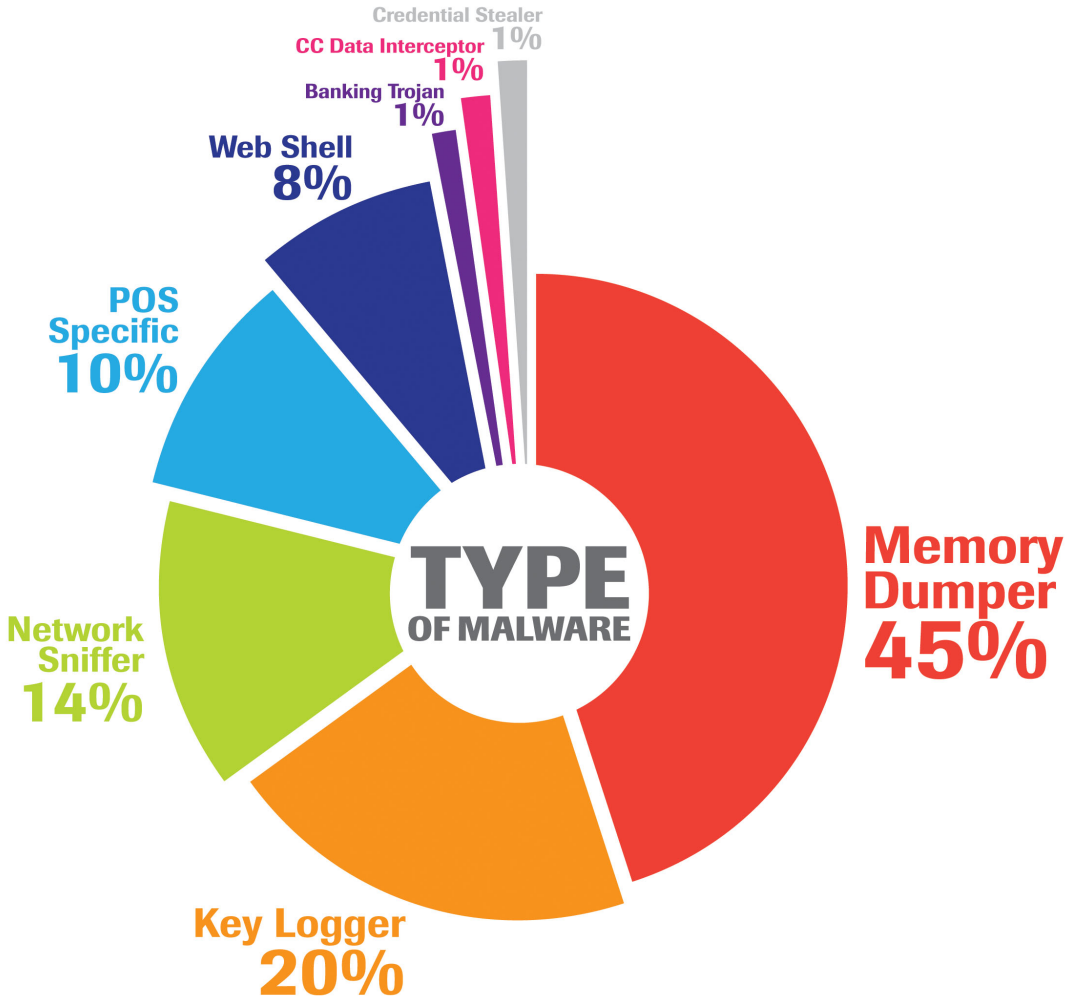
- Exfiltration



Trustwave®

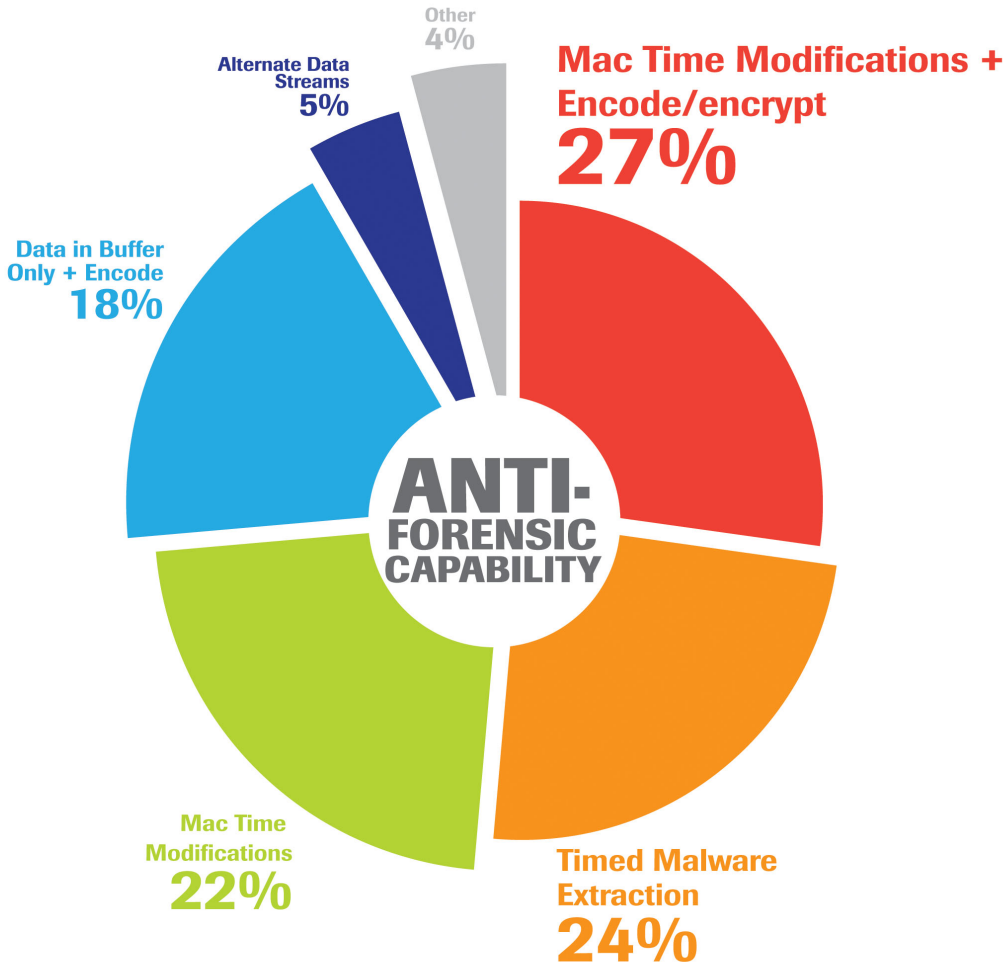
Malware Statistics

- **Data Points of Interest:** Classification

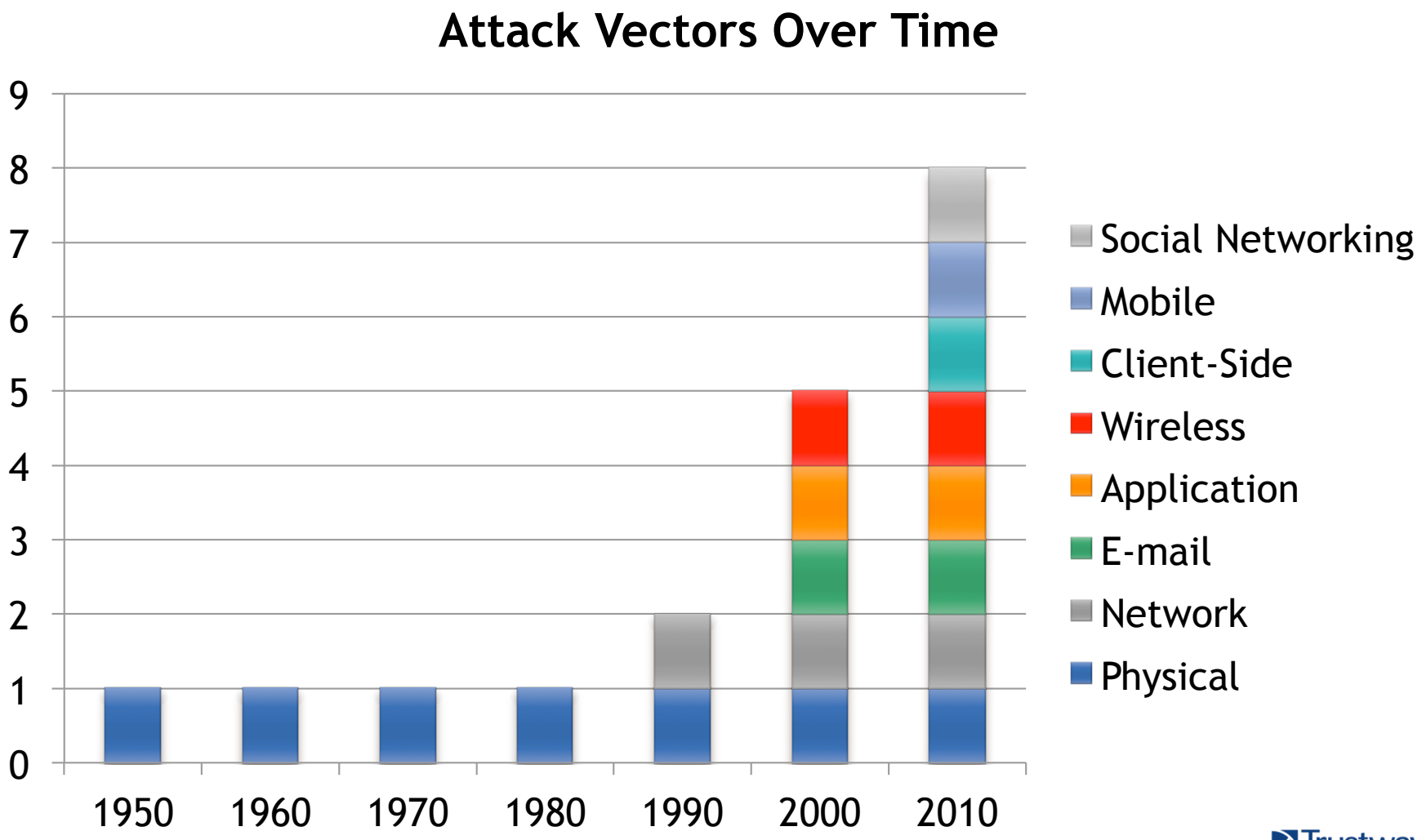


Malware Statistics

- **Data Points of Interest:** Anti-Forensics Capability



Attack Vector Evolution



Attack Vector Evolution

- **1980s:** Physical

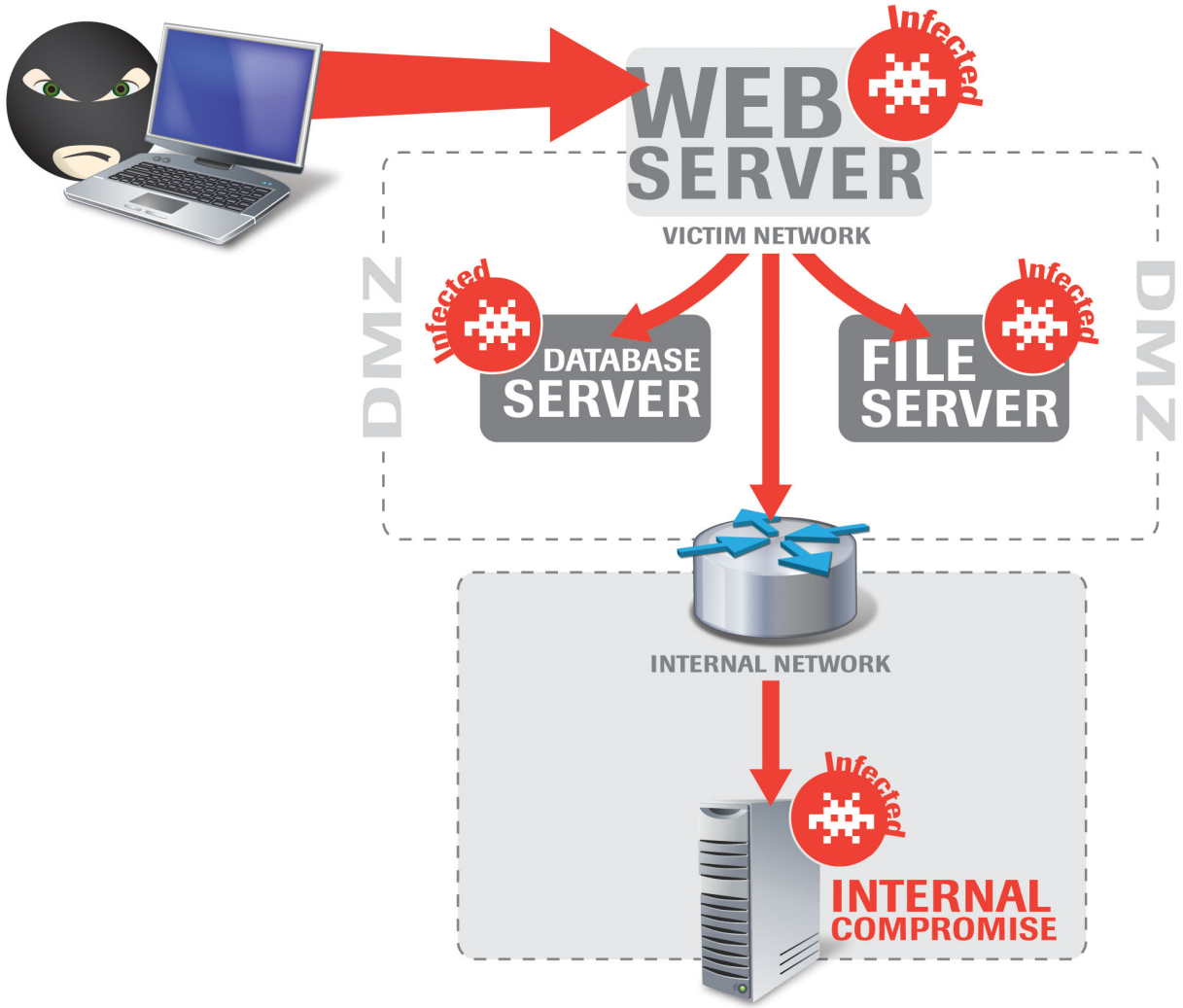
Attack Vector Evolution

- **Physical:** 2010

1. Sensitive Data Left in Plain View
2. Unlocked Accessible Computer Systems
3. Data Cabling Accessible from Public Areas

Attack Vector Evolution

- **1990s:** Network



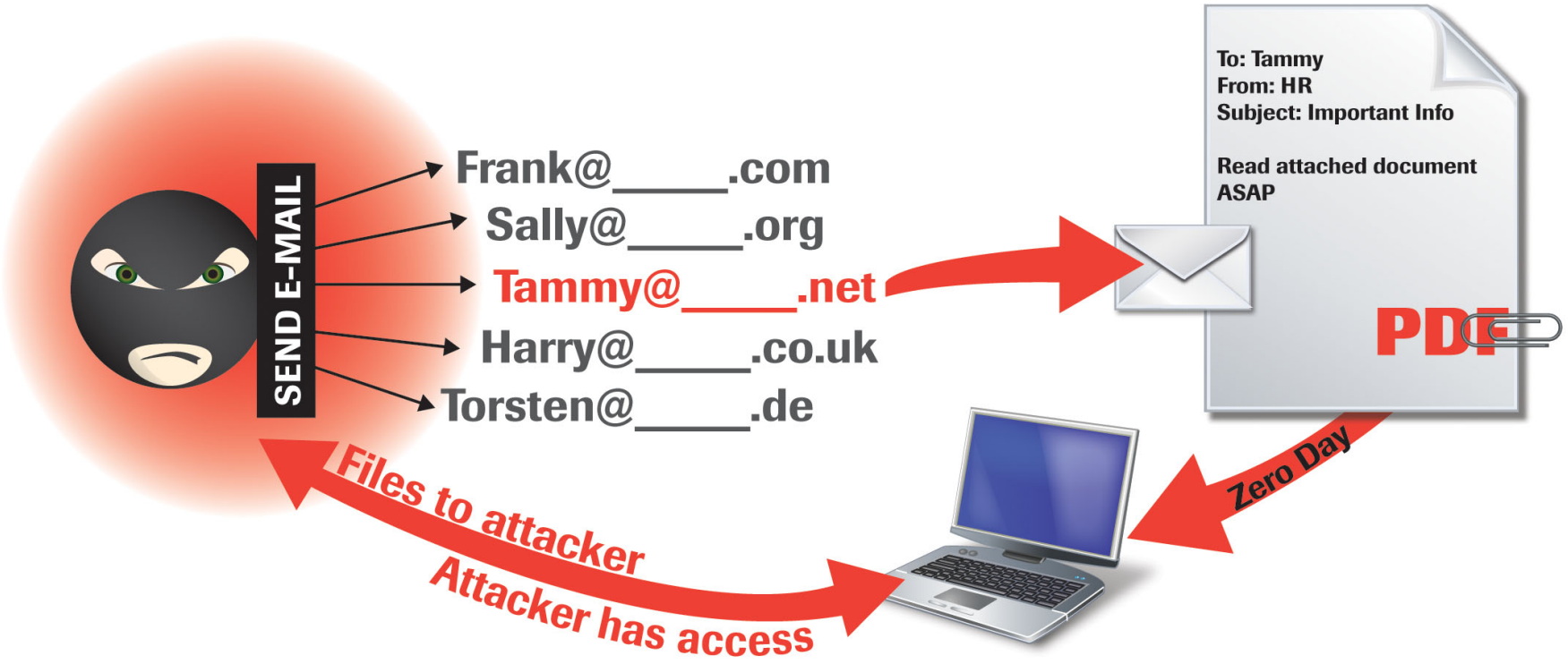
Attack Vector Evolution

- **Network:** 2010

1. Weak or Blank Administrator Passwords
2. Database Servers Accessible
3. ARP Cache Poisoning

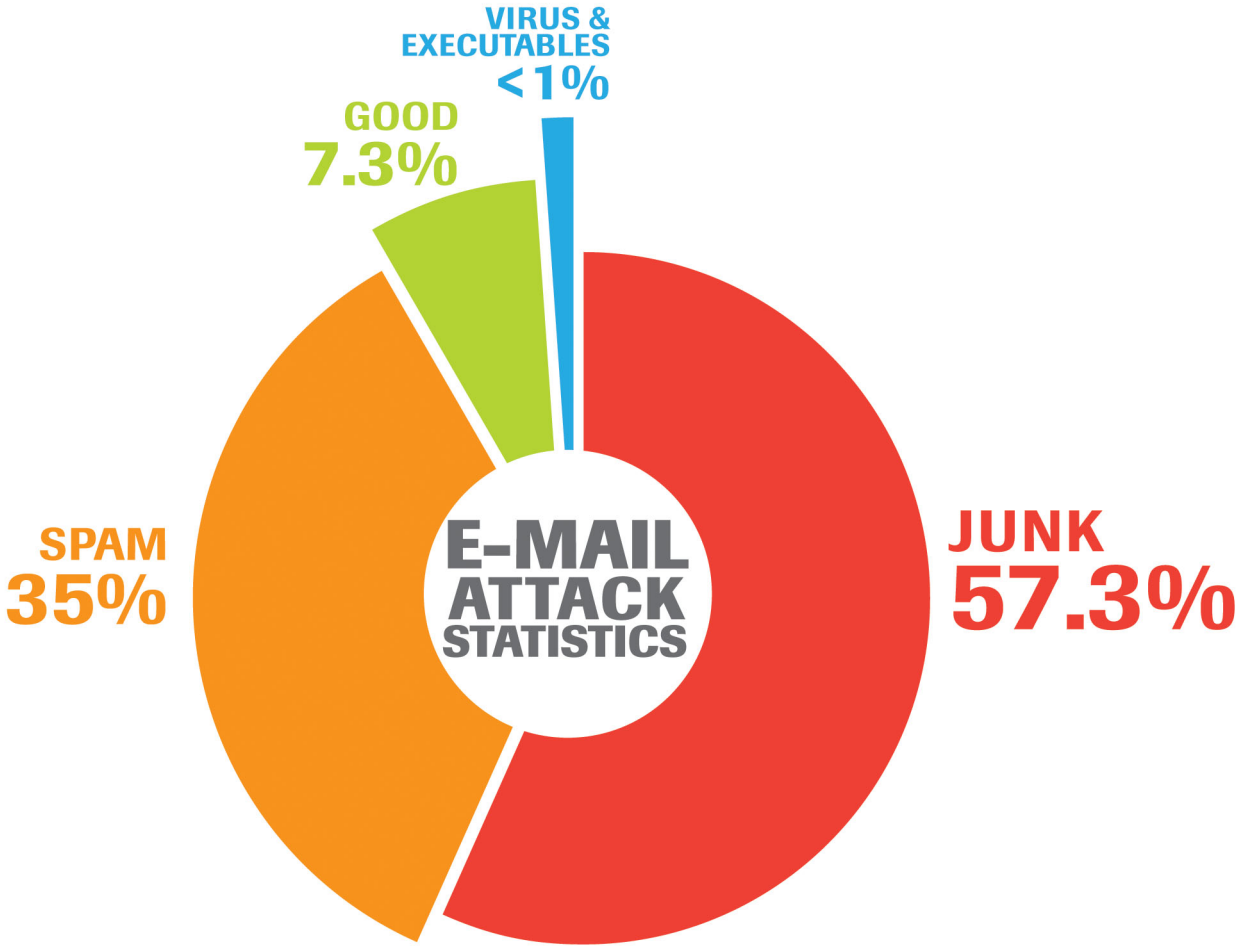
Attack Vector Evolution

- **2000s:** Email



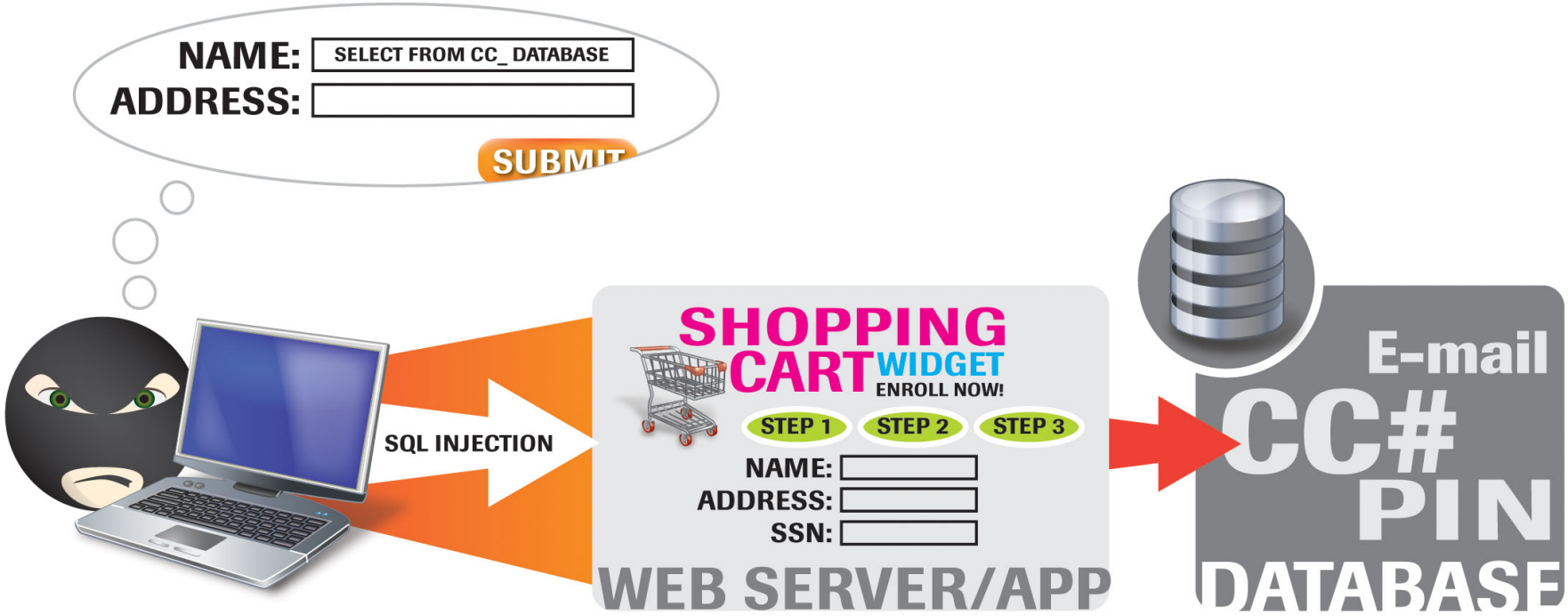
Attack Vector Evolution

- **Email:** 2010



Attack Vector Evolution

- **2000s:** Application



Attack Vector Evolution

- **Application:** 2010

1. SQL Injection
2. Logic Flaws
3. Authorization Bypass

Attack Vector Evolution

- **2000s:** Wireless

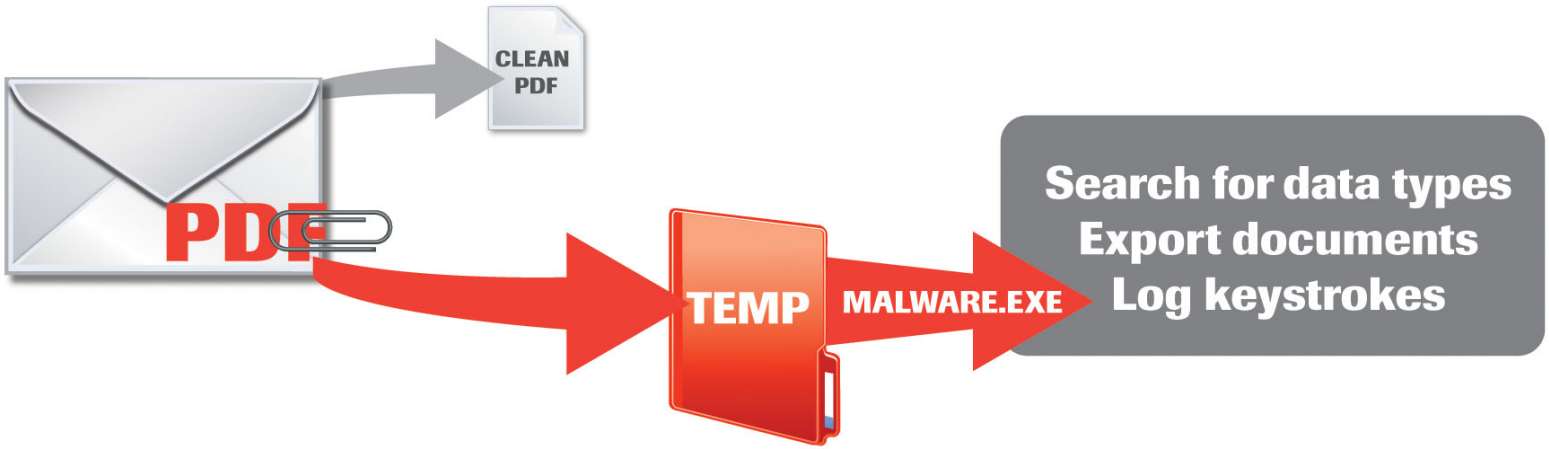
Attack Vector Evolution

- **Wireless:** 2010

1. Wireless Enabled while on Wired Network
2. Wireless Clients Associate w/ “Known” Networks
3. Easily Guessed WPA/WPA2 Pre-Shared Key

Attack Vector Evolution

- **2010s:** Client-Side



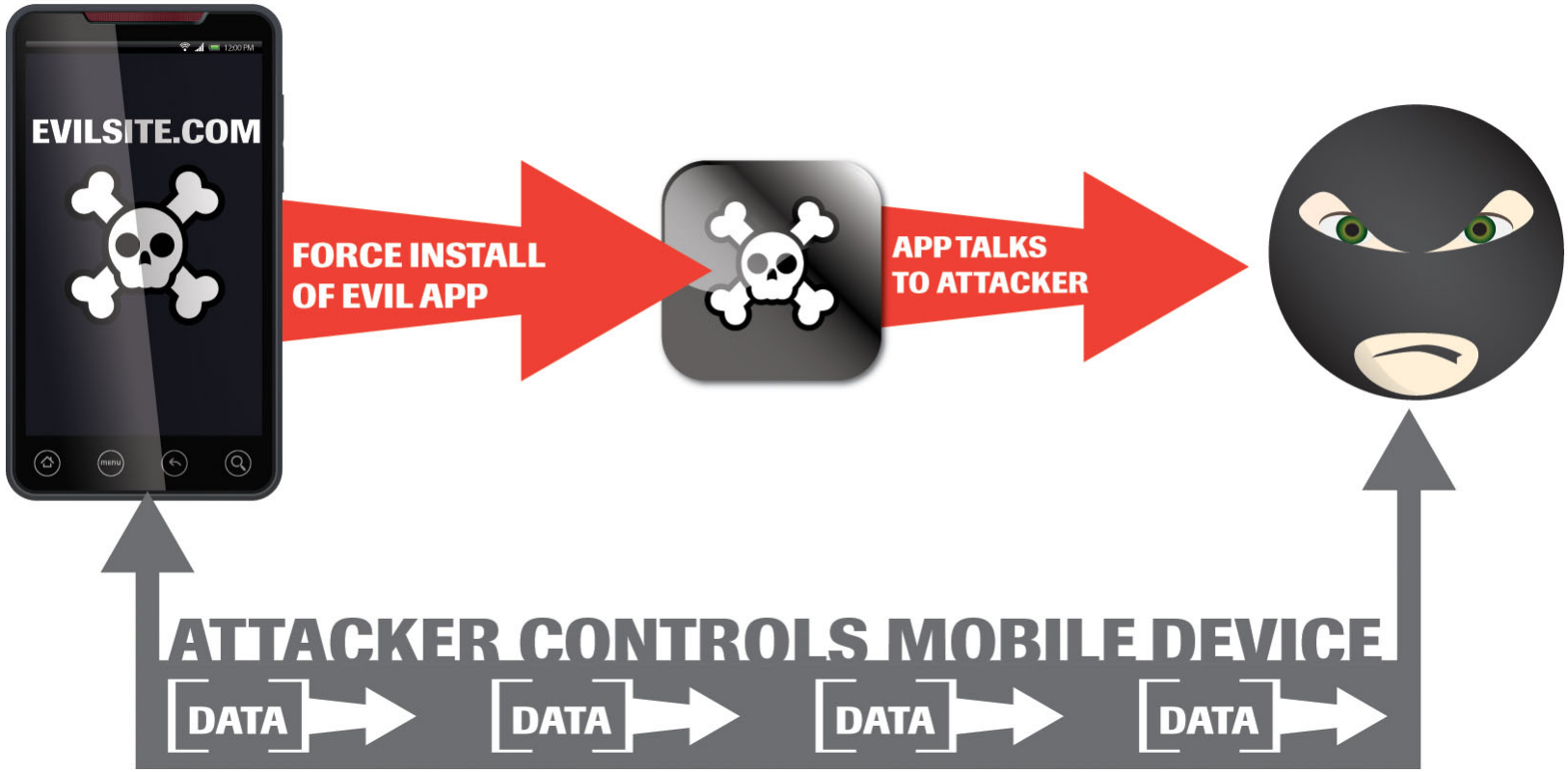
Attack Vector Evolution

- **Client Side (Malware)**

1. Targeted Attack
2. Drive-by Infection
3. Manual Installation

Attack Vector Evolution

- **2010s:** Mobile



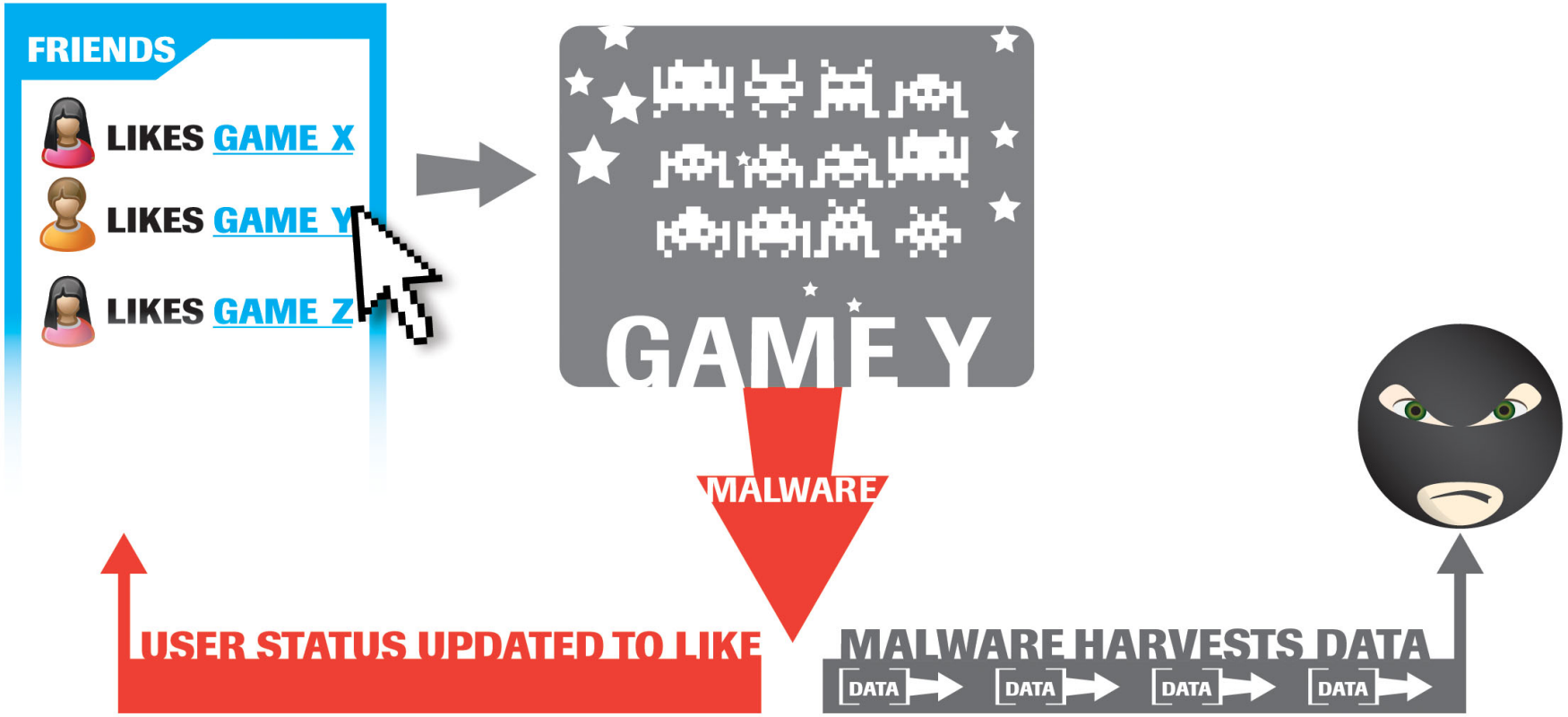
Attack Vector Evolution

- **Mobile:**

1. Mobile Phishing Attacks
2. Mobile Ransomware
3. Fake Firmware and Jailbreaks

Attack Vector Evolution

- **2010s:** Social Networking



Attack Vector Evolution

- **Social Networking**

1. Malware Propagation

2. Personal Information Exposure

3. Data Mining

Strategic Initiatives

1. Assess, Reduce and Monitor Client-side Attack Surface
2. Embrace Social Networking, but Educate Staff
3. Develop a Mobile Security Program
4. Use Multifactor Authentication
5. Eradicate Clear-text Traffic
6. Virtually Patch Web Applications Until Fixed
7. Empower Incident Response Teams
8. Enforce Security Upon Third Party Relationships
9. Implement Network Access Control
10. Analyze All Events
11. Implement an Organization-wide Security Awareness Program

Global Conclusions

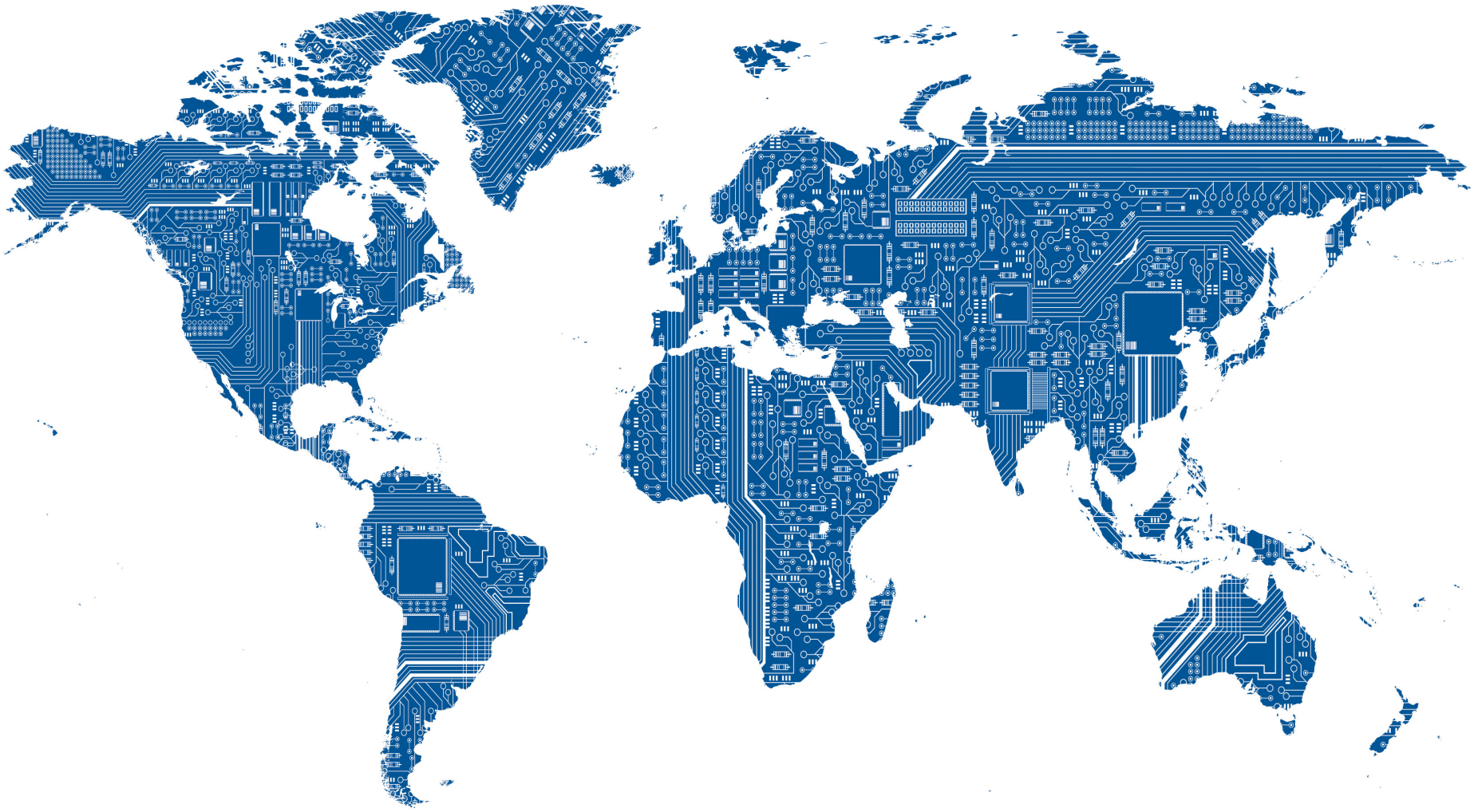
In 2010, the security landscape changed:

- Targets shifted towards endpoints and users
- Individuals became easily identifiable to attackers
- Malicious tools became more sophisticated
- New attack vectors introduced as we innovate; old vectors never die

In 2011, organizations that are firmly committed to security will be:

- Resilient to attack
- Reduce risk of data compromise
- Protect sensitive data and reputation

Questions?



Trustwave®

Contact Us

+1 312 873-7500
GSR2011@trustwave.com
https://www.trustwave.com/spiderlabs
Twitter: @SpiderLabs / @Trustwave