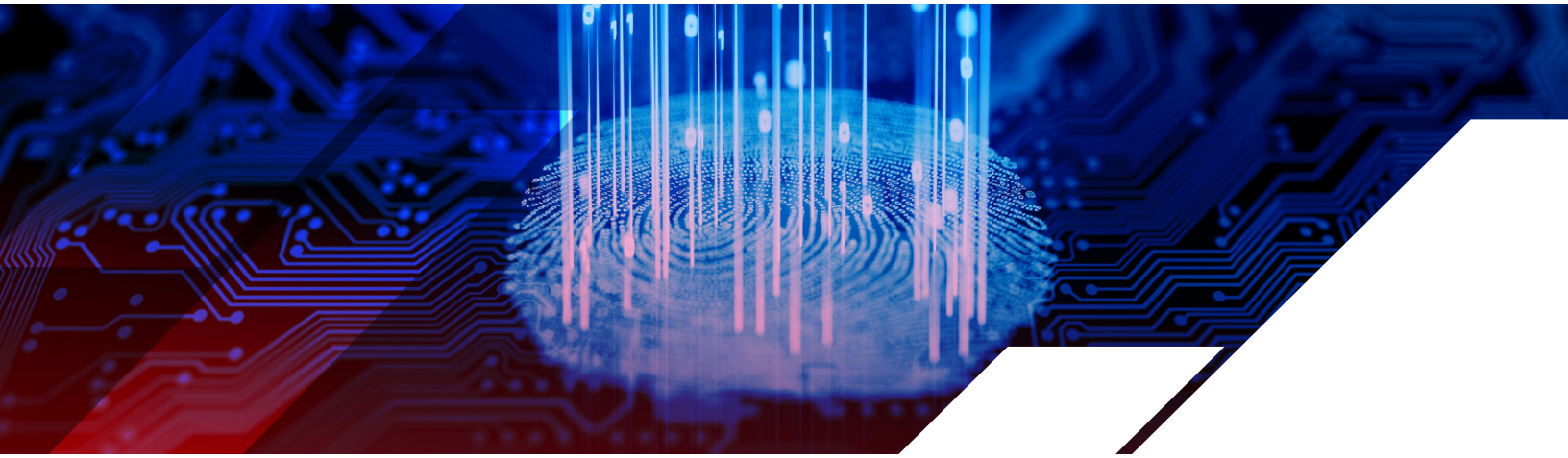

Radware Client-Side Protection

While enterprises do their best to protect customers' personal data on their application environments, the information end-users enter on their client side (for example, ID numbers, address, credit card number, contact information and so on) can be exposed to third-party services embedded in the applications—which are automatically trusted by the main application, but rarely monitored. An average application runs **dozens of different third-party JavaScript services** (Outbrain, Google Analytics, Tranzila and so on) that are loaded when the user first visits a page.

These services, often referred to as the application supply chain, sometimes even depend on their own supply chain made of services from fourth and fifth parties.

Reasons for Activating Client-Side Protection

As server-side security improves, more hackers target the less protected and rarely monitored client side. Client-side protection needs to be activated primarily to handle the following challenges:

- **Increase in Supply-chain Attacks:** There's a rise in attacks (Magecart, skimming, formjacking) through third-party services JavaScript.
- **Lack of Visibility and Control Over Third-Party Services:**
  - Unable to detect if the JS code of services in the supply chain has been breached or tampered with
  - No control of third-party services' security
  - No monitoring of supply chain (sub-services from fourth party, fifth party, etc)
- **PCI DSS 4.0 Compliance (Payment Card Industry Data Security Standard):** New client-side protection measures to be implemented by **all organizations that process credit card payments onlin**e. Best effort: March 31, 2024. Mandatory: March 31, 2025.
- **Compliance and Liability:** As organizations are responsible for the safety of their end-users data and PII, they need to ensure that their customers' privacy is not being jeopardized by any third-party services incorporated into their applications.

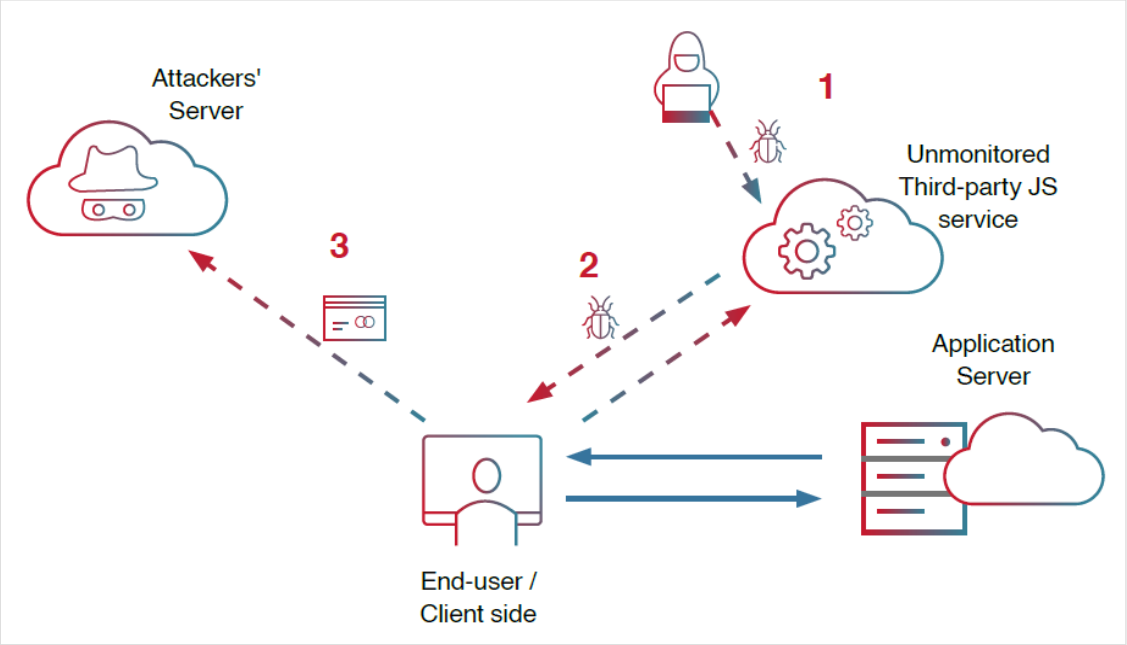

Figure 1:

How Client-side Formjacking/ Magecart/Skimming Attacks Unfold.

1. The attacker hacks a server on the supply chain and hides malicious malware.
2. When an end-user browser sends a form request to the infected server, it returns a response, injecting malicious script into the client's form.
3. The end-user's compromised sensitive personal information is now collected and sent to the attackers' remote server.

Radware Client-Side Protection Solution

As part of Radware's one-stop Cloud Application Protection service that protects the application data center and functionality, this solution offers advanced Client-Side Protection that ensures the protection of end users' data when interacting with any third-party services in the application supply chain.

- **Protect end-users from client-side attacks coming from third-party JS services** (formjacking, skimming/Magecart).
- **Improve visibility.** Discover, map and assess third-party JavaScript-based services embedded in the application.
- **Easily block requests to suspicious third-party services in the supply chain.**
- **Adhere to data security compliance standards (PCI DSS 4.0).**

Advantages of Radware Client-Side Protection

Visibility

- Continuous discovery of all 3rd party services in your supply chain
- Detailed activity tracking
- Alerts & threat level assessment according to multiple indicators including script source and destination domain

Client-Side Attack Protection

- Magecart and various skimming attacks
- Formjacking attacks
- Supply chain exploits

Data Leakage Prevention

- Unknown destinations
- Legitimate destination with illegitimate parameter
- DOM Based XSS

Surgical Enforcement

- Not standing in the way of vital JS services
- Blocking only nefarious scripts

Complete End-To-End Protection

Auto Discovery - > Risk Assessment - > Mitigation

RWI 182 | 01.12.24