Most web applications contain crucial and sensitive data that must be protected. Payment information, personal information, and credentials often reside in the app and are transmitted between servers and end-users. And that’s where bad actors try to step in. Applications and identities are the initial target in 86% of data breaches, with credentials often stolen through man-in-the-middle attacks or client-side flaws, such as malware or key loggers.

DataSafe protects credentials and data from these types of threats with application-level field encryption. Application-level field encryption goes beyond TLS encryption with protection against client-side vulnerabilities. Sensitive data from the user is automatically encrypted in the browser and remains encrypted until it’s decrypted by DataSafe and securely passed to the application.

**F5 DataSafe Features**

- App-level field encryption protects data and credentials as they pass between the user and server.
- Real-time encryption mitigates the risk of compromised data.
- Simple deployments, with no need for coding, end-user clients, or agents on the web server.

**Resources:**

- [Advanced WAF Overview](#)
- [Advanced WAF on F5.com](#)

For more information, please contact your F5 representative or call (888) 88BIGIP.