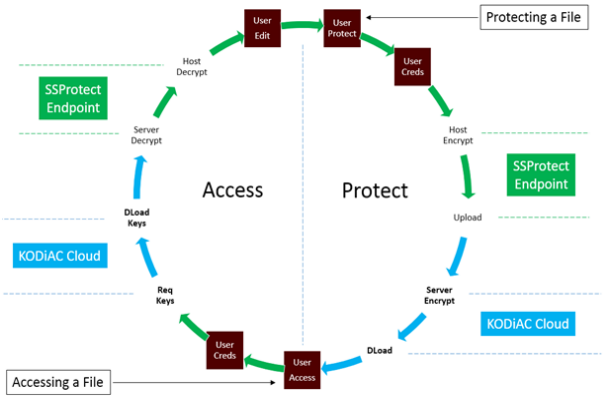
DEFINISEC
DEFINITIVE DATA SECURITY

Simple Security: Protect
Protect. Manage. Respond.

Definitive Data Security is proud to announce **SSProtect**, an integrated suite of software products designed to protect your application data from today's and tomorrow's most advanced threats. Based on the patent-pending **KODiAC Architecture**, each component contributes unique innovations not available anywhere else.

Using a self-service deployment model and native application access, SSProtect greatly reduces data exposure risks without requiring in-house expertise. Simply stated, SSProtect is the rare combination of strong protection with the unexpected ease-of-use not available using traditional security software.



In-Place Encryption: Highly Effective, Non-Intrusive Protection

Real-time Monitoring and Dataflow Management

SSProtect introduces a unique mechanism that monitors and controls sensitive data files, intercepting disk access and acquiring two-factor authentication credentials before decrypting and providing plaintext to the native application. This allows you to work with protected content just as you always have. And because the mechanism works at the driver level, additional access to plaintext is blocked, providing an exclusive session for your application. This combination of low-level security and high-level native application access mitigates host impersonation threats without changing how you work.

Two-factor authentication at the touch of a button

Two-factor authentication is often applied incorrectly, and attackers wait for users to login before stealing unlocked materials. SSProtect minimizes exposure by integrating on-demand two-factor authentication to each file using a touch-sensitive USB token. This provides granular data protection from attacks with stolen credentials without sacrificing ease of use.

2-Party Consent Trust Model: The Final Word in Authorizing Access

Isolated Cryptographic Operations and Keys

SSProtect distributes cryptographic materials required to decrypt files, only combining them when you provide authorized credentials. By that time, data flows have been locked down and content strictly isolated to authorized applications and user access. Our patent-pending cryptographic offloading solution insures that data re-encryption retains key isolation, enforcing access controls and data obfuscation without exposing sensitive materials on potentially compromised hosts.

Stop Government Subpoena and Eavesdropping

KODiAC implements a two-party consent trust model between you and your service provider. Protections follow data, and only you decide who can access protected content, at all times. Plaintext information is truly 100% isolated from cloud services - both you and the cloud service provider retain components required to access plaintext data, independently. Only when both agree to combine decryption materials will you and your peers gain access. One-sided compromise is not enough, which means government subpoena of cryptographic material or even a breach of cloud resources will never recover plaintext data. You always retain final say, and thus have perfect insight into who accesses protected data, when, and how.

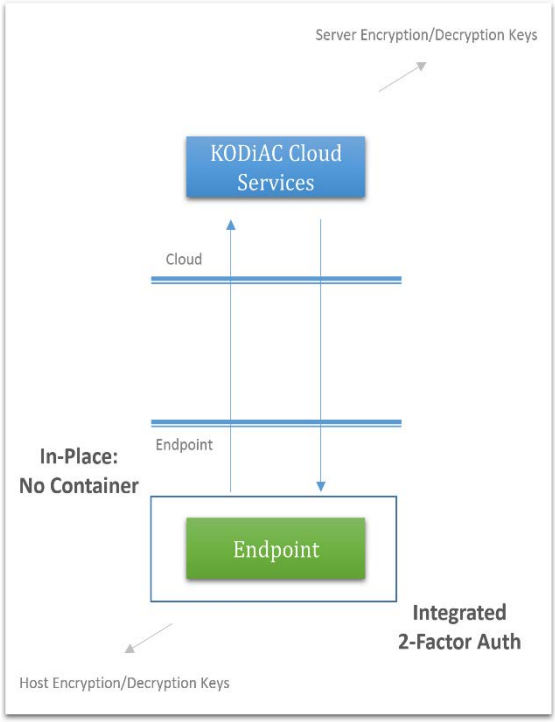
DEFINISEC
DEFINITIVE DATA SECURITY

Simple Security: Protect
Protect. Manage. Respond.

Secure Access Auditing: On-Demand Data Exposure Risk Reporting

Retain Deterministic Access Records

Because KODiAC Cloud Services provide a central control point for the distribution of decryption materials to authorized users, they are able to retain a complete, isolated, secure record of data access events. Coupled with SSProtect client authorization, this provides total visibility into who, when, from where, what, and how sensitive content is accessed. When used with proper chain of custody proceedings, data retains forensic viability. SSProtect provides priceless insight into events leading up to and including unauthorized access attempts that otherwise can cost 10s if not 100s of thousands of dollars to discover.



Immediate Insight into Breach Exposure

It is implausible to speak of a perfectly secure network of information. As security events occur, insight into data access and exposure of sensitive materials to malicious dynamics provides a critical understanding of how to best respond. With SSProtect Data Access Reporting, you can immediately, at any time, generate a report of all access events for a preselected period of time.

This provides instant insight into items that have been accessed during breach events. Determine immediately if certain information has been put at risk. Decide on the spot how to take your next best steps. No more teams of investigators taking over your network for weeks at a time to provide a, "Maybe" – with SSProtect, you have the answers any time, all the time.

Ransomware: The Next Great Threat

Inline, Integrated Version-based Backup and Restore with Honeypots

SSProtect:Recover allows you to store individual versions of protected content for recall at any time. This uses the same mechanism designed for data protections, thus recovery is nearly guaranteed. If you or any member of your team is the victim of Ransomware, because your information is encrypted, you will not be the subject of embarrassing public disclosure. At the same time, you can erase the sabotaged components and replace their encrypted copies with the latest genuinely secured version from your SSProtect archive. And now with Honeypots – essentially hidden electronic landmines attackers will not recognize – you cast a wide net and receive warnings for additional anomalous behavior that slips past other controls.

Disaster Recovery with :xRecovery Organization Archive Retrieval

Network Administrators need visibility across multiple systems and protection from internal sabotage. Access a copy of your entire Organization's data archive at any time with a secure offline copy. Never again worry about a disgruntled employee destroying data – you have constant access to stored, secured content that cannot be erased by any Organization user. This provides complete Disaster Recovery for any scenario. With our network of Data Centers and multiple layers of multi-node replication, you will always be able to acquire your information, even if an entire region of the continental US is unavailable.

DEFINISEC
DEFINITIVE DATA SECURITY

Simple Security: Protect
Protect. Manage. Respond.

Seamless Collaboration, Internally and Externally

Automatic Data Sharing Minimizes Impact

Secure data sharing often requires that you choose for whom encrypted data is to be shared when you save it. Why? Because behind the scenes, that's how public/private key pairs and certificates and symmetric cryptography works. Great for engineers, but not helpful for the rest of us. At DefiniSec, we hide the details from you and provide instant, automatic secure data sharing for all members of a single team or Organization. Deploy to any number of Users and share data just like you would with normal application files – content remains protected and accessible to teammates, but not to intruders.

Third Party Trusts for External Collaboration

Data can be shared outside the Organization by authorizing a Third Party Trust. This is a one-way association that permits you to extend access permissions to SSProtect users outside your organization. You retain complete control – secured access, auditing, backup and restore – while allowing individuals in other companies to access your data. They in turn can authorize you to access their content, creating a seamless two-way trust. Revoke at any time or extend to others – while continuing to use your favorite cloud sharing platform, thumb drives, or email – it's up to you and your IT department. We just protect it.

Protect Against 0-Days: Secure Code Built from Scratch

No Use of High-Risk Libraries

SSProtect was built from scratch, and does not use common libraries. No SSL, thus no OpenSSL. It seems every month a new critical issue is found that likely has been exploited by nation-state operators for quite some time. With SSProtect, these 0-day threats are not an issue because they are present in libraries that we don't use. The NSA in 2013 spent over $25M for 0-day threats, meaning they can more than likely compromise most any popular platform. And because these critical vulnerabilities require constant patching, SSProtect retains a high degree of protection, even if you can't apply patches immediately.

Minimal Cloud Attack Surface Without REST, Without Webservers

Webservers provide a great deal of functionality, but are ever-changing and difficult to secure. SSProtect and KODiAC do not use web services, thus do not have the burden associated with constantly chasing patches. No Flash, No Java, No SSL. KODiAC also avoids the use of at-risk REST API tokens, which though popular are not secure on compromised hosts. This risks access to sensitive cloud content, which we avoid. In fact, the SSProtect attack surface is limited to a single protocol on a single TCP/IP port replicated for high-availability. That's it – nothing further, nothing fancy. Simple. Easy. Secure.

Protect. Manage. Respond: Bringing Certainty to an Uncertain World

Available On	Microsoft Windows 7, Windows 8/8.1, Windows 10, Windows Server 2008, Windows Server 2012
Email Protection	Microsoft Outlook 2010, 2013, 2016
Cryptography	Microsoft CNG w/ AES-128, Elliptic Curve Diffie-Hellman, PBKDF2, RSA-4096, SHA-512
Footprint	< 2.5MB SSProtect Application and Driver, < 2.5MB for Product Documentation

General Information info@definisec.com
For Career Opportunities: careers@definisec.com
For Support: support@definisec.com

DefiniSec operates in the San Francisco Bay Area and offers solutions for companies operating in the United States. Inquire within for International commerce.