OSD Foreign Comparative Test – Product Template

Date: 03/09/2020

Product: Circles of Trust

Company Name: CryptoMill Cybersecurity Solutions
Country: Canada
Point of Contact: Nandini Jolly
Phone: (416) 837-9332
Website: www.cryptomill.com
Email: njolly@cryptomill.com

Short Description:

The Circles of Trust model is a zero-trust approach to data security focused on addressing today's cyber threats from external hacks, nation state driven or otherwise, internal unauthorized data leaks, accidental or malicious, as well as attacks on third parties or supply chain as a result of lingering data access (ex-employee/contractor). Circles ensures protection of all unstructured data at rest, in transit, in use and when shared externally, with dynamic controls. The default state of files protected by a Circle is encrypted and unreadable to any and all non-Circle members.

Circles of Trust security suite ensures a data-first approach to protecting sensitive information, implementing security & privacy using a unique model based on "Circles", with access on need-to-know basis and enforced using encryption. The Circle model extends beyond the organization's users and PCs, providing "cross-border" secure sharing. Security travels with the data and all digital assets stay protected on endpoints, mobile devices and when in the cloud. You can share and collaborate sensitive data securely with anyone, via any means and for as long as you need. Circles also has built in revocation to take access back and extensive logging with built in alerts for un-authorized activities.

Circles of Trust will augment US technological edge in cyberspace, addressing today's attack vectors, improving work efficiency, providing cost savings via automation and bringing robust data-centric security to all sensitive data pertaining to the US armed forces. This with the goal of maintaining mission readiness.

Technology Readiness Level (fielded, lab tested, operational test): TRL7

Countries using this product: Canada, USA, France, South Africa, India, Italy

Application: (the so what?) Circles of Trust is focused on addressing today's cyber threat from external hacks (DISA, Lifelabs, Deloitte), Nation state or otherwise, internal unauthorized data leaks (Raytheon, Desjardins, Capital One, RCMP) accidental or malicious, as well as attacks on third party/supply chain (Visser, Bird Construction/Airbus).

Science (how it works): CryptoMill's data-centric security solution, Circles of Trust (CoT), protects data across the entire organization and when shared with other organizations. An on premise solution, it provides the organization complete control over sensitive information.

This solution is unique in that it secures data within a Community of Interest, or "need to know" group, which we call a "Circle of Trust". Using Circles to protect data eliminates the risks associated with data breaches from a hacker attack on document storage servers/email servers (hosted on premise or in the cloud), network shares, and cloud storage. Circles of Trust also prevents data leaks from lost or stolen devices, and curtails leaks by internal rogue activities.

OSD Foreign Comparative Test – Product Template

With the Circles of Trust model, once the data is protected, it always stays encrypted. Whether it resides in storage, in use or being shared outside the networks, the default state is that files are encrypted, and completely unusable by anyone who is not a Circle member. With Circles' dynamic membership, users can be added to or removed from Circles, with no need to re- publish or redistribute protected assets. Easy to deploy and administer, Circles' centralized policy management and a comprehensive set of tools for automation enables agencies to streamline processes and enforce robust protection. Reduced complexity of data management is combines with greatly reduced costs associated with administration.

Furthermore, integrating into your environment is easy because Circles technology is independent of applications and data formats, and interoperable across different domains and IT jurisdictions, throughout the US government, and globally. Circles can also be integrated into hardware to protect data – for example in a drone or any UAV.

Some Key Points:

- Circle of Trust is primarily a security solution, as opposed to a collaboration tool for file sharing. As a security overlay, however, Circles is the perfect way to provide protection to the documents and files that you share with other departments and external parties.
- The Circles Solution is on-prem. This means that no files or cryptographic keys are stored in CryptoMill's cloud servers. Access to documents and files remain strictly under your organization's control.
- Circles of Trust is streamlined and requires very few IT touch points. Automation is available (for example, integration with Microsoft Active Directory), but also the solution enables authorized end-users to create and manage their own Circles on their own, quickly and conveniently, without the need of IT intervention.

Data (key tested performance metrics):

Circles of Trust uses AES

Intel Core i7 Software Only	Encrypt (MB/sec)	Decrypt (MB/Sec)
AES-128	1,590	1,414
AES-256	1,170	1,080

OSD Foreign Comparative Test – Product Template

AES Hardware Support in Modern CPUs

Intel Core i7 with AES-NI	Encrypt (MB/sec)	Decrypt (MB/Sec)
AES-128	8,262	12,206
AES-256	6,853	9,984

Encrypting Existing Assets in the Clear

Sample Asset	FileSize (in GB)	Encrypt Time (sec)	Encrypt Rate (MB/sec)	CPU Usage (%)
Large Data File – HD	5.7	47	123.3	2
Large Data File - SSD	5.7	13	445.8	5
Very Large Data File - HD	295.3	6431	47	2
Very Large Data File - SSD	295.3	1314	230.1	5

U.S. Partners:

Previous work with DoD:
No work with The United States Department of Defense yet.