CyberProof

January 6, 2019

CyberProof Hybrid Architecture

A Whitepaper

Table of Contents

Preface

The CyberProof Defense Center (CDC) orchestration platform was designed as a "pure" cloud solution.

The philosophy behind the CyberProof Defense Center platform architecture is aligned with the global trend of migrating components of the IT infrastructure and software services onto the public cloud paradigm. As the cyber orchestration model is intelligence-driven and thus highly connected to both internal and external security elements, a cloud-based platform is optimally positioned to service the operational processes of cyber defense.

However, several factors impact this pure cloud model. The main issues that hamper adoption of our model include:

- Regulatory limitations on moving data off-site or outside sovereign borders.
- Market demand for tight enterprise control of cloud migration in the form of private cloud solutions.
- Yet-to-be-stabilized security controls for cloud platforms that will move them on par with on-premises security postures.

As a result, CyberProof developed a hybrid architecture that can address these issues, providing a solution that includes most of the CDC's cutting-edge functionality for CyberProof's clients, while adhering to limitations required by the current market demand, especially in the regulated verticals.

This white paper describes the key design considerations, solution implementation and impact on the core functionality of the CDC platform. It also lays out where we see the boundary of this solution, i.e., where we will explicitly refrain from extending the architecture due to technical considerations.

The CyberProof Defense Center Architecture

The CDC is an orchestration framework that encompasses the traditional capabilities and layouts of a SOC while changing the entire scope into a team or community "shared effort" paradigm.

The general framework contains video wall support, dashboards and view concentrators, as well as a host of analytic tools and flexible screen customizations facilitating the professional tiers working around the SOC center.

At the heart of the CDC incident framework resides the ChatOps module, supporting team interaction, information transparency and near real-time input streams from both external sources and the CDC's expert tiers and AI bots. The ChatOps framework creates an ideal environment for running combined operations with multiple stakeholders and complex response scenarios.

In addition to the classical SOC posture, the CDC is enhanced by SeeMo, a set of autonomous and semi-autonomous AI bots that roam different ranges of the solution, assess data events and notification streams, and generate insights, events and elevated alerts to the SOC team.

The CDC resides in either Microsoft Azure or Amazon AWS. At its edges, the CDC deploys a rich and rapidly expanding set of adapters, not just for SIEM platforms but also for individual interfaces for security and infrastructure boxes.

The edge components of the CDC can reside either in a cloud installation or on top of an on premises SIEM and connector implementation. SeeMo (the AI bot family) can run wherever needed, ensuring data access for supported data landscapes and processing tasks.

The CDC is fully integrated with Azure's application management module, using it as a repository for quick deployment, updates and provisioning. All components run on preconfigured Dockers and load management and scaling is performed automatically with administrative oversight.

The CDC is currently deployed over Azure and Amazon in four regions, and can be deployed over additional regions as the platform scales. The CDC has an internal administration mechanism to control all the regional instances from the central hub in Tel Aviv, and to ensure all functional upgrades and configuration changes percolate across the entire set of deployments.

The CDC is an advanced security services platform and is designed to support multi-tenancy and enforce data privacy and separation between instances. Each customer is allocated a dedicated instance running on the center closest to its center of business. Franchise partners are allocated a segment of the resources of the nearest CDC, but customer separation is enforced in a similar manner.

Key Requirements for a Hybrid Architecture

The CDC doesn't normally access the original customer's data, but rather the events logs and activity journals generated by the functional IT boxes and the security applications. The CDC only sees and utilizes the kind of data normally acquired by a SIEM, even in cases where direct connectivity to security or infrastructure servers is required. Thus, the exposure level and risk of the CDC leaking or taking data out of the customer's domain (or sovereign borders) is slight.

The CDC is an integrated SOC and SOAR orchestration platform. It provides notifications and alerts to the teams staffing the SOC centers and supports their incident handling procedures by pulling in all pertinent data from the attached data sources (SIEMs or other sources directly connected) and generated by the SeeMo routines. These items and indications are displayed on the ChatOps environment – the core collaboration mechanism of the CDC.

Our engineering team designed the hybrid model to ensure that no customer data in the local MongoDB repository is moved or stored anywhere on the cloud infrastructure. All utilization during playbook execution is done by remote access and any analytic logic runs locally on the MongoDB machine, on premises.

All the ChatOps data, the SeeMo notifications and alerts, the customer's configuration and descriptive information and any other data items describing its CDC instance are stored and managed in a local instance of MongoDB. Each customer is allocated a dedicated installation of this DB and it is only accessible from the instance serving it on the CDC.

All other software components of the CDC platform are essentially using a remote-access motif to access this central repository, and do not store any data anywhere else on the CDC. Once an instance is rebooted, all memory copies of the data are scrubbed.

SeeMo is the only component that roams freely across the CDC. But all instances of the bot only use numerical indications (or enumerations from the MongoDB tables) to execute its logic. Thus, it has access to raw data but doesn't use it while executing its logic, not even in its semi-permanent memory support tables.

The Hybrid Solution Model

The CDC hybrid model relocates the MongoDB instance to the customer's premises and opens up a dedicated VPN channel for all access from the main CDC instance. The MongoDB can be installed on a dedicated machine, a virtual machine or reside next to a local SIEM installation, based on customer requirements.

The MongoDB instance is configured for full isolation, with administrative rights reserved for the CDC administrators, though an oversight account can be created

for the customer's administrators. Administrative login to the MongoDB machine uses strong authentication, and the machine is connected with a dedicated adapter directly to the CDC as part of the security self-monitoring scheme employed by the CDC.

The MongoDB uses a local disk-based backup schema, using a separate hardware configuration. Any outage recovery will be performed on the local machine, or utilize the backup hardware to re-configure a cold-standby server as replacement.

Any instance of SeeMo that requires access to MongoDB tables for executing its machine language logic will execute locally on the MongoDB server and only report its findings back to the CDC platform. Any SeeMo bot running on the CDC platform does not utilize numerical representations or enumerations to execute its logic and does not retain any raw data – even in memory.

Administration of the MongoDB instance, normally performed by automated Docker pod generation on Azure, will be performed manually during installation and configuration of the local instance of the DB. Ongoing monitoring, updates and maintenance of the entire set of applications running on the local server is done from the CDC platform using automation routines, taking care not to move any of the local data outside the customer's domain.

Impact on the CDC Chatbots

Our initial model used to assess the impact of the hybrid configuration on the central Chatbots package shows no degradation or detrimental impact on the core functionality of the platform. Provided that the VPN connection has enough bandwidth, there are no issues with performance or responsivity of the platform, and no major rewrites needed to retain functionality in the hybrid mode.

Impact on SeeMo and the CDC Analytics

SeeMo comprises a family of automatic and autonomous AI agents that perform several tasks in various parts of the CDC. All SeeMo bots are independent of any cloud infrastructure and can be moved to run on the local machine of the hybrid design, if required. The SeeMo bot family will continue to expand, while ensuring that all bots that may need access to the MongoDB instance of a hybrid architecture will execute locally and not on the cloud.

Hybrid Evolution and boundary

CyberProof regards the hybrid version of the CDC as a strategic move to accommodate a significant percentage of customers that work in regulated verticals such as finance, insurance, healthcare, pharmaceuticals and some critical infrastructure areas.

We understand the need for a private-cloud motif to adhere to both regulatory and business demands to retain control of all source data either within the customer's domain boundaries or within the sovereign borders of the country where the customer is registered.

In cases where data must be retained within a sovereign border, we can comply by ensuring the data never leaves a local installation of a cloud platform such as Azure or Amazon. In some cases, a custom port of the instance running on a local cloud provider will be provided as a custom engagement.

When no solution exists on a cloud platform, the hybrid model comes into play, by forcing all relevant users' originated data – even if it's only log records – to remain within the customer's domain.

This solution vector cannot be expanded into a full, on-premises version of our CDC platform. We are committed to the migration to cloud as a strategy, and regard the full rewrite it will necessitate to run a local version of the entire CDC as counter-productive and flying in the face of the current trend.

We believe that most customers realize the benefits of a security operations platform hosted in the cloud – a platform that offers easy access to all external threat and vulnerability intelligence sources, and a fast-evolving platform that percolates all knowledge from incident handling anywhere on the platform for the benefit of all registered customers.

Outside some national security agencies and sensitive data businesses that maintain an air-gapped IT environment by default, we believe that most of the commercial customers can adhere to regulatory demands and management concerns with the hybrid solution described in this paper.

Once implemented, the hybrid version will be integrated into the main CDC product tree and enjoy the same advantages of SW development and capability enhancements as the main, "pure cloud" platform.

Summary

CyberProof's hybrid CDC solution caters to all customers that require (and verify during audit) continuous control over any form of data generated in their production environment. We will certify the hybrid solution for industry compliance wherever applicable.

About CyberProof

CyberProof is a security services company that helps companies increase cyber resiliency. We reduce risk by managing and operating a newly architected Security Operation Center (SOC) that dramatically reduces costs while increasing the ability to rapidly react, detect and respond to cyber-attacks. We provide pioneering services that utilize new technologies, machine learning and fuse diverse sources of intelligence together to keep your organization safe from cyber threats.

CyberProof was recently ranked Leader in the Forrester Wave™ Report: Emerging MSSPs Q3 2018, validating our disruptive approach to cyber security services.

For more details, visit our website at www.cyberproof.com.