CNAM Case Study

Summary

Data centers are not just a place where one can store enormous data but there are many more things involved. The retrieval of this data that is stored in these high performance servers needs to be fast easily available. Moreover, everything that is stored requires redundancy that will make enable data recovery in case of any loss. Above all this, data centers need a very strong security as it stores confidential data.

Today, in the business world, increased expenses into R& D and Marketing has made it obligatory for companies to think of cost effective solutions, reason why companies are now open to outsource and use cloud storage for their data storage instead of acquiring their own Data servers.

Our client is a data center service provider that helps companies with their storage needs. Every customer they have not only required Data storage but they asked for a solution that can keep their data safe.

This is where we came into picture and assured our customer that we have the right solution that can give confidence to their clients about the security needs of their mission critical data. We provided them with a real time threat management solution that ran automatic procedures to keep track of attacks as well as resolve them from time to time. Moreover, it also has a built in application to track latest threat trends and their probability of affecting the systems. A proactive measure taken by company could reduce likelihood of data loss or corruption.

Another advantage that our clients had with our solution was - our pay-as-you-go payment model that we have designed as per the market need of cost effective solutions. We provide automatic data security measures, real time threat management and monitoring, and a value for money proposition.

Understanding the benefits, our client clubbed our solution along with their Data storage solution and started to offer their clients a complete solution with storage, monitoring as well as automatic threat management.

Business Challenge

Our client had data centers in major Metros in India. They had been serving clients from various industries including Telecom, Retail, Financial Services and Aviation.

Their infrastructure consisted of clusters of High performance Tier 2 and Tier 3 data centers along with high band width cabling for speedy data retrievals. These data centers were used to store huge amount of confidential data yet the capacity of data centers was not fully utilized and they were expecting more projects in the near future.

In the process of implementation, they had done a lot of investment in data centers, cooling units, power equipments, server farms, operating systems, control applications, and virtualization software's. With incorporation of Cloud computing and virtualization, there was an increased vulnerability to threats like VM attacks, and data stealing.

The company needed a low cost solution that had the capability of researching real time attacks on data so that their client information could be saved from such attacks. Thus, they required high levels of security but the challenge was the cost which company needed to optimize for their requirement.

Operational Facts

Netmonastry analyzed the security requirement of the Data Center and found:

- The data centers hosted mission critical applications and hence required maximum uptime. This made them open to real time continuous attacks. Thus they required to keep a track of such threats from time to time to figure out latest trends of attacks that could help them in taking immediate action.
- Huge racks of data servers were installed but there were only a few engineers deployed for monitoring and managing of the data centers. Thus, they required a security solution that could be automated to perform tasks required for data protection.
- Their complex system and huge number of storage structures needed customization in the security.

Product Deployed- CNAM PRO

Our flagship brand CNAM pro is a real-time threat management suite that provided them the real time threat detection system as they required. Moreover, we had the measuring metrics in place that created lists of latest attacks and trends to create actionable reports for customer from time to time.

To take care of their system processes and ensure best deployment of security measures, we provide them with a customized solution as per their need.

Solution Facts

Our solution - CNAM Pro aimed at solving various security related problems including:

1. There are various kinds of security attacks and violations that keep happening every day, most common are the worms and malwares that keep doing nasty things to computers like password stealing, phishing, leaking your personal information etc. These malwares do not show themselves in the task manager and thus the detection is possible only by a malware detection programs. Our malware detection engine detects these malwares, worms and APT to prevent malicious activities that these programs are capable to do on the machines.
2. Other than these malwares, a very common trend that has come up in past few years is DDOS attacks (Distributed Denial of services) DDOS attack servers by sending multiple connection requests that floods the servers with enormous traffic and thus the links get saturated which stops genuine request from getting attention. This drastically reduces the performance and thus affects the systems. Our traffic anomaly engine allows detection and prevention of such threats. In addition, this engine also takes care of other problems like P2P violations, proxies and Botcoms.

P2P violations: *Corporate work hard to create product documentation that is critical to use in any organizations. Many of these copyrighted files can be shared with others with peer-to-peer file sharing networks. People download P2P programs when they wish to share large files which simplify their work. However, these programs do not check on copyrighting and thus cannot detect illiberal distribution of the material. Thus, it becomes the task of the company to which the files belong, to take preventive measures.*

Botnet attacks: *Botnets do not attack directly but they have the capability to extract personal data from social media and then send genuine looking requests to download the malware, which the receiver takes seriously and download all the malware components*

3. Our managed intrusion detection takes care of the custom attacks that a system or application may face such that the problems could be proactively solved in the real time
4. We also provide threat intelligence system that collates the trends of attacks through multiple devices which reduces the detection time of the latest threats that a system faces
5. Threat detection and removal are essential but it is also required to understand the security posture of systems which includes evaluation and continuous tracking of related information that enables one to understand the needs of the system. Our solution provides this measurement of network security from time to time and generates customized actionable reports that can be worked on to tighten the security.

Benefits

- The highly customized solution enabled better management of their security system
- As the solution was based on pay-as-you-go model, it proved out to be very cost effective for them
- The automated threat management system reduced their efforts and monitoring time.
- We took the responsibility of system accuracy and the client could totally depend on us for their security. They did not need to hire professionals and work hard to take the juice out of the juicer but the solution was readily made available to them.
- Our server monitoring of the system allowed proactive tracking of threats and the resolutions were made before the attacks could harm or steal the data.
- With huge infrastructure scattered into multiple locations, the monitoring of assets was a challenge. Our scalable solution helped them in understanding their asset security posture in a single window. Thus, enabling remote monitoring of all assets.
- Our complete security solution provided a value added offering to their clients and thus creating a competitive edge.