FINANCE

THE FAMILY BUILDING SOCIETY

HOW LOGPOINT IS HELPING THE FAMILY BUILDING SOCIETY RETAIN LOG DATA, PROVIDE EFFICIENT FORENSIC ANALYSIS AND SUPPORT CYBER SECURITY PLUS ACCREDITATION

BACKGROUND

Epsom, Surrey-based Family Building Society provides mortgage products and services designed to enable family members to provide mutual assistance for capital projects while safeguarding their savings. It is very popular with parents who want to help their children get on the housing ladder. The Family Building Society brand was launched by the National Counties Building Society in July 2014.

The Family Building Society provides mortgage products and services designed to enable family members to provide mutual assistance for capital projects while safeguarding their savings.

Within its IT security team, the Family Building Society has traditionally relied on manual systems for log management and analysis. While the manual process was working for known threats, it did not allow Family Building Society to identify and deal with unknown threats to the network effectively. To minimize the time and resource needed for log management and improve responsiveness when action was required, the decision was taken to implement a new solution.

THE CHALLENGE

Family Building Society began by undertaking a holistic review of its IT landscape to understand clearly where the gaps and pain points were in their cybersecurity posture. As part of this review, log retention and log analysis were both identified as priority areas for attention, and topics that were constantly being raised in regular reviews. The Family Building Society also wanted to enable the retention of log data and effective forensic analysis of security and operational events.

FACTS	
Customer	The Family Building Society
Industry	Financial services, Mortgage products and services
Location	Surrey, United Kingdom
Objectives	Retain log data, provide efficient forensic analysis and support Cyber Security Plus Accreditation
Results	• Cuts response time to cyberthreats in half • Provides 70-80% savings on administrators resources spent on log analysis • Is a SIEM solution at a predictable cost

At the same time Family Building Society was going through the process of obtaining the Cyber Security Plus accreditation. To align with the requirements of the programme and address the input received from security assessors, having a Security Incident and Event Management (SIEM) system in place was considered a necessity.

Once Family Building Society had decided to implement a SIEM solution, they then needed to decide whether to deploy it in-house or as a managed service. With a long and successful history of providing internal IT services, the Family Building Society decided to bring the SIEM solution in-house.

They also had to ensure that they had the necessary resources available to manage the system, the support and documentation to help them through the process, and the freedom to move to a managed service in the future if required.

THE SOLUTION

Family Building Society reviewed a number of different SIEM solutions, and Logpoint ticked the boxes in all categories of the requirements. However, before deciding on a solution, the Building Society needed to be sure that that the costs of the solution would stay within budget. Predictability in the cost of deploying and using a SIEM solution is a key parameter, which is why Logpoint employs a different cost model than other vendors.

It's a fact that data will only continue to grow, a fact Logpoint believes customers shouldn't be punished for. Licensing for the Logpoint SIEM solution is based on the number of devices (nodes) sending logs, not on the volume of data (GB) or events per second (EPS). With a Logpoint license, concerns over data limits instantly disappear, allowing customers to scale for future needs predictably.

“The simple cost model that Logpoint has in place enables us to predict the costs of the SIEM solution which was extremely important to us,” said Andrew Ballard, Head of Technical Design & Delivery at Family Building Society. “We agreed that the solution was aligned with what we needed, and with support from Logpoint and Matraxis we proceeded through a successful implementation.”

When the Family Building Society started to deploy Logpoint, they used the predefined use cases set up by Logpoint so they could implement the solution as quickly as possible, maximize full benefit of the platform and achieve the best possible time-to-value.

THE RESULTS

With the deployment of the Logpoint SIEM solution and moving away from manual log analysis, the Family Building Society now has the benefit of automated, real- time analysis of logs as well as optimized access to all log sources for manual inspection, event analysis and log management.

One of the main Logpoint features utilized by the Building Society IT team is the powerful search functionality across all log sources. By normalizing the data upon ingestion, rather than upon search, this has provided the IT team with a very quick and intuitive way to set up notifications and categorize both known and unknown threats:

“The use of a single platform means that we do not need to differentiate between log sources, saving us a lot of time,” adds Andrew Ballard.

Moving forward, Family Building Society is planning to expand their use of Logpoint, particularly its Threat Intelligence application, which sources data from best in-class Logpoint Proof Point and the large collection of indicators from Logpoint Critical Stack.

With these data sources ingested, Logpoint can analyse structured and unstructured data, alerting to a match when a known- bad indicator in collected enterprise data is identified.

“We now think of Logpoint as a member of the IT Security team,” said Andrew Ballard. “It provides immediate answers to a lot of questions that we would have struggled to answer under a more manual system. We can take logs from everywhere that they need to be gathered and collate and analyse as much as we need and the process of ingesting data is very open.”

Family Building Society is also looking at how they can share information collected in Logpoint with non-IT end users within the organization to better streamline operations.

“We now think of Logpoint as a member of the IT Security team.” “It provides immediate answers to a lot of questions that we would have struggled to answer under a more manual system. We can take logs from everywhere that they need to be gathered and collate and analyse as much as we need, and the process of ingesting data is very open.”

Andrew Ballard
Head of Technical Design & Delivery

CONTACT LOGPOINT

If you have any questions or want to learn more about Logpoint and our modern SIEM solution visit www.logpoint.com