HEIMDAL SECURITY

Heimdal Security
Case Study on an Insurance Company

1. What were you trying to improve or change when you were introduced to Heimdal CORP?

We were trying to improve security, and reduce exposure to ransomware, etc. In a customer-facing environment where credit card payments are continuous, and customers are in our premises all day, any downtime is very obvious to the public. A security breach or data loss is unacceptable.

2. How did you find out about Heimdal CORP?

A friend of mine suggested it, after I told him my concerns. He already has it in a business with 300 users. We had already been hit with CryptoWall 3.0 in June 2015. We lost a few hours' work, but the damage was minimized by having useful backups & replication in place. Time was still lost identifying the issue, and rolling back. We lost half a day; it really could've been so much worse.

3. What problem did Heimdal CORP solve for you?

It helped update our client machines, and gave me personally a new comfort level when it came to ransomware protection.

4. What steps did you take to implement Heimdal CORP and how did the entire process unfold?

The first process was justifying the need for it, and the cost of it. The price is not high.

Also, I didn't see the risk of another attack as being low to medium. I felt it was inevitable.
So, after this it was just a case of rolling it out. We use Terminal servers for most of our users, so Heimdal was rolled out using a script to run it in quiet mode.

Heimdal allows the agent to be disguised too, so it's one less icon in the system tray. Running the application takes us less than a minute, and is now part of the standard build if we do roll out PCs.
One of our main challenges is that due to a specific software we use, the users need local admin rights. Needless to say, this causes me a lot of anxiety, and arguments.

The Dashboard for Heimdal management is quite useful, and shows the clients installed (the last time communicated with), the clients with Malware, and the clients with vulnerabilities. Fortunately, this Dashboard is cloud based, so doesn't require space o resources on a server.

5. Could you tell us in your view how Heimdal stopped the ransomware attack?

It was the Zepto ransomware. It occurred on the PC of one of our Senior Management. It looks to have been caused by a link in an email that he clicked on. We currently use very good content-filtering software for both email & internet, but it is not 100% safe.

The person affected actually sits in the same office as me, and would most likely have told me if he knew of an issue. Instead it looks like Zepto was activated and stopped. I only identified the threat after the incident when I noticed some files in his User Drive (mapped to a server) were encrypted with the .Zepto extension. Upon further investigation (I identified the source by the user being named as the creator of the "Help" file in the drive) I located the PC, and saw how the threat had begun and where.
Heimdal stopped the infection & encryption almost immediately, without

even the user being notified or a pop-up demanding the ransom. Only a few insignificant files were encrypted, and we experienced absolutely zero down-time. Customers were not affected, and as mentioned I only found out some time after the incident.

6. What key aspects did Heimdal CORP help you improve or change in your company?

Our client machines are now up to date with software that is often targeted (e.g. Flash, Java), and I can identify if there are any issues on the client side.

When we were affected by CryptoWall 3.0 in 2015 it was through an automatically activated Flash-based advert on a reputable website.

7. If you were to recommend Heimdal CORP to others, what would you tell them?

It is probably the best value security software on the market to prevent modern-day threats. It has stopped ransomware in its tracks while our Anti-Virus didn't even spot it after a post-attack scan.

In 18 months, I have gone from not knowing about Heimdal to having it as the number one tool in my client & sever side security arsenal.

The support we get from both the official Support Team (especially Razvan & Bogdan) and our Account Manager (admittedly this is often silly questions from me) is absolutely second to none, and a yardstick for all my dealings with vendors & suppliers.

I have also noticed that it is a continually evolving software, so it seems plenty of time & effort is being invested in the development of the product.

8. Anything you'd like to add that I haven't asked?

One of the pages on the Dashboard is "Return on Investment", which seems to be based on the number of clients and vulnerabilities identified & patched. What this doesn't do is show the amount of money saved by preventing downtime caused by ransomware. If it did, our ROI would be up to at least €5,000.