A Faddom Case Study

The text is directly from a client's internal communication and was not edited

Table of Contents:

Page 2: Executive summary
Page 3: Solution description
Page 4: Summary of software benefits
Page 7: Other use cases we evaluate
Page 9: Execution timeline
Page 9: Project governance
Executive Summary:

What is the business problem being solved? Why do we need to solve this problem now?

Knowledge is Power. The outcome of Change (Management) should be predictable, not russian roulette.

Over the years IT systems get deployed by IT Infrastructure staff in companies and the same staff frequently leaves the company for various reasons. Documentation, handover and monitoring for internal/external SSL certificates is/was not arranged well at [CLIENT] leading to knowledge gaps and P1 incidents with hefty price tags from third parties to restore the mission critical environment.

Additionally [CLIENT] is running their most sensitive applications (SAP, eDesk, ...) on legacy platforms on a public network range. Two project requests were initiated by the ICT Security & Quality manager to mitigate this risk:

• Upgrade of all Windows Server Systems to Windows 2019 (supported platforms)
• Migration of all Systems/devices from the public 132 range to private [CLIENT] IP ranges

Due to knowledge gaps, lack of confidence and fear of P1 incidents, internal staff is reluctant to proceed with these projects and the IT infrastructure remains on unsupported and vulnerable platforms.

In order to proceed with these project requests an Application Dependency and Discovery Mapping Software solution is a solution that should be highly considered. For this purpose a trial version of Faddom was deployed and evaluated and various stakeholders in various Infrastructure sub-domains have concluded the software is exceeding the requirements and in some cases is given the predicate the holy grail.

What are the internal and/or external factors driving the need for this new software?

Internal factors driving this project: Knowledge domain gaps, business continuity, network visibility (non-routed traffic is a blind spot without the solution), documentation, change management, infrastructure cloud migration, reduction of unplanned outages, mitigation of risks

External factors driving this project: Security: our mission-critical servers are running on legacy operating systems (out of support): Windows 2003, ... and on a public network range. This dual security challenge mean [CLIENT] is extremely vulnerable for cyberattacks.
Solution Description:

The software runs on Vmware and discovers all network traffic via the protocol Netflow (and s-flow) between physical servers and virtual machines. It automatically maps these server traffic flows in a graphical or table format and allows to verify changes that happened since a specific point in time (* after installation of the software) on a particular subcomponent. It is agentless software (no components need to be installed on servers in order to function) and it's main benefits are in the domains of:

- Change Management
- Network and Security
- Cloud / Firewall / Datacenter Migration
- Application Migration/Renewal
Summary of Software Benefits:

Strategic Alignment
The product allows to fill in knowledge gaps which were created at [CLIENT] for various reasons (leaving personnel, job protection, ...). It also fills a blind spot where non-routed network traffic become visible (= core functionality of the product) which obviously raises enthusiasm with the network and security engineers as it allows to create more secure firewall rules and introduce micro segmentation in the future.

The product was mainly used to inventory the network flows between servers in a public network range (132.2.5.*), which should be migrated to a private network range for security reasons. The project was evaluated at [CLIENT] impossible to accomplish, however thanks to the analysis features of the product it is clear [CLIENT] may proceed with the project, as the missing information can be obtained with a simple click of a button.

The product also allows to prepare for a potential infrastructure cloud migration, it analyses which systems belong together, calculates costs of migrating a subset of machines to Azure, AWS, etc ... and groups machines logically together in migration waves.

Figure 1: Example map of systems that interact with other systems that can be retrieved from the software.
Figure 2: The same information as above but listed in table format, identifying how frequent connections are made.

Figure 3: With some tuning (training), easy cloud cost calculation can be obtained for various cloud hosting offers (Azure, AWS). The above screenshot is a simulation of the Dosimetry application to be hosted on the AWS cloud in Frankfurt.
Business Process Improvement

In order to reach a more reliable, secure and predictable outcome of changes to the IT infrastructure environment, the product can easily demonstrate which systems will be impacted, which changes happened to a subcomponent of the environment in history (max. 60 days back).

IT Architecture

The software allows to easily retrieve information of traffic flows between systems. In case of doubt if a change will impact other systems, it is very easy to verify which components will be impacted by the non availability of a system.

Competitive Edge

The product allows to plan, execute, review, changes and replace infrastructure at a much faster rate in a reliable and secure way. The output coming out of the product allows [CLIENT] to accelerate its digital transformation journey and potentially will be a foundation block for a migration to the cloud. The Infrastructure Team will benefit considerably as “lost knowledge” can be regained by use of the tool. A migration of legacy software to a newer version does not have to be the end of the world, since persons who implemented the software have long left the company.

Risk

Visibility on how system components interact with each other is key for changes and transformation in a company.

Underachievement (performance degradation), Malware are negative factors which have been dealt with since the trial of the software started. Some of the data that the product delivers may be possible to obtain via a concatenation of output of several other tools, but will require several man hours/days to accomplish, while with one click an impressive amount of useable information is coming out of the evaluated product. The product does not make use of software agents, it is based on netflow and s-flow protocols and has no negative performance impact on other systems.

Figure 4: Inactive Servers are detected by the software, however human intelligence is required to determine if the server can be safely decommissioned.
Other use cases we evaluated

Certificate Expiry monitoring
Various incidents in the past happened at [CLIENT] where certificates were expired and not noticed by IT pro-actively, causing corporate image damage towards external clients as systems were unavailable or showing a security warning that certificates were expired. Faddom displays the status of all certificates detected on the network and allows mail notification when renewal is required.

Malware detection
Although not a marketed feature of the product, during the trial two pc's with malware were detected by accident. A high number of connections to the vCenter from an unknown pc were detected. The case was investigated and mitigated.

Discovery of DNS requests towards phased-out domain controllers
In 2020 a domain controller died due to a hardware failure. Servers who connect for DNS requests (port 53) to a DNS Server (domain controller) that is not reachable, experience serious performance impact. The product easily extracted...
a table of systems that were still connecting for DNS requests to the deceased domain controller.

DNS entries were corrected on the affected source systems after identification via standard change process.

[CLIENT] will plan the decommissioning of two additional legacy domain controllers in the next coming weeks, the same technique is considered proactively to avoid disruption.

**Removal of Adobe Flash from server systems**

Microsoft has issued a security patch to uninstall Flash from server systems as it is vulnerable legacy technology. A request was issued by the IT Security Manager to implement this patch on all server systems during the February maintenance weekend. As the implementation of the patch is irreversible (no rollback possible) it may break applications that make use of the legacy technology. Since no inventory exists at [CLIENT] for Flash based application, a query on port 1935 learns us that flash is still in use on several server systems.

**Evaluation by System Engineer of the product**

A trial version was installed and evaluated in-depth at [CLIENT]. Installation was extremely easy and straightforward to set up. During the trial a software upgrade was performed (in order to evaluate the upgrade procedure) and found extremely easy to accomplish (both Application and sensor appliances). Faddom Support proved easy, reliable to reach and answered very fast to any queries. The initial scope to evaluate the product for documentation of the 132 public range was expanded to several other use cases as described above.

The product exceeded expectations and is considered indispensable to
EXECUTION TIMELINE:

» Business case approved: 1st of February, 2021
» Software vendor contract signed: 15th of February, 2021
» Project work start date: 15th of February, 2021
» Go-live date: 1st of March, 2021
» Training for end users: 1st of March, 2021

PROJECT GOVERNANCE:

» Executive sponsor: CIO
» Business owner: ICT Operation Manager
» Project manager: Project Manager
» IT Lead: Senior System Engineer + Change Manager
» Trainer: Faddom Session
Faddom creates interactive, real-time maps of your entire IT ecosystem, offering granular detail. Our solution is completely platform-agnostic and has limitless use-cases. Uniquely, Faddom works without credentials, firewalls, or agents. With network discovery based on real traffic, you gain ultimate visibility of all dependencies and communications. Use this to efficiently assess costs, discover a hybrid ecosystem, or model workloads for migration.

Our platform is easy to deploy, highly scalable, and can be integrated with all of your current tools and products seamlessly. Whether you are primarily on the cloud, utilize hybrid or multi-cloud environments, or reside on-premises, Faddom can be used to discover, plan, and maintain the most comprehensive real-time map for your application ecosystems. You can easily configure your map to manage IT assets by business context, prioritizing the right alerts and, more importantly, keeping your business running smoothly.

Contact us at info@Faddom.com to see a live demo.