FADDOM

A Faddom Case Study

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

Table of Contents:

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

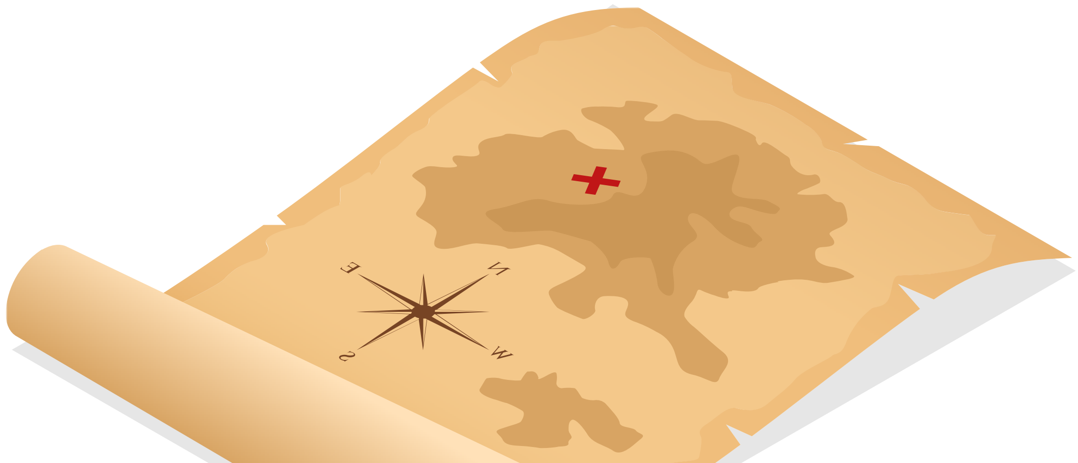
Due to knowledge gaps, lack of confidence and fear of P1 incidents, internal staff is reluctant to proceed with these projects and the IT infrastructure remains on unsupported and vulnerable platforms.

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
- Appilcation 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 visibile (= 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.

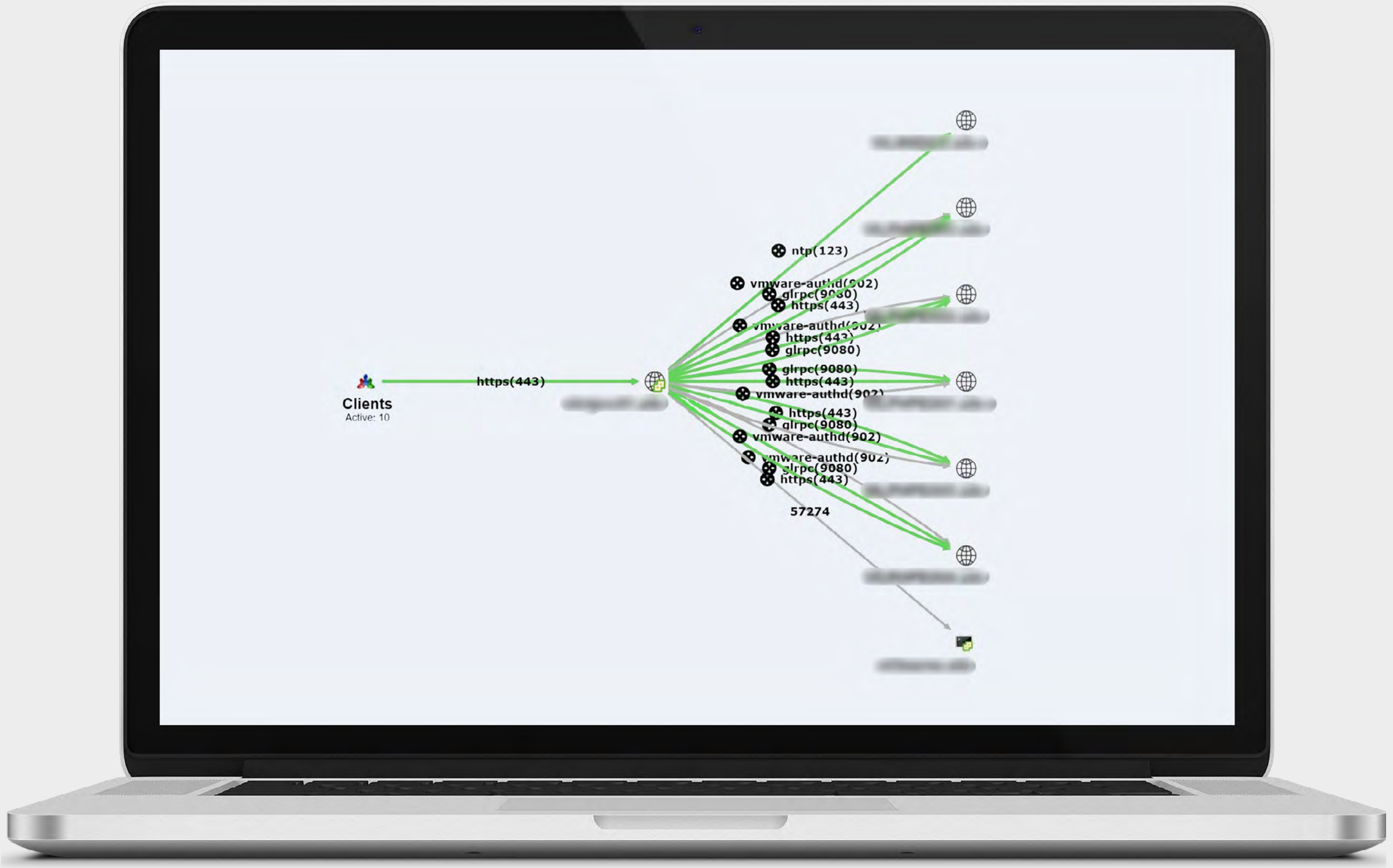
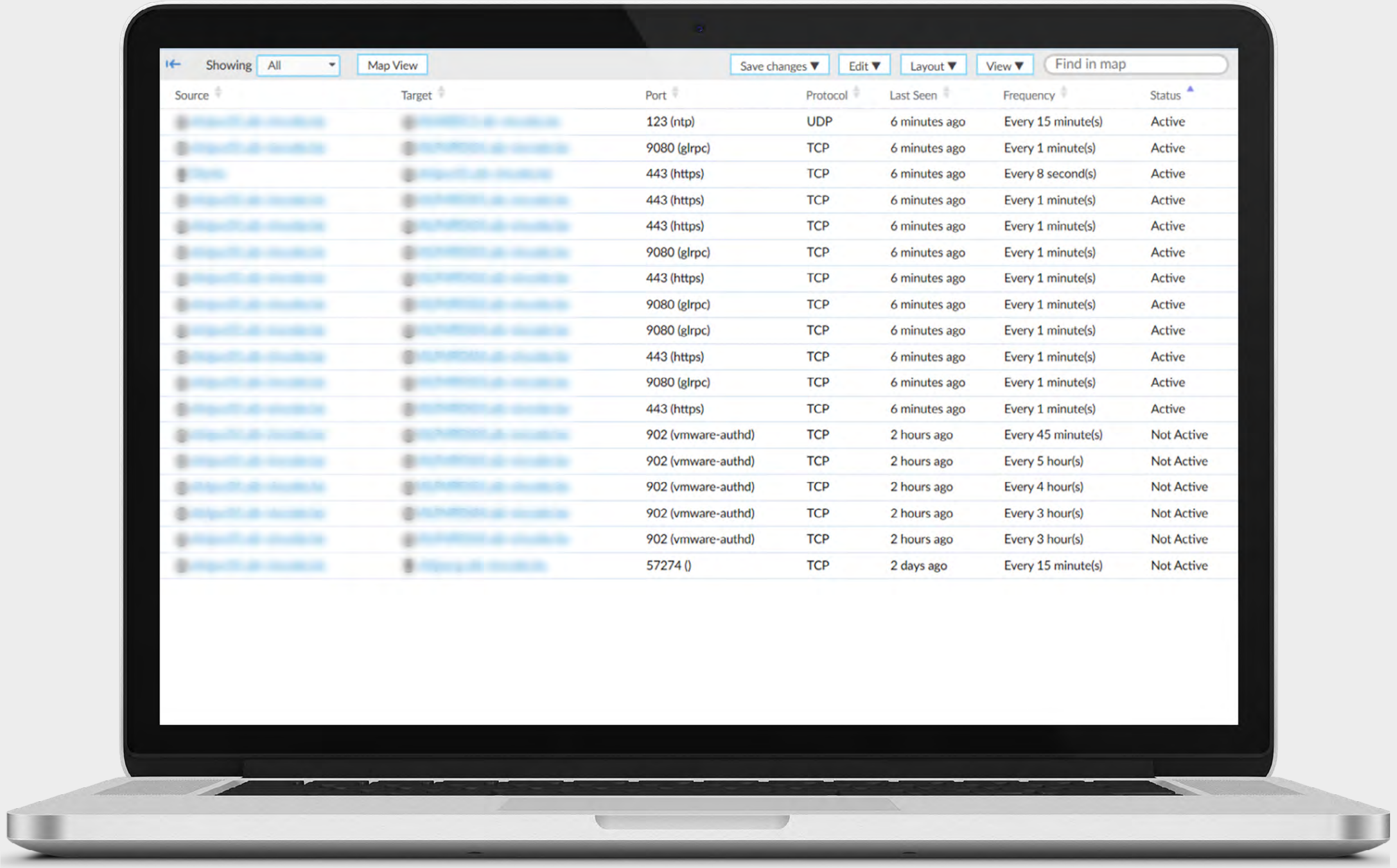
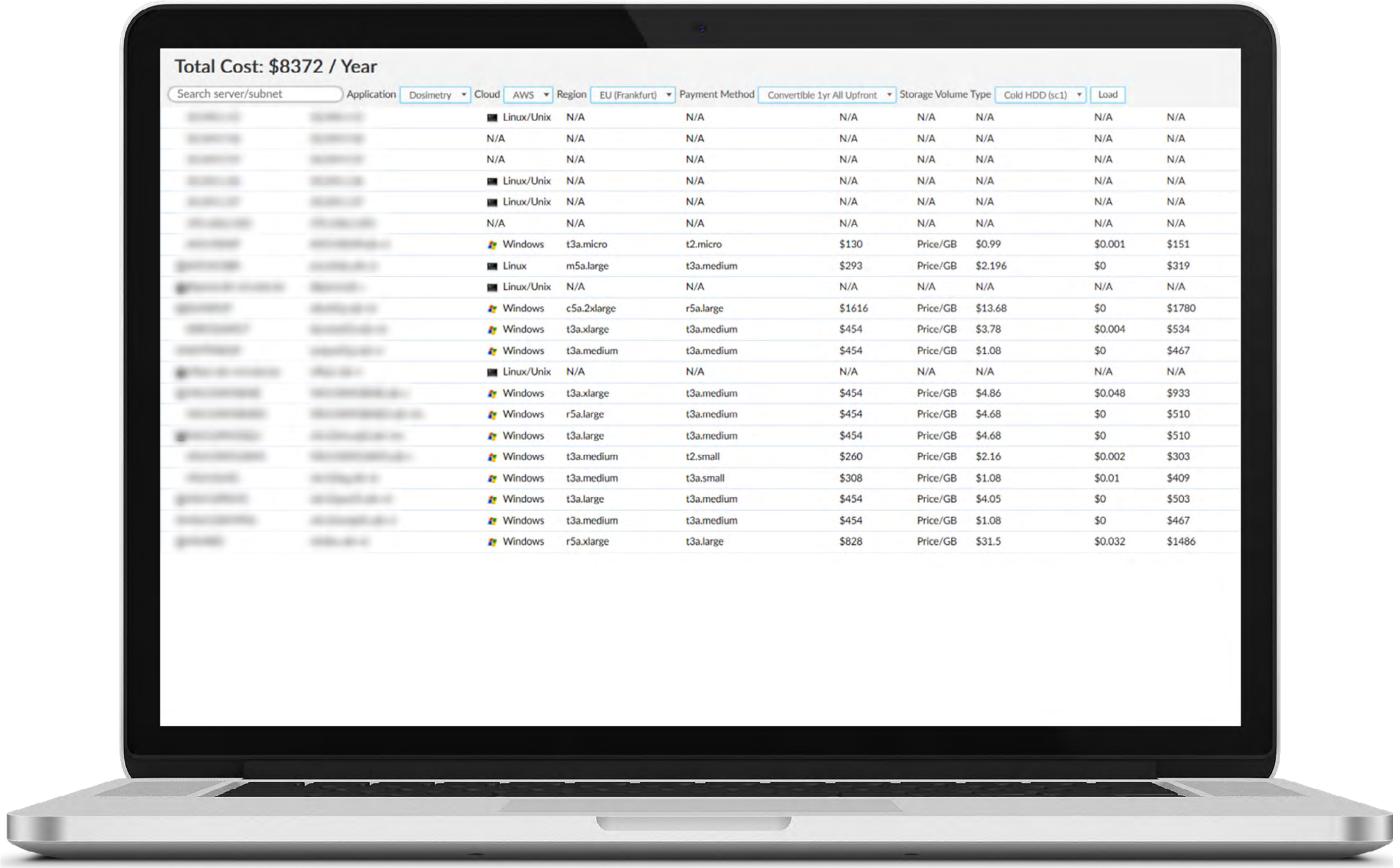


Figure 1:
Example map of systems that interact with other systems that can be retrieved from the software.



Source	Target	Port	Protocol	Last Seen	Frequency	Status
[redacted]	[redacted]	123 (ntp)	UDP	6 minutes ago	Every 15 minute(s)	Active
[redacted]	[redacted]	9080 (glrpc)	TCP	6 minutes ago	Every 1 minute(s)	Active
[redacted]	[redacted]	443 (https)	TCP	6 minutes ago	Every 8 second(s)	Active
[redacted]	[redacted]	443 (https)	TCP	6 minutes ago	Every 1 minute(s)	Active
[redacted]	[redacted]	443 (https)	TCP	6 minutes ago	Every 1 minute(s)	Active
[redacted]	[redacted]	9080 (glrpc)	TCP	6 minutes ago	Every 1 minute(s)	Active
[redacted]	[redacted]	443 (https)	TCP	6 minutes ago	Every 1 minute(s)	Active
[redacted]	[redacted]	9080 (glrpc)	TCP	6 minutes ago	Every 1 minute(s)	Active
[redacted]	[redacted]	9080 (glrpc)	TCP	6 minutes ago	Every 1 minute(s)	Active
[redacted]	[redacted]	443 (https)	TCP	6 minutes ago	Every 1 minute(s)	Active
[redacted]	[redacted]	9080 (glrpc)	TCP	6 minutes ago	Every 1 minute(s)	Active
[redacted]	[redacted]	443 (https)	TCP	6 minutes ago	Every 1 minute(s)	Active
[redacted]	[redacted]	902 (vmware-authd)	TCP	2 hours ago	Every 45 minute(s)	Not Active
[redacted]	[redacted]	902 (vmware-authd)	TCP	2 hours ago	Every 5 hour(s)	Not Active
[redacted]	[redacted]	902 (vmware-authd)	TCP	2 hours ago	Every 4 hour(s)	Not Active
[redacted]	[redacted]	902 (vmware-authd)	TCP	2 hours ago	Every 3 hour(s)	Not Active
[redacted]	[redacted]	902 (vmware-authd)	TCP	2 hours ago	Every 3 hour(s)	Not Active
[redacted]	[redacted]	57274 ()	TCP	2 days ago	Every 15 minute(s)	Not Active

Figure 2:
The same information as above but listed in table format, identifying how frequent connections are made.



Total Cost: $8372 / Year

Application: Dosimetry; Cloud: AWS; Region: EU (Frankfurt); Payment Method: Convertible 1yr All Upfront; Storage Volume Type: Cold HDD (sc1)

[redacted]	[redacted]	Linux/Unix	N/A	N/A	N/A	N/A	N/A	N/A	N/A
[redacted]	[redacted]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
[redacted]	[redacted]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
[redacted]	[redacted]	Linux/Unix	N/A	N/A	N/A	N/A	N/A	N/A	N/A
[redacted]	[redacted]	Linux/Unix	N/A	N/A	N/A	N/A	N/A	N/A	N/A
[redacted]	[redacted]	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
[redacted]	[redacted]	Windows	t3a.micro	t2.micro	$130	Price/GB	$0.99	$0.001	$151
[redacted]	[redacted]	Linux	m5a.large	t3a.medium	$293	Price/GB	$2.196	$0	$319
[redacted]	[redacted]	Linux/Unix	N/A	N/A	N/A	N/A	N/A	N/A	N/A
[redacted]	[redacted]	Windows	c5a.2xlarge	r5a.large	$1616	Price/GB	$13.68	$0	$1780
[redacted]	[redacted]	Windows	t3a.xlarge	t3a.medium	$454	Price/GB	$3.78	$0.004	$534
[redacted]	[redacted]	Windows	t3a.medium	t3a.medium	$454	Price/GB	$1.08	$0	$467
[redacted]	[redacted]	Linux/Unix	N/A	N/A	N/A	N/A	N/A	N/A	N/A
[redacted]	[redacted]	Windows	t3a.xlarge	t3a.medium	$454	Price/GB	$4.86	$0.048	$933
[redacted]	[redacted]	Windows	r5a.large	t3a.medium	$454	Price/GB	$4.68	$0	$510
[redacted]	[redacted]	Windows	t3a.large	t3a.medium	$454	Price/GB	$4.68	$0	$510
[redacted]	[redacted]	Windows	t3a.medium	t2.small	$260	Price/GB	$2.16	$0.002	$303
[redacted]	[redacted]	Windows	t3a.medium	t3a.small	$308	Price/GB	$1.08	$0.01	$409
[redacted]	[redacted]	Windows	t3a.large	t3a.medium	$454	Price/GB	$4.05	$0	$503
[redacted]	[redacted]	Windows	t3a.medium	t3a.medium	$454	Price/GB	$1.08	$0	$467
[redacted]	[redacted]	Windows	r5a.xlarge	t3a.large	$828	Price/GB	$31.5	$0.032	$1486

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

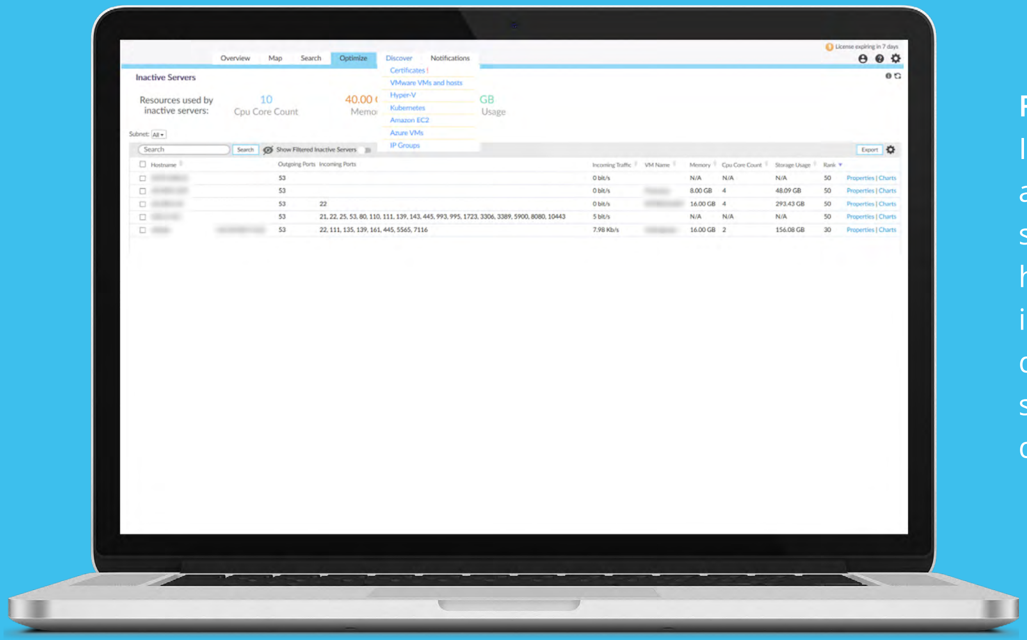
Competitive Edge

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 considerabely 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.



Inactive Servers

Resources used by inactive servers: 10 Cpu Core Count 40.00 (Memo GB Usage

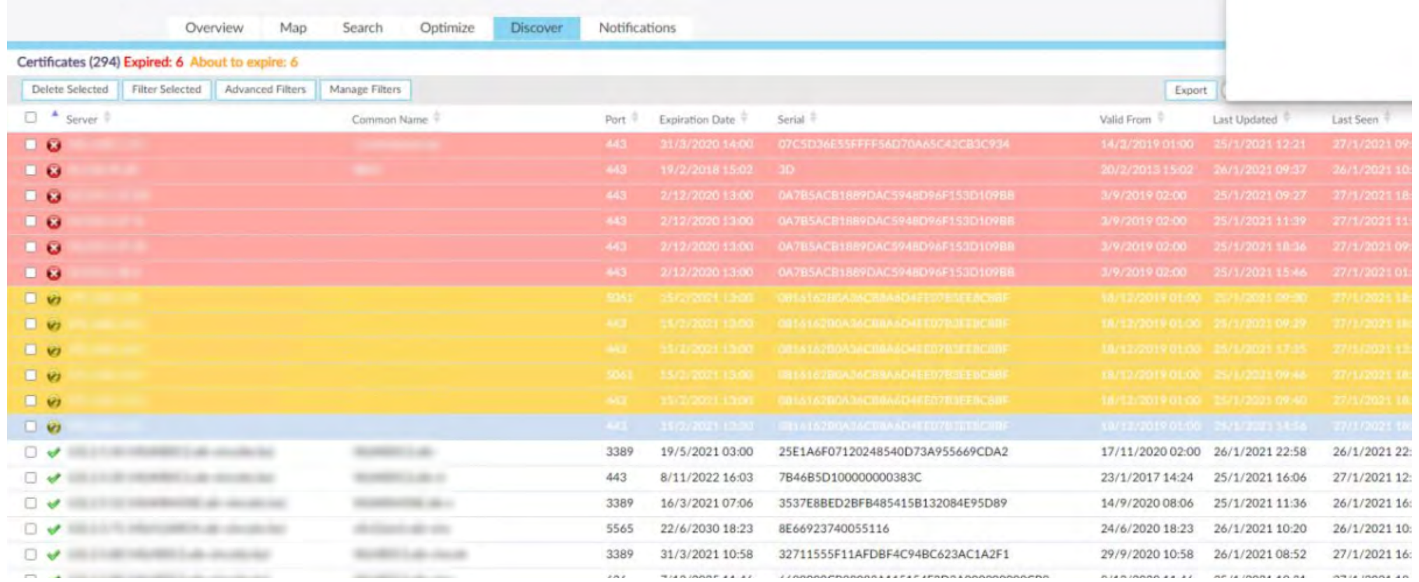
☐ Hostname	Outgoing Ports	Incoming Ports	Incoming Traffic	VM Name	Memory	Cpu Core Count	Storage Usage	Rank	
☐ [redacted]	53		0 bit/s		N/A	N/A	N/A	50	Properties | Charts
☐ [redacted]	53		0 bit/s	[redacted]	8.00 GB	4	48.09 GB	50	Properties | Charts
☐ [redacted]	53	22	0 bit/s	[redacted]	16.00 GB	4	293.43 GB	50	Properties | Charts
☐ [redacted]	53	21, 22, 25, 53, 80, 110, 111, 139, 143, 445, 993, 995, 1723, 3306, 3389, 5900, 8080, 10443	5 bit/s		N/A	N/A	N/A	50	Properties | Charts
☐ [redacted] [redacted]	53	22, 111, 135, 139, 161, 445, 5565, 7116	7.98 Kb/s	[redacted]	16.00 GB	2	156.08 GB	30	Properties | Charts

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 in required.



Certificates (294) Expired: 6 About to expire: 6

□		Server	Common Name	Port	Expiration Date	Serial	Valid From	Last Updated	Last Seen
□	✗	[redacted]	[redacted]	443	31/3/2020 14:00	07C5D36E55FFFF56D70A65C42CB3C934	14/2/2019 01:00	25/1/2021 12:21	27/1/2021 09:
□	✗	[redacted]	[redacted]	443	19/2/2018 15:02	3D	20/2/2013 15:02	26/1/2021 09:37	26/1/2021 10:
□	✗	[redacted]		443	2/12/2020 13:00	0A7B5ACB1889DAC5948D96F153D109BB	3/9/2019 02:00	25/1/2021 09:27	27/1/2021 18:
□	✗	[redacted]		443	2/12/2020 13:00	0A7B5ACB1889DAC5948D96F153D109BB	3/9/2019 02:00	25/1/2021 11:39	27/1/2021 11:
□	✗	[redacted]		443	2/12/2020 13:00	0A7B5ACB1889DAC5948D96F153D109BB	3/9/2019 02:00	25/1/2021 18:36	27/1/2021 09:
□	✗	[redacted]		443	2/12/2020 13:00	0A7B5ACB1889DAC5948D96F153D109BB	3/9/2019 02:00	25/1/2021 15:46	27/1/2021 01:
□	⚠	[redacted]		5061	15/2/2021 13:00	0B16162B0A36CB8A6D4EE07B3EEBC8BF	18/12/2019 01:00	25/1/2021 09:30	27/1/2021 18:
□	⚠	[redacted]		443	15/2/2021 13:00	0B16162B0A36CB8A6D4EE07B3EEBC8BF	18/12/2019 01:00	25/1/2021 09:29	27/1/2021 18:
□	⚠	[redacted]		443	15/2/2021 13:00	0B16162B0A36CB8A6D4EE07B3EEBC8BF	18/12/2019 01:00	25/1/2021 17:35	27/1/2021 12:
□	⚠	[redacted]		5061	15/2/2021 13:00	0B16162B0A36CB8A6D4EE07B3EEBC8BF	18/12/2019 01:00	25/1/2021 09:46	27/1/2021 18:
□	⚠	[redacted]		443	15/2/2021 13:00	0B16162B0A36CB8A6D4EE07B3EEBC8BF	18/12/2019 01:00	25/1/2021 09:40	27/1/2021 18:
□	⚠	[redacted]		443	15/2/2021 13:00	0B16162B0A36CB8A6D4EE07B3EEBC8BF	18/12/2019 01:00	25/1/2021 14:56	27/1/2021 16:
□	✓	[redacted]	[redacted]	3389	19/5/2021 03:00	25E1A6F07120248540D73A955669CDA2	17/11/2020 02:00	26/1/2021 22:58	26/1/2021 22:
□	✓	[redacted]	[redacted]	443	8/11/2022 16:03	7B46B5D100000000383C	23/1/2017 14:24	25/1/2021 16:06	27/1/2021 12:
□	✓	[redacted]	[redacted]	3389	16/3/2021 07:06	3537E8BED2BFB485415B132084E95D89	14/9/2020 08:06	25/1/2021 11:36	26/1/2021 16:
□	✓	[redacted]	[redacted]	5565	22/6/2030 18:23	8E66923740055116	24/6/2020 18:23	26/1/2021 10:20	26/1/2021 10:
□	✓	[redacted]	[redacted]	3389	31/3/2021 10:58	32711555F11AFDBF4C94BC623AC1A2F1	29/9/2020 10:58	26/1/2021 08:52	27/1/2021 16:

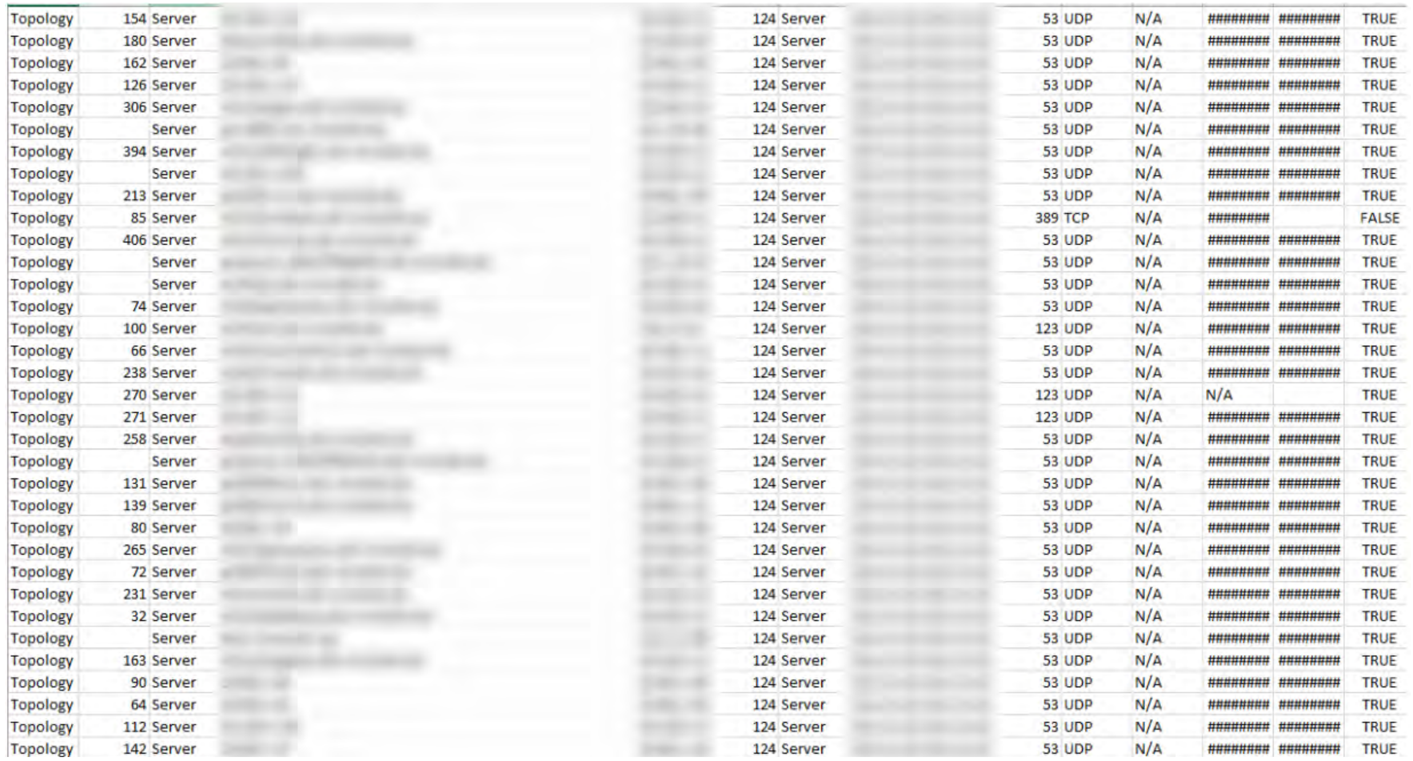
Figure 5:
Expiry status of SSL Certificates.

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



Topology	154	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	180	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	162	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	126	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	306	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology		Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	394	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology		Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	213	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	85	Server	[redacted]	[redacted]	124	Server	[redacted]	389	TCP	N/A	########		FALSE
Topology	406	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology		Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology		Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	74	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	100	Server	[redacted]	[redacted]	124	Server	[redacted]	123	UDP	N/A	########	########	TRUE
Topology	66	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	238	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	270	Server	[redacted]	[redacted]	124	Server	[redacted]	123	UDP	N/A	N/A		TRUE
Topology	271	Server	[redacted]	[redacted]	124	Server	[redacted]	123	UDP	N/A	########	########	TRUE
Topology	258	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology		Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	131	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	139	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	80	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	265	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	72	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	231	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	32	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology		Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	163	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	90	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	64	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	112	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE
Topology	142	Server	[redacted]	[redacted]	124	Server	[redacted]	53	UDP	N/A	########	########	TRUE

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.

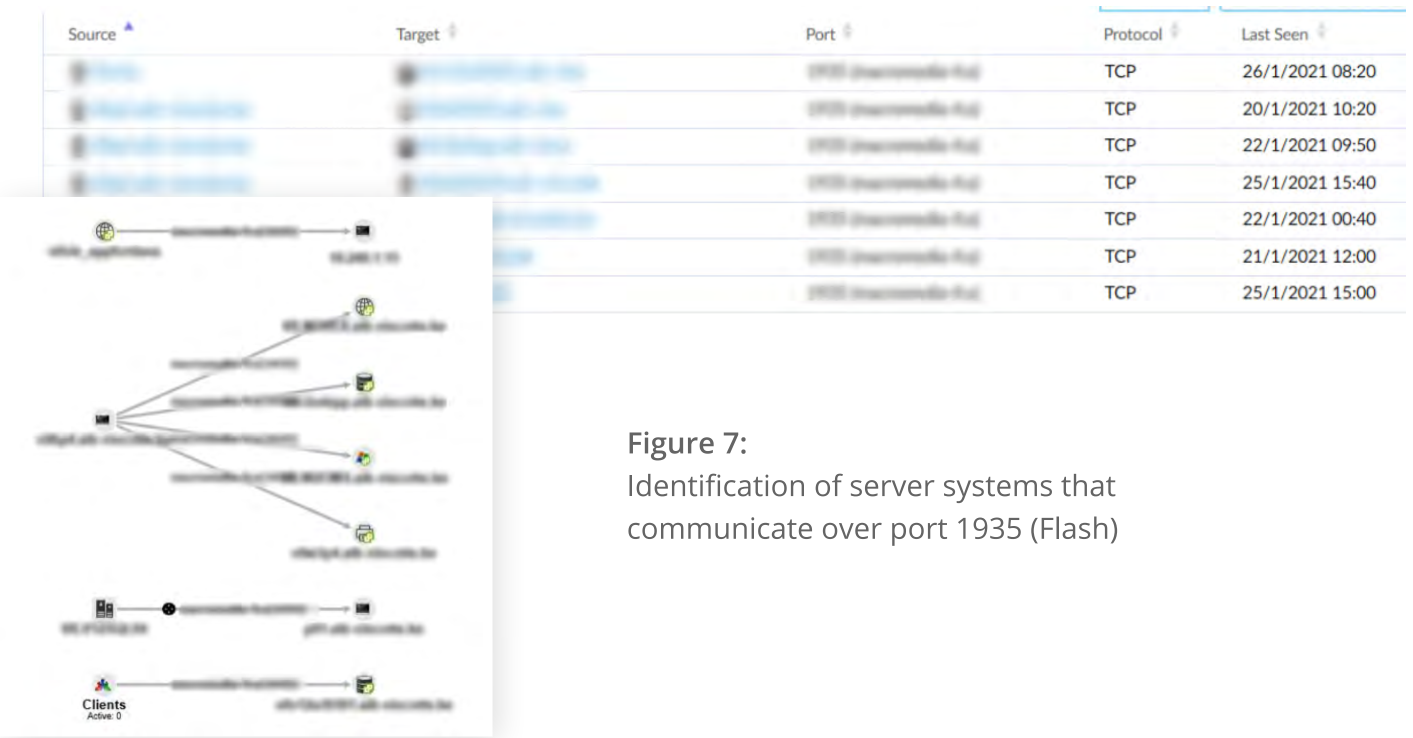
[CLIENT] will plan the decommissioning of two additional legacy domain controllers in the next coming weeks, the same technique is considered pro-actively to avoid disruption.

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



Source	Target	Port	Protocol	Last Seen
[redacted]	[redacted]	[redacted]	TCP	26/1/2021 08:20
[redacted]	[redacted]	[redacted]	TCP	20/1/2021 10:20
[redacted]	[redacted]	[redacted]	TCP	22/1/2021 09:50
[redacted]	[redacted]	[redacted]	TCP	25/1/2021 15:40
[redacted]	[redacted]	[redacted]	TCP	22/1/2021 00:40
[redacted]	[redacted]	[redacted]	TCP	21/1/2021 12:00
[redacted]	[redacted]	[redacted]	TCP	25/1/2021 15:00

Figure 7:
Identification of server systems that communicate over port 1935 (Flash)

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 th 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 + Chage Manager
- **Trainer:** Faddom Session

About Faddom

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.