Jisc

certero.

SaaS Shadow IT:

Bringing Shadow SaaS Spend and Risks Under Control

eBook

SaaS Shadow IT - Turn the Unknown into the Known

Shadow IT comes in many forms and is indicative of organisations no longer requiring the technical enablement of an internal IT team to access and reap the benefits of technology enabled by the cloud.

This means that IT's long-established governance and control over IT assets is typically circumvented, resulting in pockets of technology spending and company data residing in systems and software that aren't centrally known, commercially optimised or secured.

To coincide with the launch of Certero's new Shadow IT solution for SaaS, we will look at the challenges around finding shadow Software-as-a-Service (SaaS) and how these unauthorised IT assets can be brought into a mature and sustainable long-term software management process. Strong governance practices combined with new technologies to capture SaaS usage will protect the business from the risks posed by unwanted business applications.

In parallel, the identification of SaaS apps that become approved is a strong indication of where organisations can gain value through software in practice. SaaS apps are often selected because they make tasks faster, better and easier or are more collaborative, for example. These useful applications can potentially become centrally managed and commercially optimised through an approved software policy, so Shadow IT certainly presents an opportunity, if the risks can be understood and controlled.

SaaS Discovery and optimisation is essential to be able to combine a modern, frictionless and user-lead software policy with essential controls to keep your organisation productive and safe. In this eBook, we'll look at how this can be achieved and some of the best approaches, risks and challenges to be aware of.

CONTENTS

CHAPTER 1

The Challenge of Shadow SaaS

Over-spending on known SaaS subscriptions can be as high as 50%. Consider the spend on SaaS you can't see.

Certero helps organisations 'see', understand and optimise their IT assets everywhere. One of the biggest market drivers for Certero customers, is gaining centralised visibility of their IT infrastructure and understanding precisely what software is out there - whether it's correctly licensed, if it's secure and if they're wasting money on software *that is never actually used*.

It's widely agreed that in the on-premises world, approximately 30% of software deployed is a wasted investment.

Alarmingly, with the nature of SaaS applications being licensed on a much more granular 'Named User' basis that typically renew automatically, we frequently see this level of wastage increase to 50%.

Logically then, similar levels of financial inefficiency could be occurring with the SaaS applications that aren't centrally procured or managed, and a recent Gartner report stated that '**by 2027, 75% of employees will acquire, modify or create technology outside IT's visibility**'**.

This financial inefficiency is combined with other potential business risks, such as:

- **Data Security**
  Who is accessing confidential company information?
- **Rapidly Changing Stack of Applications**
  With a typical annual churn of approx. 39%.
- **Rapid Growth**
  SaaS expenditure is projected to grow 20% to £194.6bn in 2024*** (Gartner) and businesses typically have upwards of 500 SaaS applications active within their environment.
- **Data Location**
  Are SaaS apps compliant with privacy laws and regulations.

CHAPTER 2

SaaS and Business Policy

Shadow SaaS is ultimately a 'people and culture' issue, as logically, the simplest way to limit the business risk would be to set out a business culture and code of conduct that would discourage users or departments from going out and sourcing their own IT software and services.

Given that the shadow IT issue is growing so rapidly, modern business culture prioritises the frictionless nature of cloud enablement and growth over the challenges of securing and controlling the risks that come with it.

This same working culture may also enable employees to utilise their own devices under a 'bring-your-own-device' (BYOD) policy. This opens new avenues in which organisations potentially forego their data security and governance in favor of employee satisfaction and comfort.

Cyber security research suggests* that employees will tend to use their own devices even if the practice is forbidden, so it is important for organisations to make clear and informed judgments on these working practices and to communicate policies clearly, as well as find ways to follow them up and enforce them.

In this context, SaaS discovery is in equal parts a way to identify and to address unwanted employee behaviors, and a means to govern and serve new business needs at the pace and in the style that users prefer.

SaaS Discovery Challenges

So, why is Shadow SaaS a challenge to discover?

1 Cloud-based	SaaS applications operate in the cloud and are accessed via the internet, rather than being installed locally on individual machines. Because SaaS apps don't leave a local footprint on devices, traditional ITAM and SAM tools can't detect or inventory them.
2 Free SaaS Blind Spot	Finance, expense, and accounting tools typically capture data on paid subscriptions and transactions. However, they do not track or record instances of free SaaS applications, as no financial transactions are involved with these apps, creating a blind spot for free SaaS apps.
3 Single Sign-on Tools	Single sign-on (SSO) tools streamline the login process by allowing users to access multiple applications with one set of credentials. However, they only track login activities. This means if a user has access to an application but doesn't log in, the SSO tool won't capture their non-usage.
4 Bring-Your-Own-Device	In a BYOD setup, employees use their personal devices for work purposes. Unlike company-issued devices, these personal devices are not under the direct control of the organisation's IT department. As a result, IT cannot monitor activities on these devices as effectively.
5 Detective Job	However evidence of SaaS is discovered, there still needs to be a robust process in place to go and question users on their activity, make them aware if web apps may be prohibited and to identify what, how and why shadow SaaS software is being used.

Technical Approach

The one thing that is consistent with the use of all SaaS applications, is that they require a web browser to access them.

This raises three important points of control:

- ***Do you have an approved web-browser policy to prevent 'unmanageable' browsers from being used?***
- ***Can you see all of your end-user devices?***

Approved / Denied Web Browsers

Many organisations have an approved web-browser policy in place, but most do not enforce it with any kind of active measure, such as having a way to restrict access to software and web browsers at a device or user level.

You Still Can't Manage What You Can't See

Even with SaaS apps, there's just no escaping the need for solid network discovery and inventory to bring end-user devices and activity into focus. End-user devices everywhere must be brought into centralised visibility and control if organisations are to be able to identify shadow SaaS through a browser.

How Certero Do It

Certero has the ability to actively restrict access to software including web browsers, within the Access Control module. This can be used to enforce software policy lists across installed applications and devices.

How Certero Do It

Certero combines the management of traditional on-premises, remote and cloud / SaaS IT within one single platform solution.

SaaS Inventory and Data Normalisation

Once a view of user web activity has been captured, there needs to be an automated way to identify all of the websites that could potentially be SaaS applications and for these to be logically categorised into meaningful groups that can then be investigated and managed.

You Will Want To Know:

- What SaaS apps are being potentially accessed, by whom and what they are for (file sharing, web calling etc.).
- Which SaaS apps may present a cost, data or potential security risk.
- Scope and scale of usage.
- Patterns of usage.
- Which applications and users are your highest priorities to bring under control.

Once discovered, SaaS applications will need to be organised and logically categorised to help understand the reason for using them.

It is best practice to 'tag' discovered web apps, helping to create meaningful connections to business functions, such as Research and Development, Marketing or Engineering.

Where a discovered SaaS application is already an approved business application, an 'application owner' should be assigned to these 'managed' SaaS apps.

Risk Management

Just like the management of on-premises software, managed through an ITAM / SAM solution, the aim of SaaS discovery is to bring these web applications into a managed software policy that includes an 'approved and denied' list of web applications.

Within Certero for SaaS Shadow IT, applications can be easily categorised down to a granular level. This shows that software policy is rarely a 'one-size fits all' approach when it comes to 'approved software'.

You May Categorise SaaS Apps as:

- Fully allowed
- Allowed for specified users
- Denied for specified users
- Fully denied
- Security risk

Authentication Standards

Whether or not SaaS apps meet corporate security standards can be a leading factor as to whether they become 'allowed' or 'denied' within your organisation.
For example – do discovered SaaS apps require 2 factor authentication? Certero for SaaS Shadow IT can help to enrich understanding of SaaS application security through intelligent, automated recognition and categorisation.

Sensitive Data

There is always a potential for SaaS apps to contain sensitive data or personally identifiable information. These SaaS apps can typically be recognised through their categorisation and their risk assessed accordingly.

How Certero Do It

Certero for SaaS Shadow IT automates the identification and normalisation processes by referencing a database of over 30,000 known SaaS applications; applying industry standard definitions and categorisations so you can quickly and easily make informed decisions.

SaaS Optimisation

With ‘allowed’ applications there are commercial risks to be avoided and governance processes to be followed, including:

Ownership

As described above, ‘allowed’ software that is deemed to be of no (current) risk and is of value to the organisation, should be given a Software Application Owner, where possible, to support the long-term understanding of what and why the application is present.

Automated Commercial SaaS Optimisation

SaaS costs can easily grow out of control, be brought back under control, and then go out of control again! The long-term management and optimisation of costs is best performed through centralised procurement and, where possible, a centralised universal connector into an available SaaS tenant.

This is where ‘allowed’ SaaS apps can become ‘managed’ and commercially optimised using a solution that has a connector to the SaaS vendor portal (such as with Microsoft 365 for example).

This provides a way to connect and visualise all of your named user subscriptions, costs, usage, wastage and how well your license types are tailored to real-world usage.

Proactive optimisation of known SaaS apps managed through a connector to the tenant, provides the opportunity to reduce licensing costs quickly, as the risk of routine over-licensing and auto-renewals is always high.

How Certero Do it

Discovering SaaS in a Safe Way

There is a new way to capture evidence of SaaS applications safely through user’s web activity. This pioneering approach is used by the new Certero for SaaS Shadow IT solution, that:

- Captures evidence of users’ web activity and highlights where they have accessed SaaS applications.
- Automatically cleanses data to indicate SaaS application usage.
- Does not allow invasive, personal or confidential information to be captured through keystrokes or passwords etc.
- Enables rich information on users due to being part of the Certero platform that spans on-premises ITAM & SAM, as well as SaaS and cloud. This provides full-spectrum hardware and software discovery, the ability to push-out and remove software and valuable broader integrations with information sources, including Active Directory.
- Can easily integrate information into any ITSM tool, for example to populate a Configuration Management Database.

CASE STUDY

Microsoft 365 Optimisation

This transport and logistics business was able to identify a $1.6m cost saving by gaining transparency of all their M365 subscriptions, identifying:

- **Subscription Utilisation:**
  The solution quickly identified areas where licenses were not being utilised, creating significant cost saving opportunities.

- **Security Risks:**
  Identification of users who had not reset their password in the time frame outlined within the company policy, creating a security risk.

- **Right sizing Licenses:**
  A number of users who were not using the full functionality of their allocated license and could be reassigned a 'better fit license', creating substantial cost saving opportunities.

How Certero Do It

Certero for SaaS includes out-of-the-box connectors to the largest 'Tier 1' SaaS vendors, like M365, Adobe Creative Cloud, Salesforce.com and Google Workspace, as well as universal connectors to other SaaS applications to help with the centralised management and optimisation of one of IT's fastest growing expenses.

SaaS Optimisation (continued)

Manual SaaS Entitlement Management

Where it may not be possible to connect to a SaaS vendor portal to see your licensing centrally, it will usually be possible to import or add licensing detail manually into a SaaS optimisation solution.

The optimisation process and principals here are just the same, but are approaching the challenge from the user side, rather than the vendor portal – where licenses assigned to a user but no indication of activity is found through their device.

This is another way of identifying wastage, which is an optimisation opportunity and would be detectable through a SaaS discovery solution.

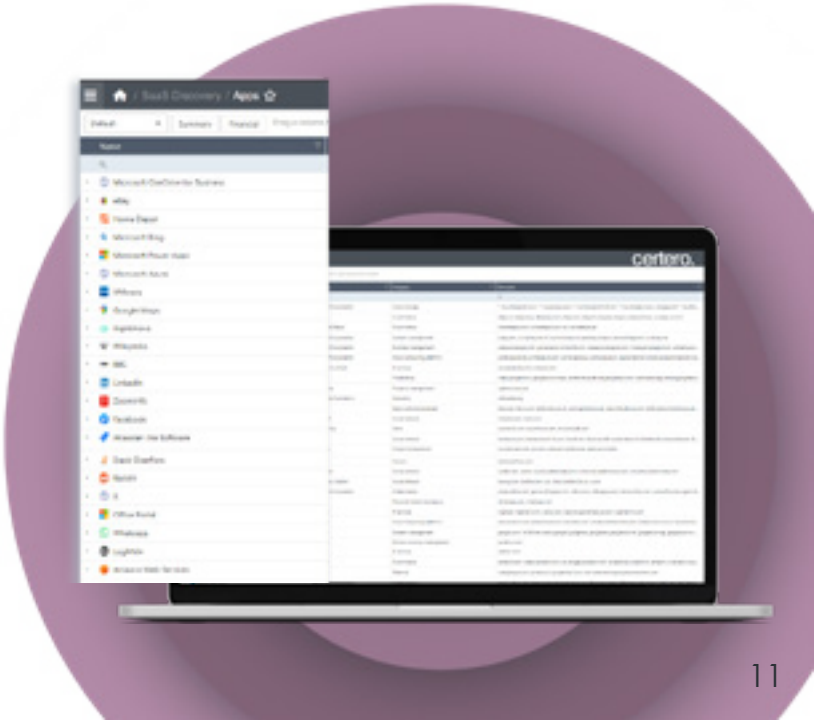
SaaS Rationalisation

As shadow SaaS applications are not procured in a centrally controlled way, it is likely that applications are in use across the business that deliver equal or similar functions and could simply be refined down to a less exhaustive, less risky or less expensive list. For example – multiple video conferencing and messaging apps create split lines of communication that could be avoided.

A SaaS discovery solution will shed light on the functionality, proliferation and usage of apps across a particular category, enabling policy decisions to be made and enforced.

User Profiling

It's likely that users within certain roles, teams or departments are likely to use the same SaaS applications. This can be useful insight to have when tracking potential security concerns, as well as assisting the understanding of SaaS costs for potential new users within the organisation and how IT should be provisioned for them.



Automating and Future Proofing SaaS Discovery

As the discovery and management of SaaS applications is an on-going task that will increase over time, here's a summary of the ways you can avoid potential technological barriers, dead-ends and unnecessary or complex manual processes when developing a SaaS discovery and management process:

Build SaaS management into existing ITAM / SAM / software policy and processes – do not treat it in isolation, as to discover SaaS through web browsers means that your end-user devices must remain visible. So select an ITAM / SAM / SaaS solution that can discover everything.

Make sense of SaaS discovery data as quickly and automatically as possible. For example - Certero for SaaS can recognise and categorise 30k+ SaaS apps straight out of the box.

Use evidence of your organisation's SaaS app preferences to inform your business software policy – users have selected these software tools for a reason, so if they're not a risk, empower user productivity where possible.

Aim to manage and optimise the use of approved shadow SaaS apps through a centralised connector and product owner where possible.

Reduce the risk of shadow SaaS by providing tools that users can use to browse and select applications they need through an automated self-service app store.

Completing the Process of Software Discovery

The addition of Certero for SaaS Shadow IT to the Certero platform, has been described by a Certero customer as completing the full process of software discovery, management, security and optimisation, both on-premises and in the cloud:

"The new SaaS Shadow IT module of Certero adds lots of value when chasing down redundant usage of cloud software and websites – allowing more efficiency and making possible the identification for removal of undesired software.

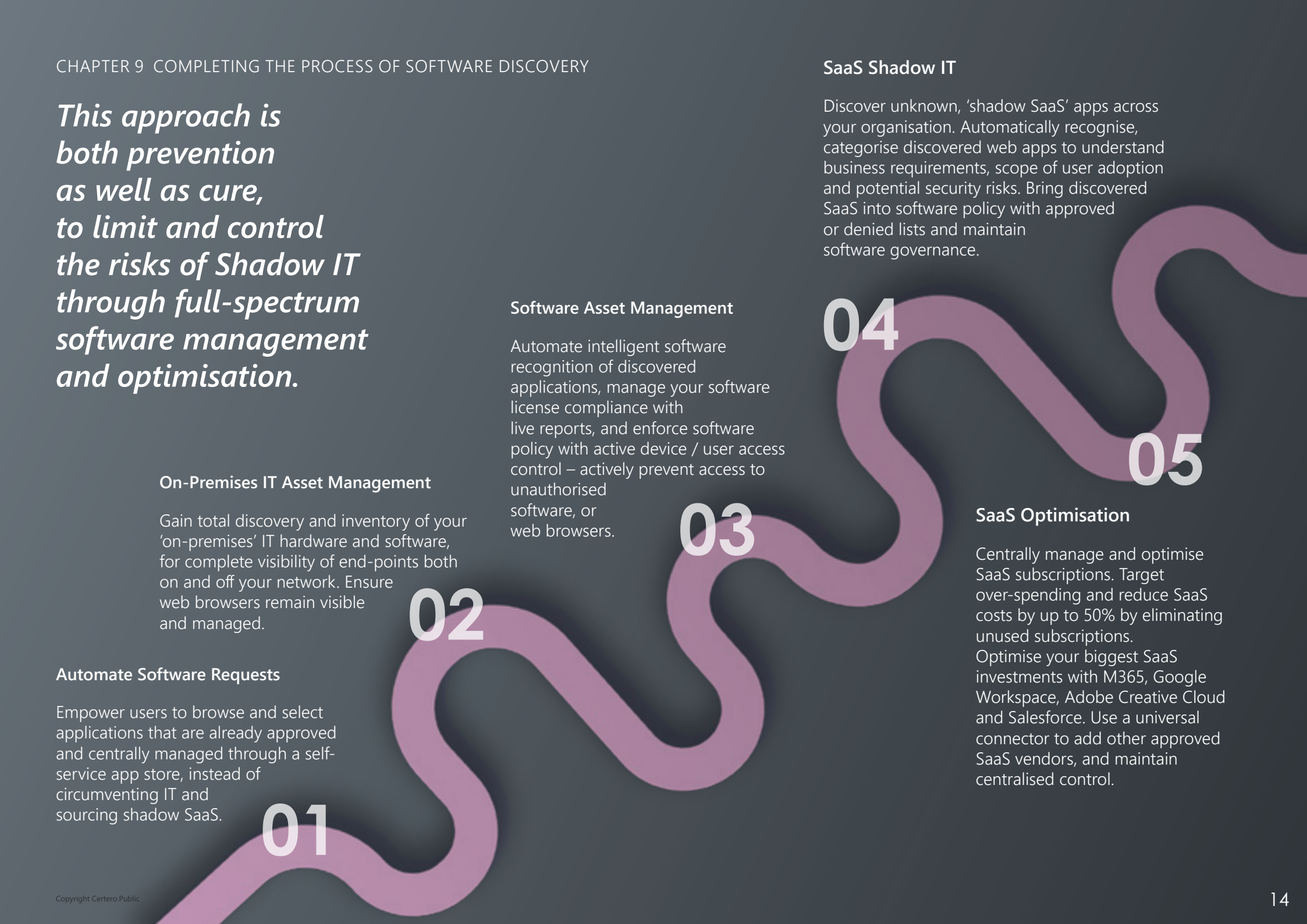
With the new SaaS Shadow IT module, Certero is proving the whole circle of discovery of shadow IT – for any size of business it completes the full control of all software usage."

— License Manager,
Transport and Logistics sector

How Certero Do It

This full-scope management of IT assets through a 'single pane of glass solution', is the driving force behind the products that can all be simply activated within the Certero platform.

This approach is both prevention as well as cure, to limit and control the risks of Shadow IT through full-spectrum software management and optimisation.



01

Automate Software Requests

Empower users to browse and select applications that are already approved and centrally managed through a self-service app store, instead of circumventing IT and sourcing shadow SaaS.

02

On-Premises IT Asset Management

Gain total discovery and inventory of your 'on-premises' IT hardware and software, for complete visibility of end-points both on and off your network. Ensure web browsers remain visible and managed.

03

Software Asset Management

Automate intelligent software recognition of discovered applications, manage your software license compliance with live reports, and enforce software policy with active device / user access control – actively prevent access to unauthorised software, or web browsers.

04

SaaS Shadow IT

Discover unknown, 'shadow SaaS' apps across your organisation. Automatically recognise, categorise discovered web apps to understand business requirements, scope of user adoption and potential security risks. Bring discovered SaaS into software policy with approved or denied lists and maintain software governance.

05

SaaS Optimisation

Centrally manage and optimise SaaS subscriptions. Target over-spending and reduce SaaS costs by up to 50% by eliminating unused subscriptions. Optimise your biggest SaaS investments with M365, Google Workspace, Adobe Creative Cloud and Salesforce. Use a universal connector to add other approved SaaS vendors, and maintain centralised control.

Contact Certero

UK Head Office
Cedarwood 2, Kelvin Close
Birchwood
Warrington
WA3 7PB
T: +44 (0) 1925 868970

info@certero.com

https://www.linkedin.com/company/certero

https://www.certero.com/

Contact Jisc

UK Head Office
4 Portwall Lane
Bristol
BS1 6NB

T: 0300 300 2212

help@jisc.ac.uk

https://www.linkedin.com/company/jisc/

https://www.jisc.ac.uk/

Solutions mentioned in this eBook:

ITAM | SAM | SaaS Shadow IT | SaaS Optimisation | Access Control | Self-Service App Store

RESOURCES

Page 4

* https://www.linkedin.com/pulse/optimising-cloud-spending-uncovering-30-waste-finops-cervantes-knox/
** https://www.resmo.com/blog/shadow-it-statistics#:~:text=Gartner%20estimates%20that%2030%2D40,average%20more%20than%20%244.2%20million
*** https://www.digit.fyi/gartner-public-cloud-spending-to-increase-to-531-6bn-in-2024/#:~:text=Despite%20the%20strong%20growth%20in,%C2%A3194.6bn%20in%202024

Page 5

* https://www.resmo.com/blog/shadow-it-statistics#:~:text=Gartner%20estimates%20that%2030%2D40,average%20more%20than%20%244.2%20million