IMPLEMENTASI *CITRIX ENDPOINT MANAGEMENT* PADA RANCANGAN *SOFTWARE AS A SERVICE* DALAM MENANGANI PERANGKAT *ENDPOINT*

Lela Nurlaela[1)], Septiana Ningtyas[2)], Usanto S[3)]
[1,2]Prodi Teknik Informatika, Fakultas Teknologi, ITB Swadharma
[3]Prodi Sistem Informasi, Fakultas Teknologi, ITB Swadharma

Correspondence author: L.Nurlaela, lela@swadharma.ac.id, Jakarta, Indonesia

Abstract

Endpoint device management has a significant impact on organizational efficiency and productivity. Companies in the information technology sector must be ready to face the challenges of managing endpoint devices that are increasingly complex and varied. This research aims to design a Software-as-a Service (SaaS) solution using Citrix Endpoint Management to overcome these challenges. This research adopts a qualitative method with a case study approach. Data was collected through interviews and observation of existing IT infrastructure. A literature study was also conducted to obtain information about the concepts of endpoint device management, SaaS, and Citrix endpoint management. The result of the research is a SaaS design using Citrix Endpoint Management that will manage endpoint devices centrally and efficiently. This SaaS solution will provide features such as security policy enforcement, device monitoring, and automatic software updates. The SaaS implementation is expected to reduce the cost and time needed to manage endpoint devices, thereby increasing the productivity and focus of companies on their core business. This research contributes to the development of an endpoint device management system using a SaaS approach with Citrix Endpoint Management. The results are expected to provide guidance to other companies facing similar challenges in optimizing the management of their endpoint devices.

Keywords: endpoint device, management, software-as-a service, citrix

Abstrak

Pengelolaan perangkat *endpoint* memberikan dampak yang signifikan terhadap efisiensi dan produktivitas perusahaan. Perusahan dalam bidang teknologi informasi harus siap dalam menghadapi tantangan mengelola perangkat *endpoint* yang semakin kompleks dan bervariasi. Penelitian ini bertujuan untuk merancang sebuah solusi *Software as a Service* (SaaS) menggunakan *Citrix Endpoint Management* guna mengatasi tantangan tersebut. Penelitian ini mengadopsi metode kualitatif dengan pendekatan studi kasus. Data dikumpulkan melalui wawancara serta observasi infrastruktur IT yang ada. Studi pustaka juga dilakukan untuk mendapatkan informasi tentang konsep pengelolaan perangkat *endpoint*, SaaS, dan *Citrix Endpoint Management*. Hasil penelitian berupa desain SaaS menggunakan *Citrix Endpoint Management* yang akan mengelola perangkat

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 04 NOMOR 02 JULI 2024
ISSN 2774 – 5775 | eISSN 2774-5767

endpoint secara terpusat dan efisien. Solusi SaaS ini akan menyediakan fitur-fitur seperti penerapan kebijakan keamanan, monitoring perangkat, dan pembaruan perangkat lunak otomatis. Implementasi SaaS diharapkan dapat mengurangi biaya dan waktu yang dibutuhkan untuk mengelola perangkat *endpoint*, sehingga dapat meningkatkan produktivitas dan fokus perusahaan pada inti bisnis mereka. Penelitian ini memberikan kontribusi dalam pengembangan sistem pengelolaan perangkat *endpoint* menggunakan pendekatan SaaS dengan *Citrix Endpoint Management*. Hasilnya diharapkan dapat memberikan panduan bagi perusahaan lain yang menghadapi tantangan serupa dalam mengoptimalkan pengelolaan perangkat *endpoint* mereka.

Kata Kunci: perangkat *endpoint*, *software-as-a-service*, pengelolaan perangkat, citrix

A. PENDAHULUAN

Saat ini, Tim IT menghadapi tantangan dalam memahami dampak lingkungan kerja baru, yaitu *Work From Anywhere* (WFA). Konsep *Work From Anywhere* (WFA) telah mengubah lanskap kerja global, sehingga perusahaan harus menyesuaikan pengelolaan sumber daya teknologi informasi mereka. Tim IT, sebagai pihak yang bertanggung jawab atas keamanan dan kinerja infrastruktur IT perusahaan, kini menghadapi tantangan besar dalam memahami dan mengelola efek dari lingkungan kerja yang lebih fleksibel dan tersebar ini.

Software as a Services (SaaS) merupakan kemampuan yang diberikan kepada pengguna dalam menggunakan aplikasi penyedia yang berjalan pada infrastruktur *cloud*. Aplikasi tersebut dapat diakses dari berbagai perangkat pengguna melalui antarmuka seperti *browser* web (misalnya, email berbasis web), atau antarmuka program. Pengguna tidak mengelola atau mengontrol infrastruktur *cloud* yang mendasarinya termasuk jaringan, *server*, sistem operasi, penyimpanan, atau bahkan kemampuan aplikasi individu, dengan kemungkinan pengecualian pengaturan konfigurasi aplikasi khusus pengguna yang terbatas (Miyachi, 2018).

Cloud publik adalah lingkungan multitenant di mana pengguna akhir membayar untuk penggunaan sumber daya pada jaringan sumber daya komoditas bersama dengan pengguna lain. Pengguna akhir tidak memiliki visibilitas ke lokasi fisik tempat perangkat lunak mereka berjalan selain di mana pusat data berada. Lapisan abstraksi dibangun di atas perangkat keras fisik dan diekspos sebagai API kepada pengguna akhir, yang memanfaatkan API ini untuk membuat sumber daya komputasi virtual yang berjalan di kumpulan sumber daya yang digunakan bersama oleh banyak pengguna. (Kavis, 2014)

Pengelolaan perangkat *endpoint* adalah tugas utama bagi Tim IT karena perangkat seperti PC, Laptop, Smartphone, dan Tablet merupakan sarana utama bagi pengguna akhir untuk mengakses sumber daya perusahaan (Adame, 2021). Salah satu alasan penting untuk mengelola *endpoint* adalah memastikan perangkat tersebut memenuhi konfigurasi dasar tertentu yang diperlukan untuk mengurangi risiko ancaman. Kesalahan konfigurasi tetap menjadi salah satu dari lima penyebab utama pelanggaran data menurut laporan investigasi pelanggaran data verizon 2020 (Agustina & Nasution, 2023), menekankan pentingnya pengelolaan *endpoint* yang efektif untuk melindungi data sensitif perusahaan.

Selain itu, pengelolaan dan konfigurasi *endpoint* juga penting untuk memastikan Tim IT dapat melaksanakan tanggung jawab

utama mereka, seperti penyebaran dan pembaruan perangkat lunak, dukungan sistem operasi, serta dukungan jarak jauh dan pemecahan masalah pada perangkat endpoint. Kurangnya pengelolaan yang tepat dapat menyulitkan pemantauan perangkat *endpoint* pengguna yang bekerja dari mana saja (*Work From Anywhere/WFA*) (Adame, 2021). Peran Tim IT sangat krusial dalam mengelola perangkat *endpoint* perusahaan dan memastikan visibilitas yang memadai terhadap perangkat tersebut, baik yang berada di dalam maupun di luar kantor.

Endpoint Security merupakan perlindungan keamanan sistem perangkat *endpoint* dari penggunaan, akses, dan / atau kontrol yang tidak sah. Contoh sistem untuk perlindungan perangkat *endpoin*t termasuk sistem *anti-malware*, sistem otentikasi pengguna, sistem enkripsi, sistem privasi, layanan penyaringan spam, dan sejenisnya (Schafer, 2021). Dengan demikian dapat disimpulkan bahwa *Endpoint Security* adalah perlindungan keamanan sistem perangkat endpoint dari akses dan kontrol yang tidak sah. Konsep *Work From Anywhere* (WFA) telah mengubah lanskap kerja global, sehingga perusahaan harus menyesuaikan pengelolaan sumber daya teknologi informasi mereka. Tim IT, sebagai pihak yang bertanggung jawab atas keamanan dan kinerja infrastruktur IT perusahaan, kini menghadapi tantangan besar dalam memahami dan mengelola efek dari lingkungan kerja yang lebih fleksibel dan tersebar ini(Ngo et al., 2023).

Alasan lain untuk mengelola dan mengonfigurasi *endpoint* adalah untuk memastikan bahwa Tim IT dapat melaksanakan tanggung jawab utama seperti penyebaran dan pembaruan perangkat lunak, dukungan sistem operasi, serta dukungan jarak jauh dan pemecahan masalah pada perangkat endpoint. Apabila perangkat *endpoint* tidak dikelola dengan baik, Tim IT mungkin akan kesulitan memantau perangkat *endpoint* pengguna yang bekerja dari mana saja (WFA) (Adame, 2021). Peran Tim IT sangat penting dalam mengelola perangkat *endpoint* perusahaan dan harus memiliki visibilitas yang memadai terhadap perangkat tersebut, baik di dalam maupun di luar jaringan perusahaan.

Berdasarkan latar belakang yang telah diuraikan di atas, dapat disimpulkan bahwa fokus penelitian ini adalah mengelola perangkat *endpoint* dengan merancang *Software as a Service* (SaaS) menggunakan *Citrix Endpoint Management*.

B. METODE PENELITIAN

Metode penelitian adalah panduan penting untuk membantu menghasilkan data yang akurat, objektif, dan dapat diandalkan. Untuk merancang solusi *Cloud Software as a Service (SaaS)* yang kompleks, diperlukan metode pengembangan yang mampu melakukan analisis mendalam sehingga desain solusi lebih tepat. Penelitian ini menggunakan pendekatan kualitatif deskriptif, yang melibatkan pengumpulan data, analisis, dan pemaparan hasil pengamatan di lapangan (Sugiyono, 2021). Penelitian kualitatif lebih berfokus pada perspektif di mana peneliti mengumpulkan data berupa cerita rinci dari para informan dan menyampaikannya sesuai dengan bahasa dan pandangan mereka. Oleh karena itu, penelitian kualitatif sering disebut sebagai penelitian deskriptif. Observasi dilakukan dengan mengamati proses pengelolaan perangkat *endpoint* yang sedang berlangsung, untuk mempelajari cara pengelolaan perangkat tersebut, kendala yang dihadapi, dan proses yang terlibat dalam manajemen perangkat. Selain itu, wawancara dilakukan dengan pihak terkait, seperti manajer IT dan staf yang terlibat langsung dalam pengelolaan perangkat *endpoint,* untuk mendapatkan pemahaman mendalam tentang kebutuhan, masalah, dan harapan terkait pengelolaan perangkat endpoint.

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 04 NOMOR 02 JULI 2024
ISSN 2774 – 5775 | eISSN 2774-5767

C. HASIL DAN PEMBAHASAN

Saat ini sistem pengelolaan perangkat endpoint yang terfragmentasi. Tim IT menggunakan berbagai solusi untuk mengelola perangkat *Windows OS dan Mac OS*. Hal ini membuat Tim IT sulit untuk memantau dan mengelola perangkat secara efisien, serta meningkatkan kompleksitas dan risiko keamanan.

Sistem yang ada saat ini tidak mampu memberikan visibilitas *real-time* untuk semua perangkat *endpoint*. Tim IT harus mengandalkan laporan manual dari pengguna atau alat pengelolaan terpisah untuk memperoleh informasi tentang status perangkat. Hal ini menyulitkan pemantauan dan pengelolaan perangkat secara efisien, serta meningkatkan risiko keamanan.

Selain itu, sistem tidak mampu memberikan manajemen yang efisien untuk berbagai sistem operasi. Tim IT harus menggunakan solusi berbeda untuk masing-masing sistem operasi, yang mempersulit upaya pengelolaan yang efisien. Hal ini menghabiskan waktu dan sumber daya yang berharga, serta meningkatkan kompleksitas dan kemungkinan kesalahan manusia dalam mengelola perangkat. Sistem yang ada juga tidak mampu memberikan keamanan yang kokoh untuk melindungi perangkat. Dalam skenario *Work From Anywhere* (WFA), banyak perangkat beroperasi di luar jaringan internal perusahaan, meningkatkan risiko keamanan. Tanpa sistem pengelolaan yang terintegrasi dan responsif, Tim IT kesulitan menerapkan kebijakan keamanan yang konsisten dan memastikan perlindungan yang baik untuk semua perangkat endpoint. Ini dapat meningkatkan risiko serangan malware, kebocoran data, atau akses tidak sah ke aplikasi bisnis yang sensitif.

Model Layanan *Cloud Computing Software as a Service (SaaS)* dalam penggunaannya untuk manajemen perangkat *endpoint* terus mengalami perkembangan. Konsep *Bring-Your-Own-Device* (BYOD) adalah konsep yang memungkinkan karyawan menggunakan perangkat seluler pribadi mereka untuk mengakses dan mengelola data perusahaan dari mana saja dan kapan saja. BYOD dapat meningkatkan produktivitas karyawan dan menghemat biaya bagi organisasi.

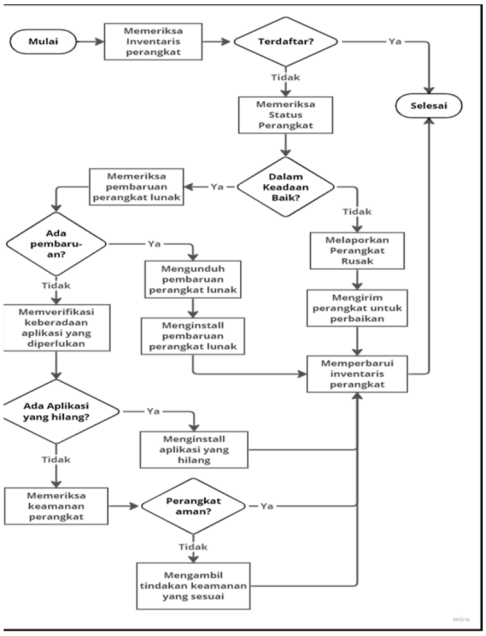
Manajemen perangkat seluler (MDM) adalah skema penerapan dan manajemen perusahaan untuk perangkat seluler seperti telepon seluler dan tablet. Skema ini umumnya terdiri dari kebijakan dan aplikasi, dengan aplikasi yang terakhir digunakan untuk mengelola kebijakan yang membatasi hak pemasangan aplikasi seluler karyawan dan menerapkan protokol keamanan. Pembatasan ini dirancang untuk menerapkan pembaruan keamanan, mengurangi risiko *malware*, dan mengurangi risiko pengungkapan data non-publik, termasuk informasi yang dapat diidentifikasi secara pribadi (PII) dan kekayaan intelektual (Hayes et al., 2020).

Manajemen aplikasi seluler (MAM) menjelaskan perangkat lunak dan layanan yang bertanggung jawab untuk menyediakan dan mengontrol akses ke aplikasi seluler yang dikembangkan secara internal dan yang tersedia secara komersial yang digunakan dalam lingkungan bisnis. Strategi ini dimaksudkan untuk mengimbangi risiko keamanan dari strategi kerja *Bring Your Own Device* (BYOD). Ketika seorang karyawan membawa perangkat pribadi ke dalam lingkungan perusahaan, MAM memungkinkan staf TI perusahaan untuk mentransfer aplikasi yang diperlukan, mengontrol akses ke data bisnis, dan menghapus data bisnis yang tersimpan secara lokal dari perangkat tersebut jika perangkat tersebut hilang, atau ketika pemiliknya tidak lagi bekerja di perusahaan. Kontainerisasi adalah solusi keamanan BYOD alternatif. Daripada mengontrol seluruh perangkat karyawan, aplikasi *containerisation* membuat kantong yang terisolasi dan aman yang terpisah dari semua data pribadi. Kontrol perusahaan atas perangkat hanya

meluas ke wadah tersebut saja (Salama et al., 2020).

Client Management Tools (CMT) digunakan untuk mengotomatisasi tugas-tugas manajemen titik akhir. CMT dapat melakukan fungsi-fungsi berikut ini: penyebaran sistem operasi, membuat inventaris perangkat keras dan perangkat lunak, distribusi perangkat lunak, manajemen tambalan, manajemen konfigurasi, manajemen konfigurasi keamanan, dan kendali jarak jauh (Schafer, 2021).

Untuk mengatasi masalah-masalah ini, dibutuhkan solusi terintegrasi yang mampu menyediakan visibilitas real-time, manajemen yang efisien, dan keamanan yang kuat untuk semua perangkat *endpoint. flowchart* pengelolaan perangkat *endpoint* yang sedang berjalan.



Gambar 1. Flowchart Pengelolaan Perangkat

Pada gambar 1 diatas dapat dijelaskan mengenai alur proses pengelolaan perangkat *endpoint* perusahaan yang masih dilakukan secara manual: (1). Proses dimulai dengan pemeriksaan inventaris perangkat endpoint. Jika perangkat belum terdaftar, maka perangkat tersebut ditambahkan ke dalam inventaris; (2). Jika perangkat sudah terdaftar, langkah selanjutnya adalah memeriksa status perangkat. Jika perangkat rusak, maka perangkat dilaporkan dan dikirim untuk perbaikan, kemudian inventaris diperbarui; (3). Jika perangkat dalam kondisi baik, dilakukan pemeriksaan pembaruan perangkat lunak. Jika ada pembaruan, perangkat lunak tersebut diunduh dan diinstal, lalu inventaris diperbarui; (4). Jika tidak ada pembaruan perangkat lunak, dilakukan verifikasi keberadaan aplikasi yang diperlukan. Jika ada aplikasi yang hilang, maka aplikasi tersebut diinstal dan inventaris diperbarui. Jika semua aplikasi telah terpasang, dilakukan pemeriksaan keamanan perangkat; (5). Jika perangkat tidak aman, tindakan keamanan yang sesuai diambil dan inventaris diperbarui. Jika perangkat aman, inventaris diperbarui; (6). Proses pengelolaan perangkat endpoint berakhir. Flowchart ini memberikan gambaran tentang langkah-langkah yang harus diikuti dalam pengelolaan perangkat endpoint perusahaan yang masih dilakukan secara manual.

Permasalahan yang ada saat ini telah dianalisa dengan menggunakan analisis SWOT. Analisis SWOT adalah metode untuk mengidentifikasi kekuatan, kelemahan, peluang, dan ancaman dalam suatu entitas. Dengan mempertimbangkan faktor internal dan eksternal, SWOT membantu merumuskan strategi guna mencapai tujuan dan mengatasi tantangan. Analisis SWOT dapat dilihat pada gambar 2. berikut ini

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 04 NOMOR 02 JULI 2024
ISSN 2774 – 5775 | eISSN 2774-5767

INTERNAL / EKSTERNAL	Strenght	Weakness
	• Memiliki pengetahuan dan pemahaman yang mendalam tentang teknologi dan infrastruktur IT. • Memiliki basis karyawan yang memiliki pengalaman dan keahlian di bidang IT.	• Kondisi pengelolaan perangkat endpoint yang tidak terpusat • Tuntutan Fleksibilitas WFA untuk karyawan tertentu menyebabkan keamanan perusahaan menjadi lebih berisiko. • Tim IT tidak memiliki visibilitas dalam monitoring perangkat dalam skenario WFA • Kompleksitas perangkat endpoint membuat operasional pengelolaan menjadi lebih rumit
Opportunities	**SO Strategy**	**WO Strategy**
• Sistem SaaS dapat meningkatkan efisiensi operasional pengelolaan perangkat endpoint. • Sistem SaaS memungkinkan Tim IT memiliki visibilitas terhadap perangkat endpoint secara real-time • Sistem SaaS dapat memantau, mengontrol perangkat endpoit lintas OS dalam single console. • Sistem SaaS memungkinkan Tim IT melakukan Push Policy jarak jauh untuk memastikan perangkat patuh terhadap aturan perusahaan.	• Memanfaatkan keahlian dan pengalaman sebagai perusahaan IT services solution untuk mengembangkan solusi SaaS yang dapat memenuhi kebutuhan pengelolaan perangkat endpoint lintas OS yang efisien & memiliki visibilitas.	• Memanfaatkan Sistem SaaS untuk mengelola kompleksitas perangkat endpoint secara terpusat sehingga lebih efisien. • Memanfaatkan Sistem SaaS untuk memastikan perangkat yang digunakan karyawan dalam skenario WFA patuh terhadap aturan perusahaan. • Memanfaatkan Sistem SaaS untuk menyederhanakan pengelolaan perangkat endpoint. • Memanfaatkan Sistem SaaS agar Tim IT dapat melakukan Push Policy jarak jauh untuk memastikan perangkat patuh terhadap aturan perusahaan.
Threat	**ST Strategy**	**WT Strategy**
1. Perkembangan teknologi yang cepat 2. Pihak diluar perusahaan juga memiliki kontrol terhadap sumber daya sistem SaaS	• Melakukan verifikasi ketat & evaluasi secara berkala terhadap anomali sistem SaaS • Melakukan verifikasi & evaluasi ketat terhadap system administrator sebagai pihak yang bertanggung jawab terhadap kinerja sistem SaaS	• Memanfaatkan Sistem SaaS untuk mengelola kompleksitas perangkat endpoint secara terpusat sehingga lebih efisien. • Memanfaatkan Sistem SaaS untuk memastikan perangkat yang digunakan karyawan dalam skenario WFA patuh terhadap aturan perusahaan. • Melakukan enkripsi untuk menghindari akses yang tidak sah terhadap intergritas data yang berhubungan dengan sistem SaaS

Gambar 2. Analisis SWOT

Berdasarkan analisis SWOT yang dilakukan, dapat disimpulkan bahwa perusahaan memiliki kekuatan dalam pengetahuan teknologi dan infrastruktur IT yang mendalam, serta memiliki karyawan yang berpengalaman di bidang tersebut. Namun, ada beberapa kelemahan yang perlu diatasi, seperti pengelolaan perangkat endpoint yang tidak terpusat, peningkatan risiko keamanan akibat tuntutan fleksibilitas WFA, dan kompleksitas dalam pengelolaan perangkat endpoint.

Peluang yang ada meliputi pemanfaatan sistem SaaS untuk meningkatkan efisiensi operasional dalam pengelolaan perangkat endpoint, memberikan visibilitas real-time kepada tim IT, mengontrol perangkat endpoint lintas OS dalam satu konsol, dan melakukan pengaturan kebijakan jarak jauh. Meskipun ancaman seperti perkembangan teknologi yang cepat dan kontrol eksternal terhadap sumber daya sistem SaaS ada, perusahaan dapat mengembangkan solusi SaaS yang efisien dengan memanfaatkan keahlian dan pengalaman mereka dalam bidang solusi layanan IT.

Strategi yang direkomendasikan adalah menggunakan sistem SaaS untuk mengelola kompleksitas perangkat endpoint secara terpusat, memastikan kepatuhan perangkat dalam skenario WFA, serta melakukan verifikasi dan evaluasi ketat terhadap sistem SaaS dan administratornya. Selain itu, langkah-langkah keamanan seperti enkripsi juga perlu diterapkan untuk melindungi integritas data yang terkait dengan sistem SaaS.

SaaS Citrix Endpoint Management

Software as a Service (SaaS) adalah solusi yang dirancang untuk mengotomatiskan proses pengelolaan perangkat endpoint. Sistem ini menggantikan metode pengelolaan yang masih dilakukan secara terpisah atau manual dengan menyediakan platform terpusat yang mampu mengelola semua perangkat endpoint dalam satu lokasi.

Citrix Cloud Connector merupakan penghubung antara layanan Citrix Cloud dengan lokasi sumber daya. Sumber daya yang digunakan, misalnya Microsoft Azure Public Cloud (Viitanen, 2020).

Dalam rancangan SaaS ini, *Citrix Endpoint Management (CEM*) akan digunakan sebagai Cloud Service untuk mengelola perangkat endpoint seperti ponsel, tablet, laptop, dan perangkat lainnya secara efisien dan aman. Sistem ini memberikan kontrol penuh kepada administrator IT untuk memantau, mengelola, dan mengamankan perangkat endpoint dari satu titik akses terpusat.

Rancangan *Software as a Service (SaaS) Citrix Endpoint* Management memiliki fitur-fitur berikut: (1).Pengelolaan Perangkat Endpoint*: SaaS Citrix Endpoint Management* memungkinkan admin IT untuk mendaftarkan dan mengelola perangkat endpoint dari berbagai platform; (2). Pengiriman Aplikasi Secara Terpusat: Dengan *SaaS Citrix Endpoint Management*, admin IT dapat mengirim dan mengelola aplikasi perusahaan secara terpusat ke perangkat *endpoint* yang sesuai; (3). Pengelolaan Kebijakan Keamanan: *SaaS Citrix Endpoint Managemen*t memungkinkan admin IT untuk menerapkan kebijakan

keamanan yang konsisten dan standar di semua perangkat endpoint; (4). Monitoring dan Pelaporan: Sistem ini menyediakan fitur pemantauan real-time untuk melacak kinerja perangkat endpoint dan mendiagnosis masalah potensial; (5). Penyelesaian Masalah Jarak Jauh: Dengan *SaaS Citrix Endpoint Management*, admin IT dapat mengelola perangkat endpoint dan menyelesaikan masalah secara jarak jauh.

Keuntungan mengelola perangkat endpoint menggunakan SaaS Citrix Endpoint Management antara lain: Efisiensi operasional; Keamanan yang ditingkatkan; Pengalaman pengguna yang lebih baik; (4). Pembaruan dan Penyesuaian yang Mudah; (5). Skalabilitas dan Fleksibilitas: (6). Dengan *SaaS Citrix Endpoint Management*, dapat mengoptimalkan pengelolaan perangkat endpoint, menghemat waktu, meningkatkan keamanan, dan meningkatkan efisiensi operasional

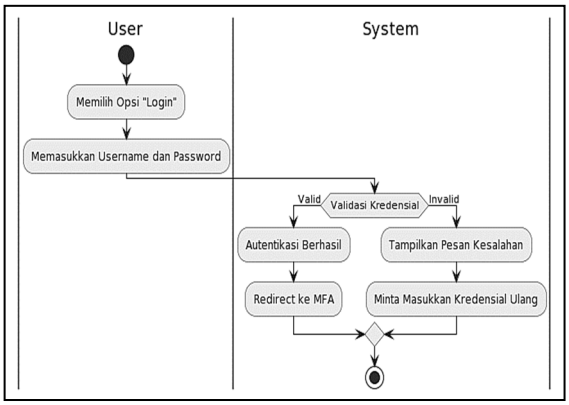
Fungsi dan Aktivitas Sistem SaaS

Use case diagram menggambarkan bagaimana sistem yang diusulkan akan beroperasi dan memenuhi kebutuhan pengguna. Selain itu, diagram ini membantu menggambarkan interaksi antara aktor-aktor yang terlibat dalam penggunaan sistem SaaS yang dirancang, yaitu *SaaS Citrix Endpoint Managemen*t, untuk mengelola perangkat endpoint, gambar Use case digram dapat dilihat pada gambar 3 berikut ini :

Gambar 3. Use case diagram

1. *Login*

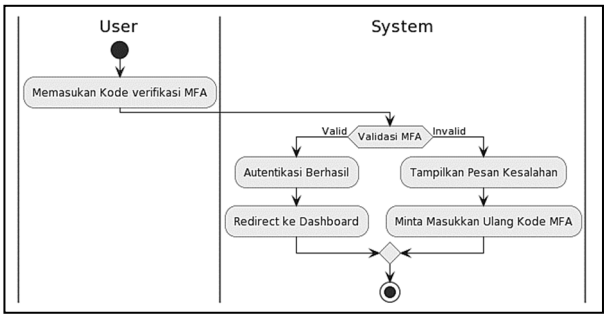
Activity diagram ini menunjukkan langkah-langkah untuk melakukan proses *login* ke sistem SaaS *Citrix Endpoint Management*



Gambar 4. Login

2. *Multi-Factor Authenticator* (MFA)

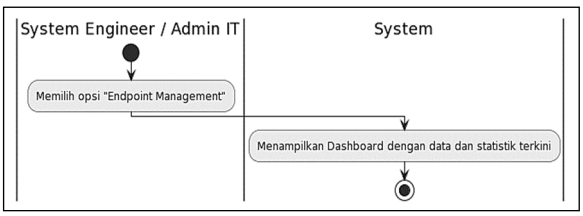
Pada *activity diagram* ini, akan dijelaskan bagaimana sistem SaaS *Citrix Endpoint Management* menerapkan metode autentikasi MFA untuk meningkatkan keamanan.



Gambar 5. *Multi-Factor Authenticator* (MFA)

3. *SaaS Citrix Endpoint Management (CEM)*

Activity diagram ini menunjukan bagaimana mengakses sistem SaaS CEM dari sistem *Citrix Cloud Services*.

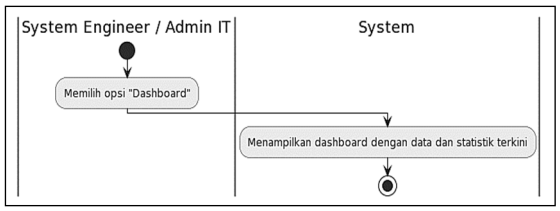


Gambar 6. SaaS CEM

JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 04 NOMOR 02 JULI 2024
ISSN 2774 – 5775 | eISSN 2774-5767

4. *Dashboard*

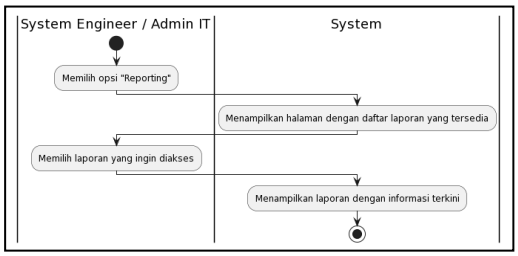
Activity diagram ini menunjukan bagaimana mengakses tampilan *dashboard* dari *sistem SaaS Citrix Endpoint Management*.



Gambar 7. *Dashboard*

5. *Reporting*

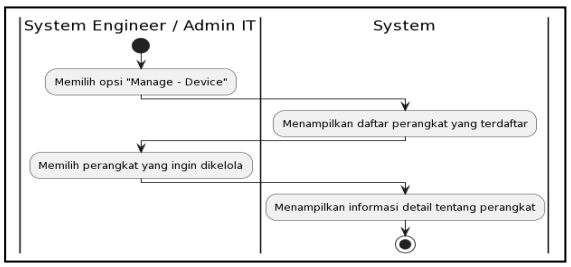
Activity diagram ini, menunjukan bagaimana sistem SaaS *Citrix Endpoint Management* menyediakan fitur pelaporan yang berguna untuk analisis dan *monitoring.*



Gambar 8. *Reporting*

6. *Manage Device*

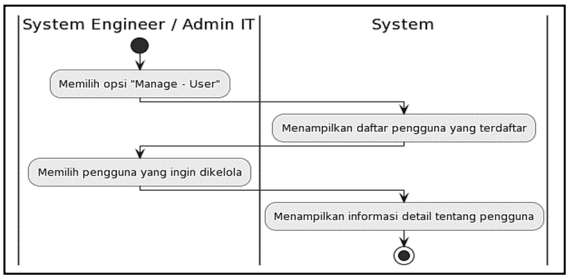
Activity diagram ini menjelaskan tentang bagaimana aktor dapat mengelola perangkat yang terhubung ke sistem SaaS *Citrix Endpoint Management.*



Gambar 9. *Manage Devices*

7. *Manage User*

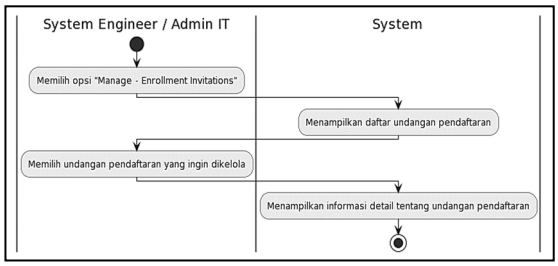
Pada *activity diagram* ini, menunjukan langkah-langkah untuk mengelola akun pengguna dalam sistem SaaS *Citrix Endpoint Management.*



Gambar 10. *Manage User*

8. *Manage Enrollment Invitations*

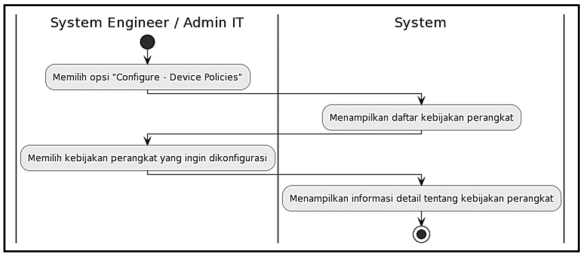
Activity diagram ini menunjukkan proses mengelola undangan pendaftaran yang dikirimkan kepada pengguna untuk mengakses sistem SaaS *Citrix Endpoint Management.*



Gambar 11.*Manage Enrollment Invitations*

9. *Configure Device Policies*

Pada *activity diagram* ini, menjelaskan langkah-langkah untuk mengonfigurasi kebijakan perangkat dalam sistem SaaS *Citrix Endpoint Management.*



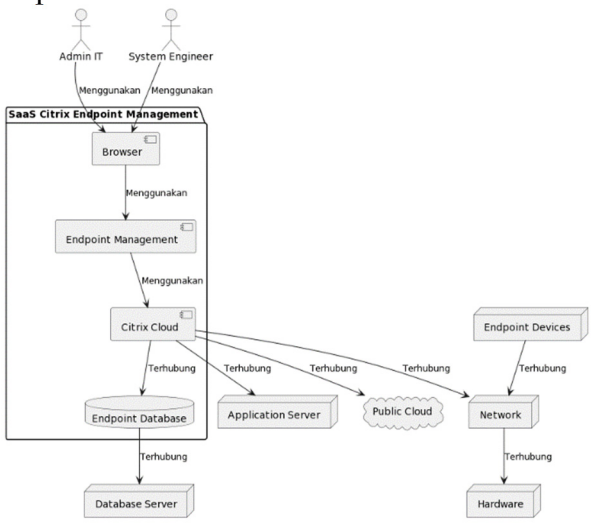
Gambar 12. *Configure Devices Policies*

Arsitektur

Dengan menggunakan *deployment diagram*, dapat dengan mudah memahami bagaimana komponen-komponen saling berinteraksi dalam sistem dan bagaimana infrastruktur mendukung operasional sistem secara efisien.

Deployment diagram sistem *SaaS Citrix Endpoint Management* menunjukkan

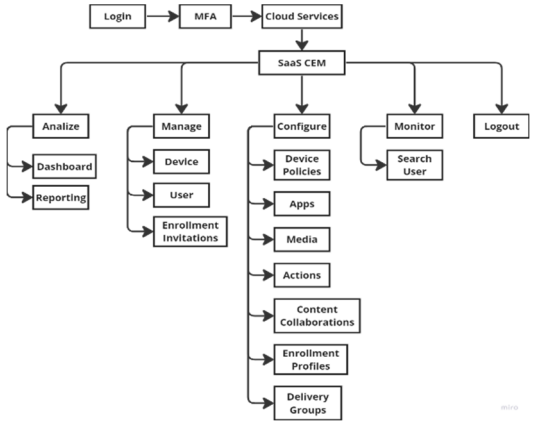
penempatan komponen perangkat keras dan perangkat lunak dalam sistem. Diagram ini memvisualisasikan interaksi antara komponen-komponen tersebut dan memberikan panduan visual yang jelas untuk implementasi sistem.



Gambar 13. Arsitektur SaaS

Struktur Tampilan

Struktur tampilan digunakan untuk menjelaskan hirarki dari semua tampilan yang dirancang. Struktur tampilan system SaaS Citrix Endpoint Management akan di jelaskan menggunakan deployment diagram sebagai berikut.

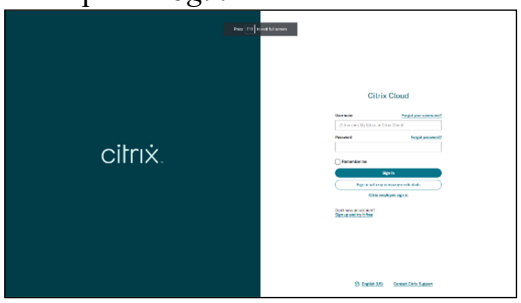


Gambar 14. Struktur Tampilan

Struktur Layar

Berikut merupakan tampilan layar dari SaaS *Citrix Endpoint Management*

1. Tampilan *Login*

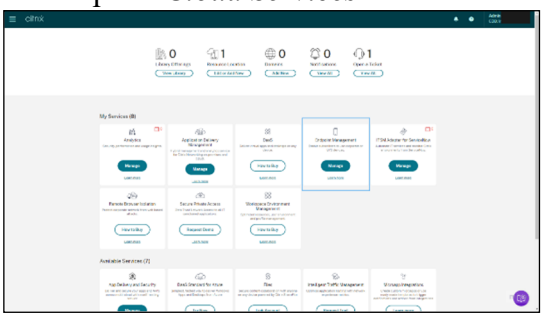


Gambar 15. *Login Page*

2. Tampilan *Multi-Factor Authenticator* (MFA)

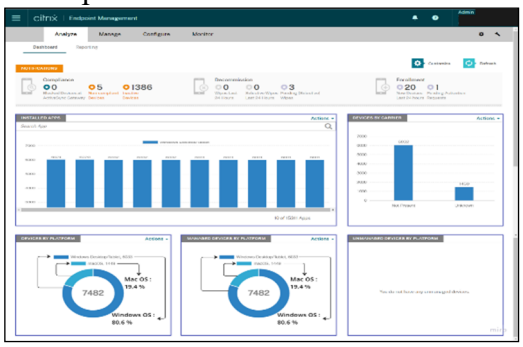
Gambar 16. *Multi-factor Authentication*

3. Tampilan *Cloud Services*



Gambar 17. *Beranda Citrix Cloud Services*

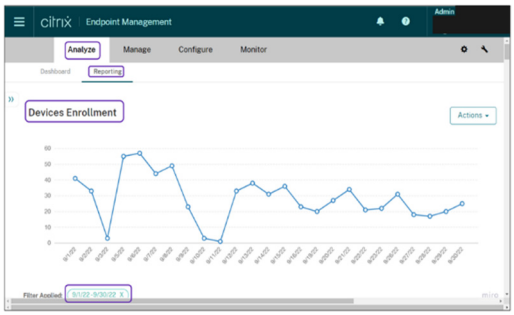
4. Tampilan *Dashboard*



Gambar 18. *Dashboard SaaS CEM*

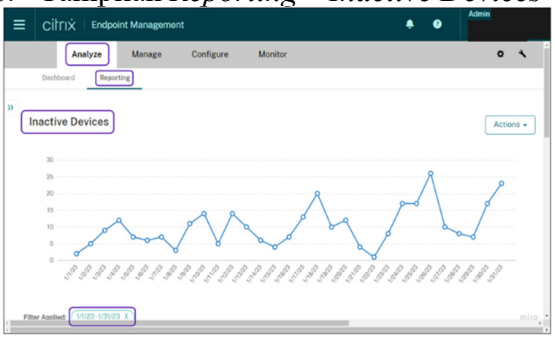
JURNAL ELEKTRO & INFORMATIKA
SWADHARMA (JEIS)
VOLUME 04 NOMOR 02 JULI 2024
ISSN 2774 – 5775 | eISSN 2774-5767

5. Tampilan *Reporting – Enrollment Devices*



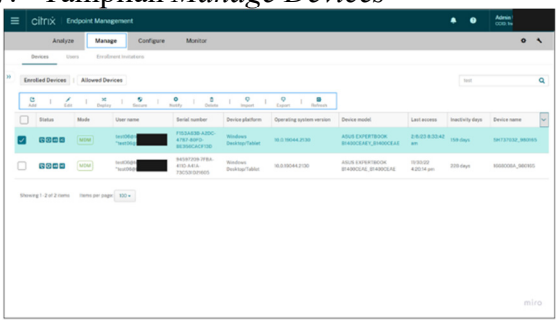
Gambar 19. *Reporting - Enrollment Devices*

6. Tampilan *Reporting – Inactive Devices*



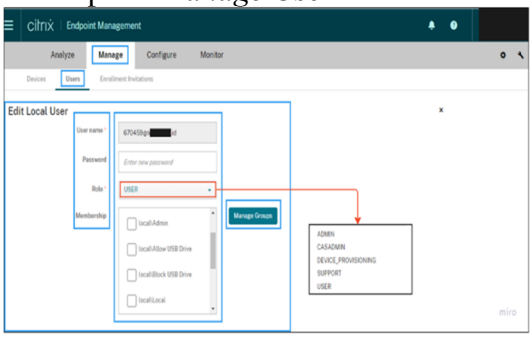
Gambar 20. *Reporting – Inactive Devices*

7. Tampilan *Manage Devices*



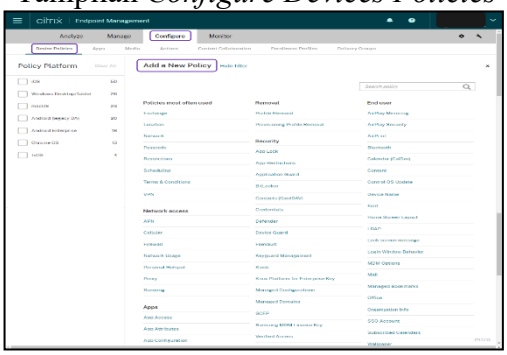
Gambar 21. *Manage Devices*

8. Tampilan *Manage User*



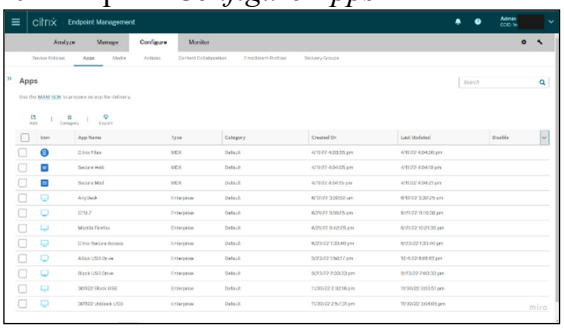
Gambar 22. *Manage User*

9. Tampilan *Configure Devices Policies*



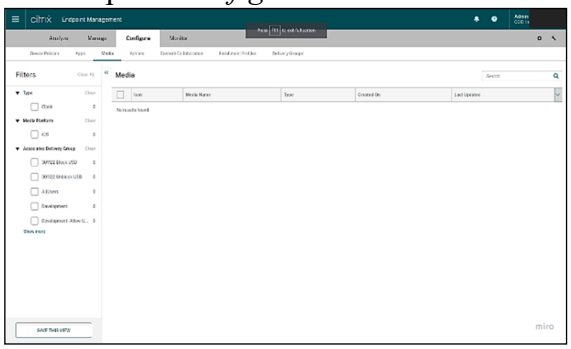
Gambar 23. *Configure Device Policies*

10. Tampilan *Configure Apps*



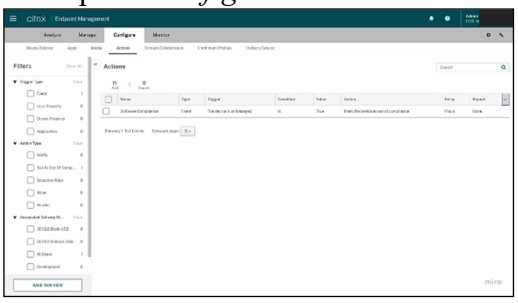
Gambar 24. *Configure Apps*

11. Tampilan *Configure Media*



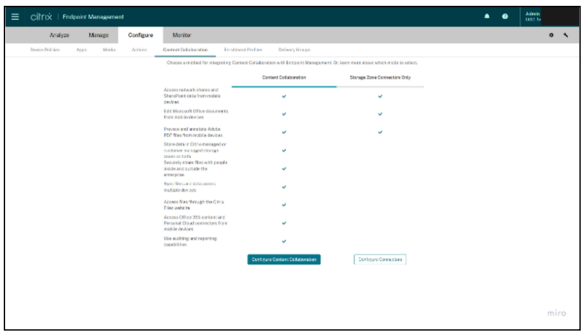
Gambar 25. *Configure Media*

12. Tampilan *Configure Actions*



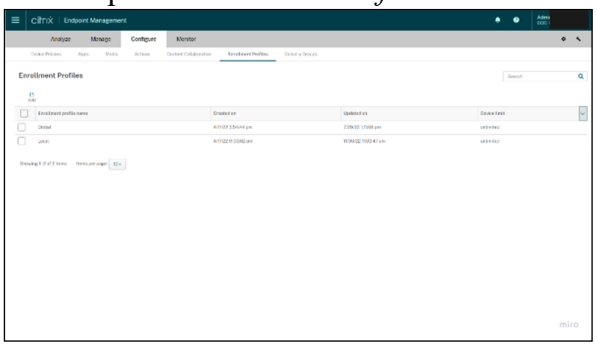
Gambar 26. *Configure Actions*

13. Tampilan *Configure Content Collaborations*



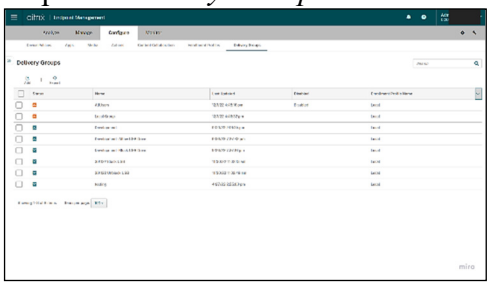
Gambar 27. *Configure Content Collaborations*

14. Tampilan *Enrollment Profiles*



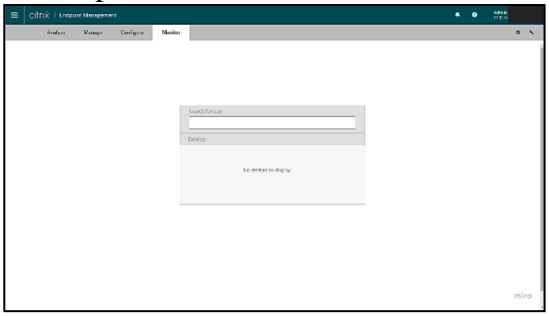
Gambar 28. *Enrollment Profiles*

15. Tampilan *Delivery Groups*



Gambar 29. *Delivery Groups*

16. Tampilan *Monitor – Search User*



Gambar 30. Monitor – Search Us

Dalam merancang *SaaS Citrix Endpoint Management* untuk mengelola sekitar 250 perangkat, berikut adalah analisis kebutuhan perangkat lunak:

1. *Citrix Cloud Connector*:
   a. Sistem SaaS memerlukan *Citrix Cloud Connector* untuk mengintegrasikan arsitektur Endpoint Management ke dalam infrastruktur eksisting.
   b. *Citrix Cloud Connector* harus menjadi member dari *Active Directory Domain* yang ada.
   c. *Citrix Cloud Connector* akan mengintegrasikan sumber daya infrastruktur yang berada di *On-Premise Data Center* ke *Citrix Endpoint Management Cloud Service* dengan aman melalui port HTTPS (443), LDAP, PKI *Server, internal DNS queries, dan enumerasi Citrix Workspace*.
2. Citrix Gateway:
   a. SaaS Citrix Endpoint Management memerlukan Citrix Gateway berupa 2 Virtual Machine (VM)
   b. Untuk skenario tersebut, diperlukan Citrix ADC VPX 2x3000Mbps untuk VPN atau akses corporate data.

Jika diperlukan mikro VPN untuk akses ke internal network resource untuk business apps yang akan di-wrap dengan teknologi Citrix MDX, maka Mikro VPN membutuhkan Citrix Gateway untuk terhubung ke infrastruktur back-end di internal.

D. PENUTUP

Berdasarkan permasalahan dan rancangan sistem yang telah dijelaskan, maka dari hasil penelitian ditemukan bahwa penggunaan Citrix Endpoint Management sebagai solusi SaaS adalah rancangan sistem yang relevan dan bermanfaat. Rancangan sistem ini memungkinkan pengelolaan perangkat endpoint perusahaan secara efisien

dan terpusat. Administrator dapat dengan mudah mengatur kebijakan keamanan, konfigurasi, pemantauan, dan pembaruan perangkat endpoint secara konsisten dan efektif. Penggunaan sistem ini membantu meningkatkan produktivitas tim IT dan mengurangi beban administratif terkait pengelolaan perangkat. Akses jarak jauh dan kompatibilitas dengan berbagai jenis perangkat memungkinkan karyawan bekerja produktif tanpa terikat oleh batasan fisik atau perangkat tertentu. Penggunaan Citrix Endpoint Management sebagai solusi SaaS akan meningkatkan efisiensi, keamanan, dan fleksibilitas dalam pengelolaan perangkat endpoint.

Hasil penelitian ini dapat menjadi landasan dalam merencanakan dan melaksanakan rancangan sistem tersebut untuk meningkatkan kinerja dan keamanan sistem informasi perusahaan. Dengan demikian, penggunaan SaaS Citrix Endpoint Management dianggap sebagai langkah yang tepat dan berpotensi memberikan manfaat signifikan. Evaluasi secara berkala terhadap sistem yang telah diimplementasikan sangat penting untuk mengidentifikasi area yang perlu diperbaiki atau ditingkatkan, serta melakukan pembaruan sistem secara teratur guna mengikuti perkembangan teknologi dan memenuhi kebutuhan yang terus berkembang.

E. DAFTAR PUSTAKA

Adame, D. (2021). Managing and Securing Endpoints: A Solution for a Telework Environment. *Electronic Theses, Projects, and Dissertations*, *1316*. https://scholarworks.lib.csusb.edu/etd/1316/

Agustina, D., & Nasution, M. I. P. (2023). Sistem Data Security pada Pembelajaran Online di Perguruan Tinggi. *IJM: Indonesian Journal of Multidisciplinary*, *1*(3), 1173–1179.

Hayes, D., Cappa, F., & Le-Khac, N. A. (2020). An Effective Approach to Mobile Device Management: Security and Privacy Issues Associated with Mobile Applications. *Digital Business*, *1*(1), 1–8. https://doi.org/10.1016/j.digbus.2020.100001

Kavis, M. J. (2014). *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)*. New Jersey : John Wiley & Sons Inc.

Lebek, B., Degirmenci, K., & Breitner, M. (2013). Investigating the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices. *Proceedings of the Nineteenth Americas Conference on Information Systems*, 1–8.

Miyachi, C. (2018). What is "Cloud"? It is time to update the NIST definition? *IEEE Cloud Computing*, *5*(03), 6–11.

Ngo, H. Q., Guo, M., & Nguyen, H. (2023). Near optimal strategies for honeypots placement in dynamic and large active directory networks. *Proceedings of the 2023 International Conference on Autonomous Agents and Multiagent Systems*, 2517–2519.

Salama, R., Uzunboylu, H., & Alkaddah, B. (2020). Distance learning system, learning programming languages by using mobile applications. *New Trends and Issues Proceedings on Humanities and Social Sciences*, *7*(2), 23–47.

Schafer, J. (2021). *Unified Endpoint Management Software for a Small Company*. Metropolia University of Applied Sciences.

Sugiyono. (2021). *Metode Penelitian Kuantitatif, Kualitatif dan R&D, Cetakan Ketiga*. Bandung : Alfabeta.

Viitanen, S. (2020). *Citrix Cloud multi-tenant resurssit hybrid cloud toteutus*. Hame University of Applied Sciences.