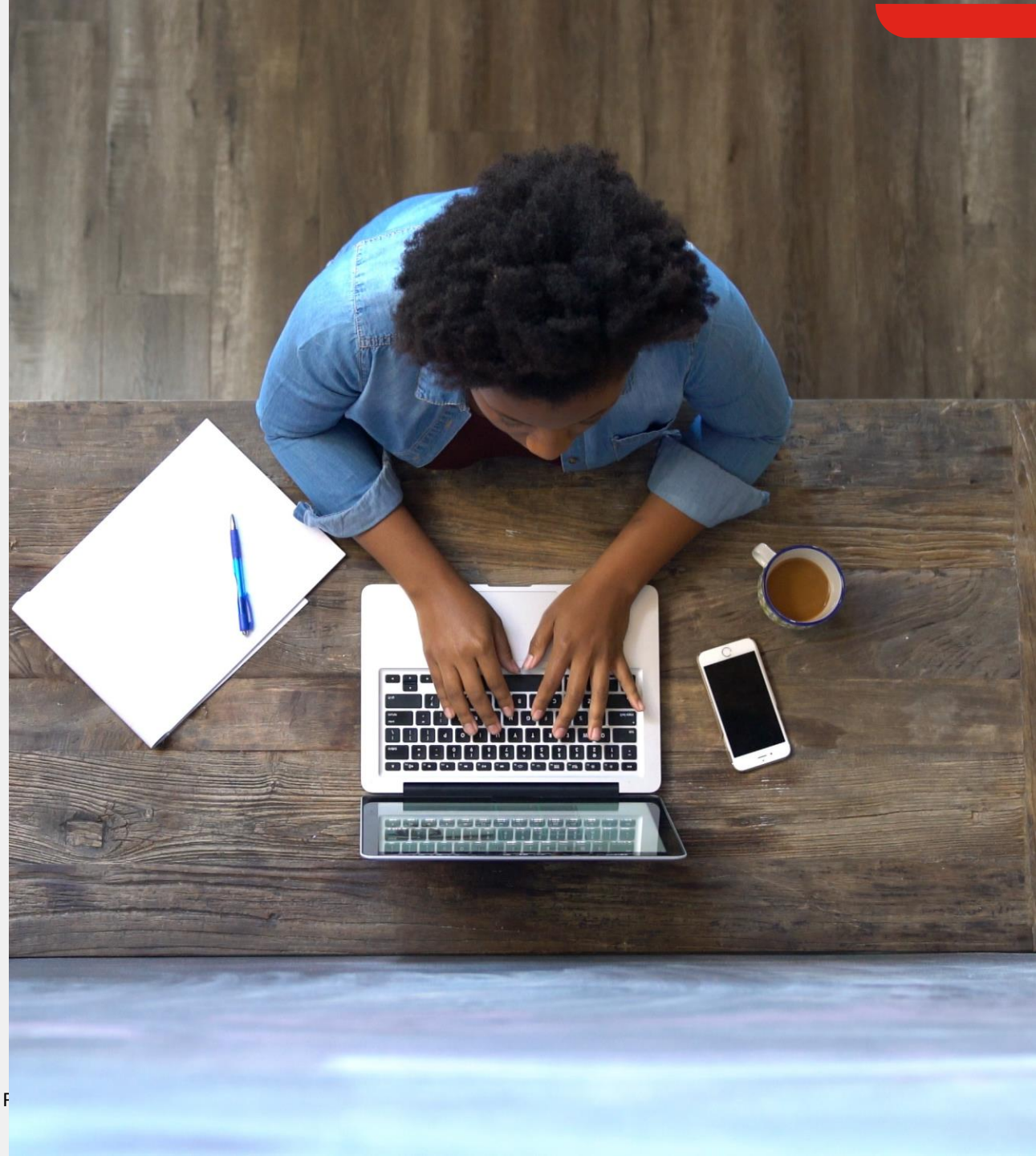
IAM.
Оркестрація доступу від принтерів та співробітників до підрядників.

Євгеній Таран, Systems Engineer
ytaran@fortinet.com

ЗМІСТ



IAM рішення від Fortinet

Fortinet Security Fabric

Кожен продукт самодостатній та разом вони творять магію автоматизації та спільної роботи

Комплексний підхід до безпеки

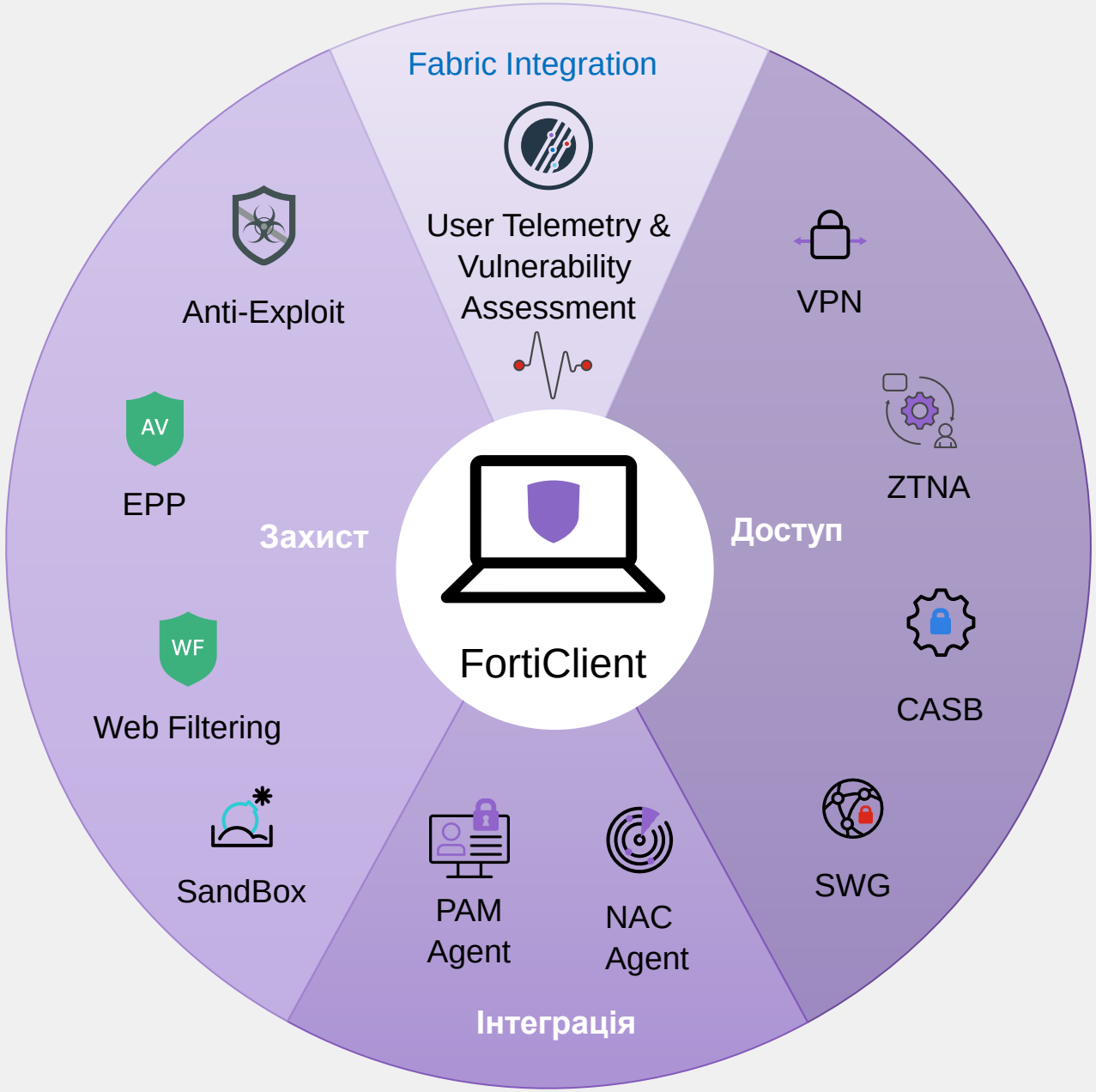
MITRE Pre-ATT&CK

MITRE ATT&CK

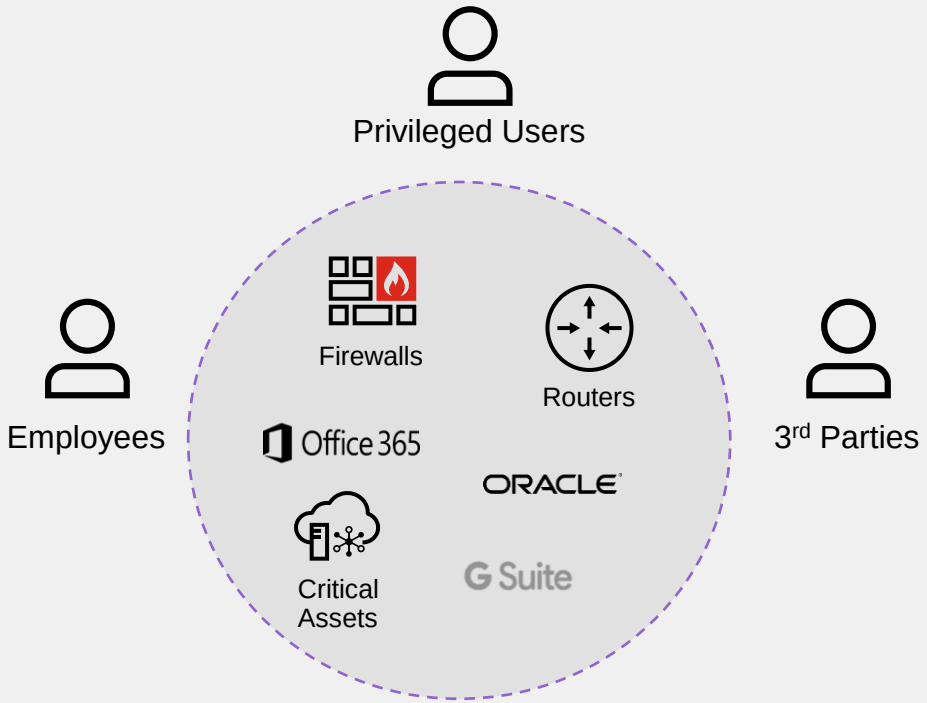
	Recon	Weapon	Delivery	Exploit	Installation	C2	Action
Продукти та рішення	FortiRecon FortiDeceptor	FortiRecon FortiDeceptor	FortiGate (HW/VM/CN/SASE) FortiProxy FortiClient FortiEDR FortiADC FortiWeb FortiNDR AV+ANN FortiMail FortiCASB FortiCWP	FortiGate (HW/VM/CN/SASE) FortiProxy FortiClient FortiEDR Defuse compromised endpoint FortiADC FortiWeb Web application FortiDeceptor Threat detection, analysis, and response FortiSIEM UEBA	FortiGate (HW/VM/CN/SASE) FortiClient FortiEDR Defuse exploit FortiDeceptor Defuse Lateral Movement FortiCWP FortiSIEM UEBA	FortiGate (HW/VM/CN/SASE) FortiClient FortiEDR Defuse compromised endpoint FortiNDR FortiSIEM UEBA	FortiAnalyzer Event handlers & reports FortiSIEM Rules Engine & Threat Hunting FortiSOAR Playbooks IOC Threat hunting Outbreak Detection ZTNA Auto tagging FortiClient Endpoint search FortiEDR|XDR FortiDeceptor Threat intelligence, & attack isolation
Сервіси FortiGuard та AI		Credential Stuffing Prevention Service	Anti-malware, AV pre-Filter, SBX, Endpoint Vulnerability Protection, App Control, IL CASB, Credentials AV · IL SBX · IL CASB	IPS, Application, FW, IOT, OT IPS · IoT · OT	URL, AV URL · AV	Botnet, C2, DNS BOT · C2 · DNS	
SOC	Знайте свої ризики та вразливості **Security Assessments**	Навчання SOC **IRR, Playbooks, Training**	Керуйте пошуком та знешкодженням **MDR**	Покращення SOC **SOC as a Service**	Швидка та ефективна відповідь **Incident Response**		

Один агент для всього*

- Єдиний агент для:
  - Доступу (ZTNA, VPN)
  - Захисту ПК (EPP)
  - SASE
  - Digital Experience (DEM)
  - Fabric Support (PAM, NAC, FortiWeb)

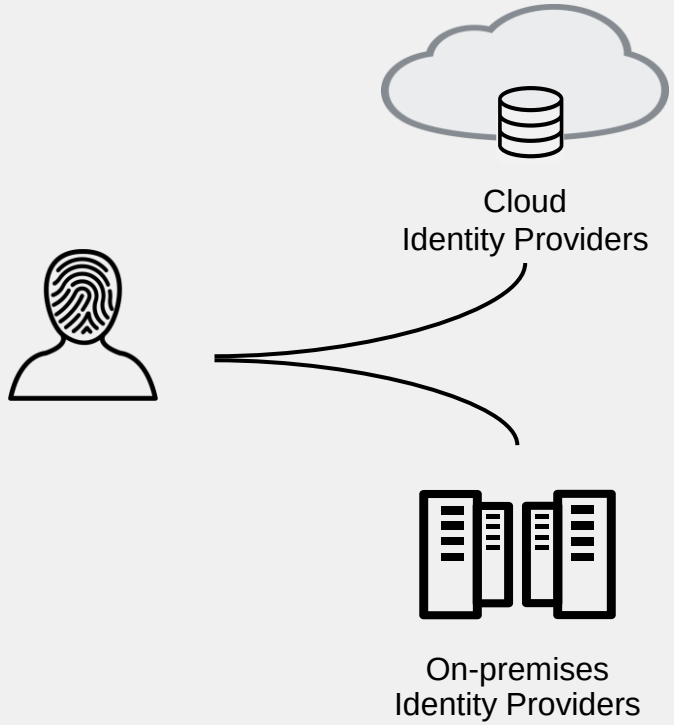


Тренди ідентифікації



Користувачі це - Новий Периметр

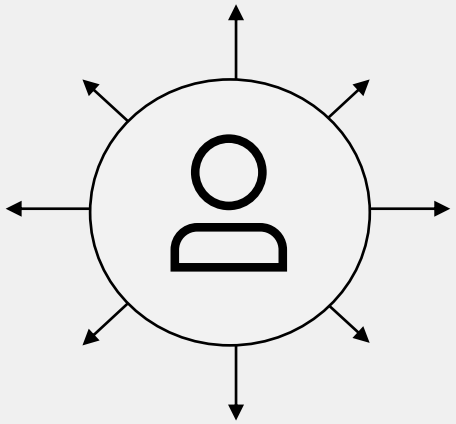
Користувачі **Звідусіль** отримують доступ до **Ресурсів**, збільшуючи поверхню атаки



Гібридні Середовища

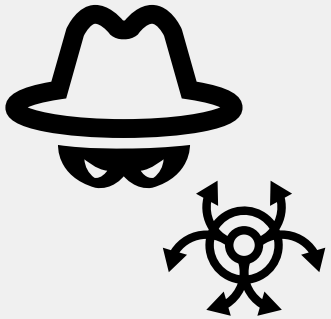
з декількома системами ідентифікації

Виклики ідентифікації



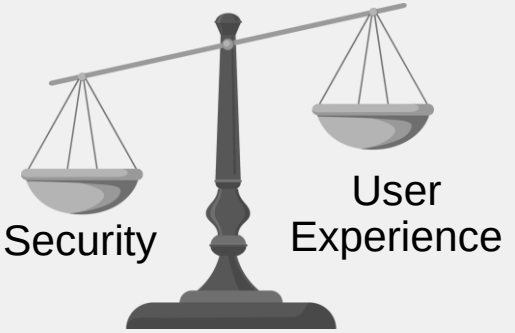
Легкий доступ до персональних даних

можна легко отримати з чорного ринку, включаючи імена користувачів і паролі



Identity Threats

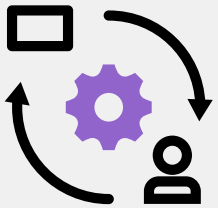
Identity threats розвиваються найшвидше та коштують у середньому 4,5 мільйона доларів США за інцидент*



Проблема зручності

Підвищення безпеки не повинно ускладнювати роботу користувачів

*Source: *IBM Cost of a Data Breach Report 2022*



Визначення Zero Trust

NIST	Evolving set of cybersecurity paradigms that move defenses from static, network- based perimeters to focus on users, assets, and resources	Новий набір парадигм кібербезпеки, що переміщує захист від статичних мережевих периметрів до зосередження на користувачах, активах і ресурсах
Gartner	**Identity**-based schema, resource secure access, continuous trust evaluation and adaptive access control	Схема на основі **ідентифікації**, безпечний доступ до ресурсів, безперервна оцінка довіри та адаптивний контроль доступу
Forrester	Zero Trust is an information security model that denies access to applications and data by default.	Zero Trust модель інформаційної безпеки, яка за умовчанням забороняє доступ до програм і даних.

Концепт Zero Trust

Zero Trust	Що це таке?:	Філософія довіри користувачеві чи пристрою лише після явного підтвердження їх **ідентичності** та **статусу**. Вони зосереджується на користувачах, пристроях і конкретних ресурсах, до яких здійснюється доступ, використовуючи сегментацію та зони контролю.
Zero Trust архітектури	Стратегія:	Системний підхід до заміни неявної довіри на явну довіру після перевірки. Вимагає кількох технологій для захисту користувачів, пристроїв, мереж і хмарних ресурсів. Пропоновані архітектури:
		• NIST SP 800-207 Zero Trust Architecture: NGFW, IAM, **ZTNA**, micro-segmentation
		• Forrester Zero Trust Edge: NGFW, SD-WAN, CASB, SWG, **ZTNA**
		• Gartner Secure Access Service Edge (SASE): SD-WAN, FWaaS SWG, CASB, **ZTNA**
Zero Trust ініціативи	Специфічні компоненти:	• Remote Access / Work From Anywhere
		• **Identity Access Management**
		• Network Segmentation / Micro-Segmentation

Zero Trust Access – ідентифікація користувачів

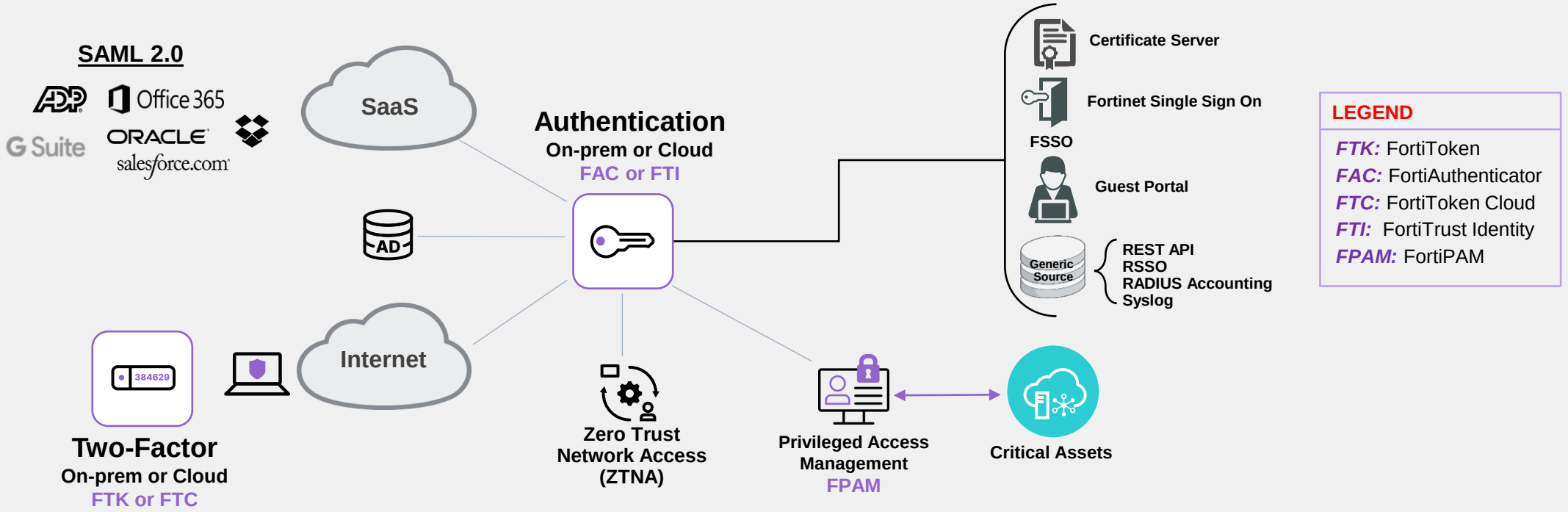
Знайте, **хто** є в мережі

ІДЕНТИФІКАЦІЯ — НАРІЖНИЙ КАМЕНЬ СТРАТЕГІЇ БЕЗПЕКИ ZERO TRUST

- Ким є користувач?
  - Співробітник?
  - Гість?
  - Постачальник?
  - Тимчасовий працівник?
- Який доступ він повинен отримати?
  - Роль користувача визначає права доступу та служби безпеки
  - **Політика мінімального доступу** дозволяє отримати доступ лише до ресурсів, необхідних для ролі/роботи
  - Легке скасування доступу за потреби

Zero Trust Access - забезпечення ідентифікації користувача

Знаючи, **хто** є в мережі, надайте **найменш привілейований** доступ

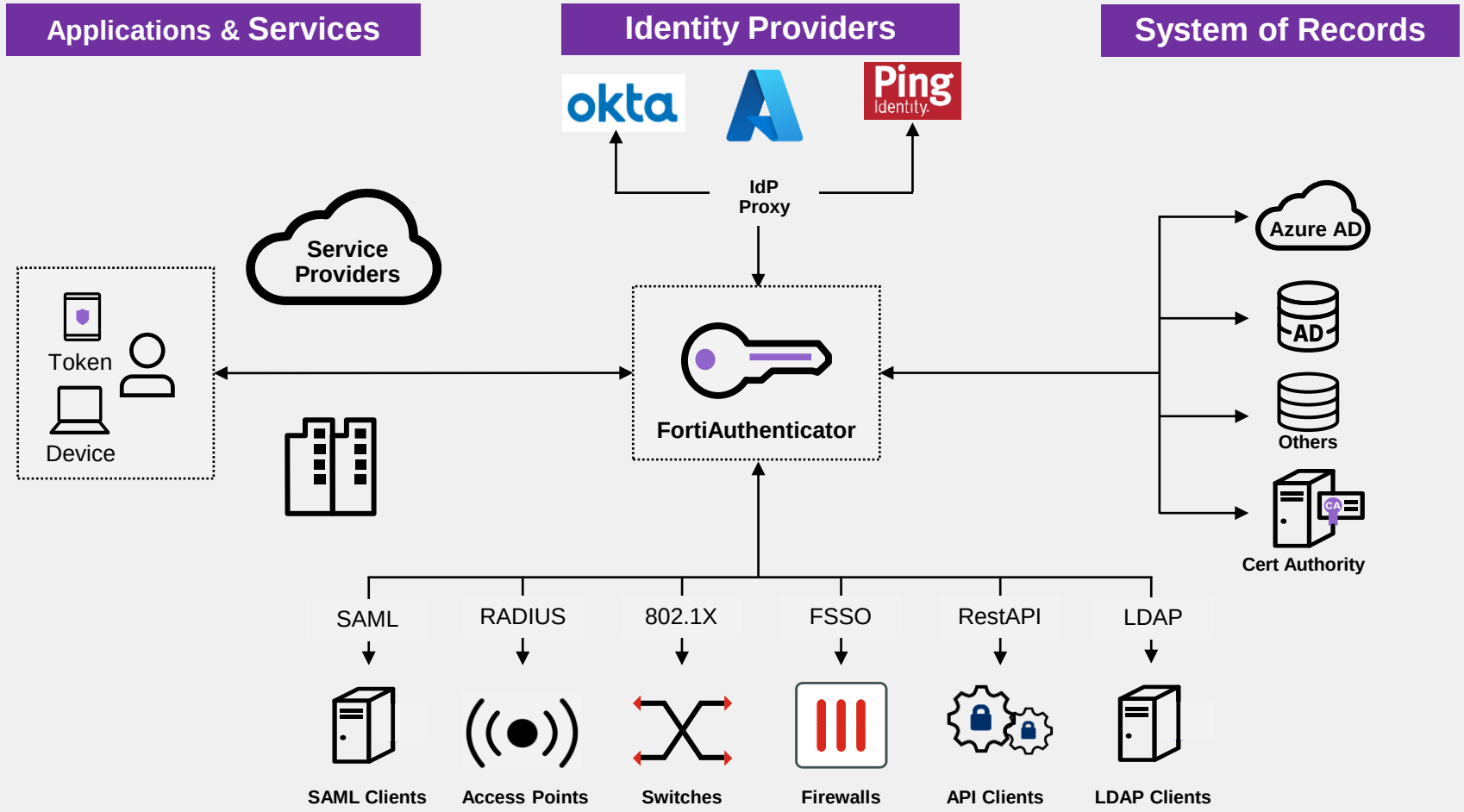


Authentication	Role-based Access	Single Sign On
Establish/re-verify identity though user log-in, certificate, and/or multifactor input	Provide information from authentication source for use in accessing company resources	Provide better user experience for logins while maintaining security

FortiAuthenticator

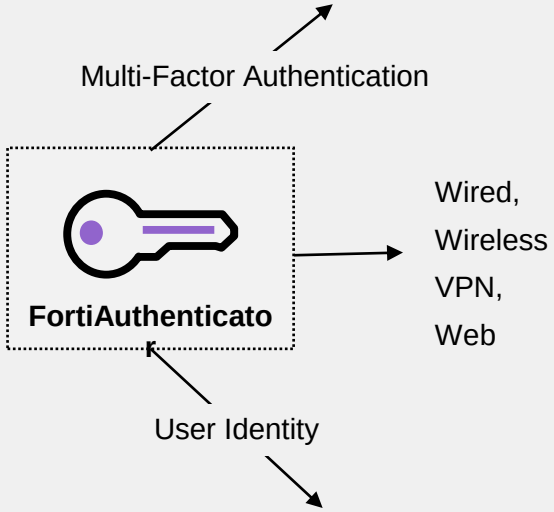
FortiAuthenticator

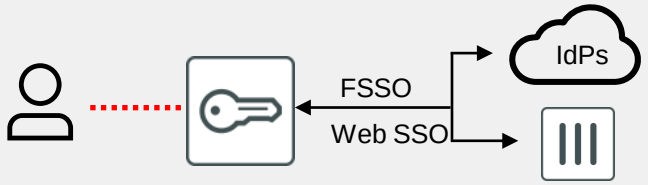
Джерело ідентифікації для Fortinet Security Fabric



- Централізована аутентифікація та політика
- Контроль доступу на основі ролей (співробітник, гість, партнери тощо)
- Адаптивна-, MFA Аутентифікація,
- Fortinet SSO та Web SSO
- Керування сертифікатами
- Зручність для користувачів – портали самообслуговування, безпарольна аутентифікація

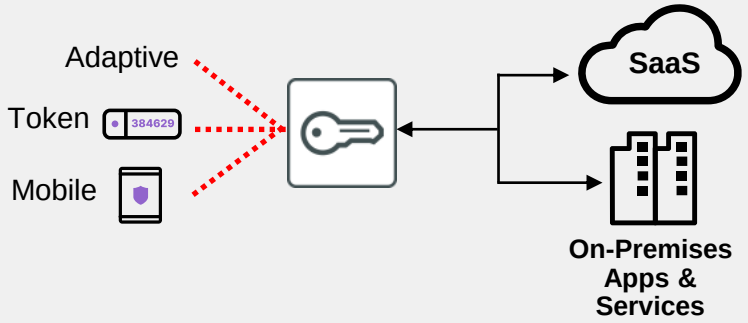
Приклади





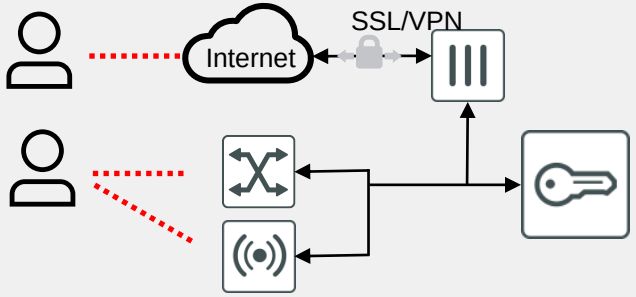
Fortinet SSO та Web SSO

- AD/LDAP, Kerboros, eDirectory
- SSO Mobile Agent, Agentless
- Third party systems via SAML (IdP, SP, IdP Proxy), RADIUS, TACACS+, Syslog and API Integration



Multi-Factor Authentication

- OTP Token, Physical and Mobile
- SMS and Email
- FortiToken Cloud
- Адаптивна аутентифікація
- Керування сертифікатами



Authentication & Authorization

- SSL/VPN, IPSEC VPN
- LDAP, 802.1X, RADIUS, RADSEC, TACACS
- OAuth, SAML, Web Portal, RestAPI
- Self-Service, Guest service
- Certificate Authority
  - X509 Cert Sign, Issue, Revoke
  - OCSP, SCEP, CMP2

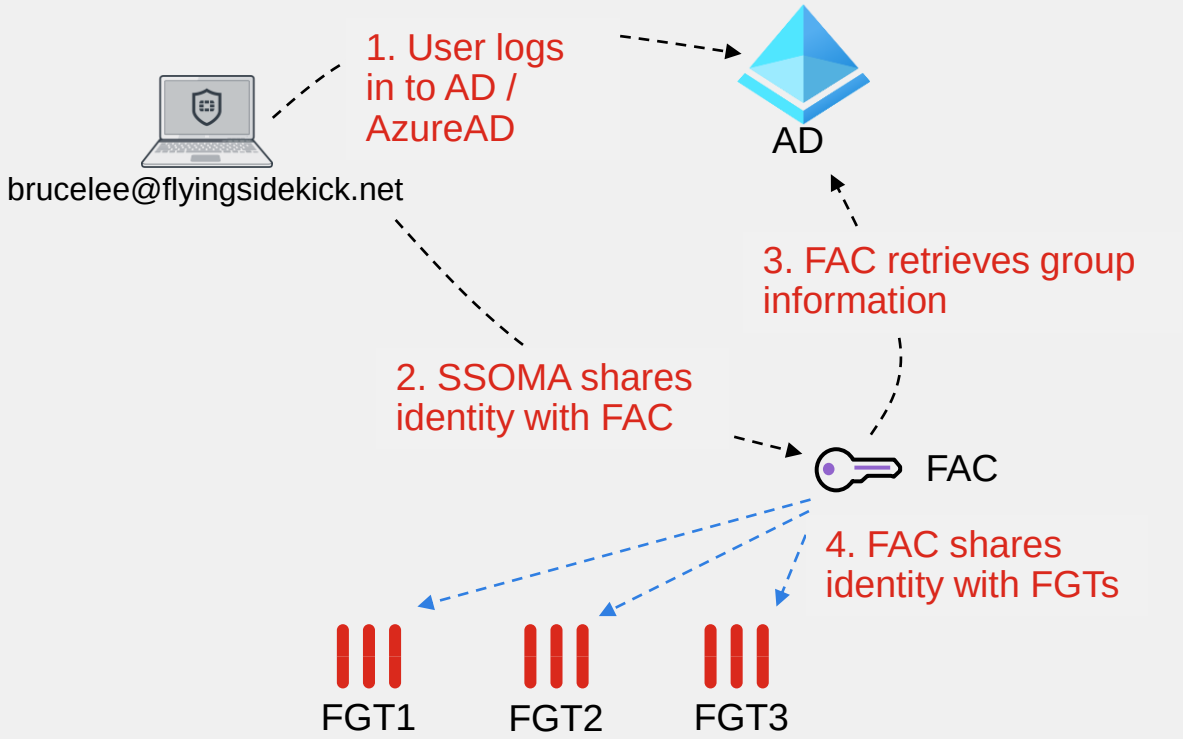
Апаратні моделі

	FAC-300F	FAC-800F	FAC-3000F
Users (base / max.)	1,500 / 3,500	8,000 / 18,000	40,000 / 240,000
Max. FortiTokens	3,000	16,000	480,000
Max. NAS Devices	500	2,666	80,000
Max. User Groups	150	800	24,000
Max. CA Certificates	10	50	300
Max. User Certificates	7,500	40,000	1,200,000
Interfaces	4x GE RJ45	4x GE RJ45 2x GE SFP	4x GE RJ45 2x GE SFP
Storage Capacity	2 x 1 TB	2 x 2 TB	2 x 2 TB

VM Series

	FAC-VM Base	FAC-VM-100-UG	FAC-VM-1000-UG	FAC-VM-10000-UG
Max. Local and/or Users	100	+100	+1,000	+10,000
Max. FortiTokens	200	+200	+2,000	+20,000
Max. NAS Devices	33	+33	+333	+3,333
Max. User Groups	10	+10	+100	+1,000
Max. CA Certificates	5	+5	+50	+500
Max. User Certificates	500	+100	+1,000	+10,000
Interfaces (Min/Max)	1 / 4			
Virtual CPUs (Max)	64			
Storage Capacity (Min Max)	60 GB / 16 TB			

SSO Mobility Agent



Ліцензування FortiAuthenticator SSO Mobility Agent

	FCC-FAC2K-LIC	FCC-FAC10K-LIC	FCC-FACUNL-LIC
Max. Users	2 000	10 000	Unlimited

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortiauthenticator.pdf

FortiToken

FortiToken

- Проста безстрокова ліцензія. Без прихованих витрат
- Апаратні форм-фактори - USB, брелок
- Мобільний додаток підтримкою PUSH

FortiToken Mobile

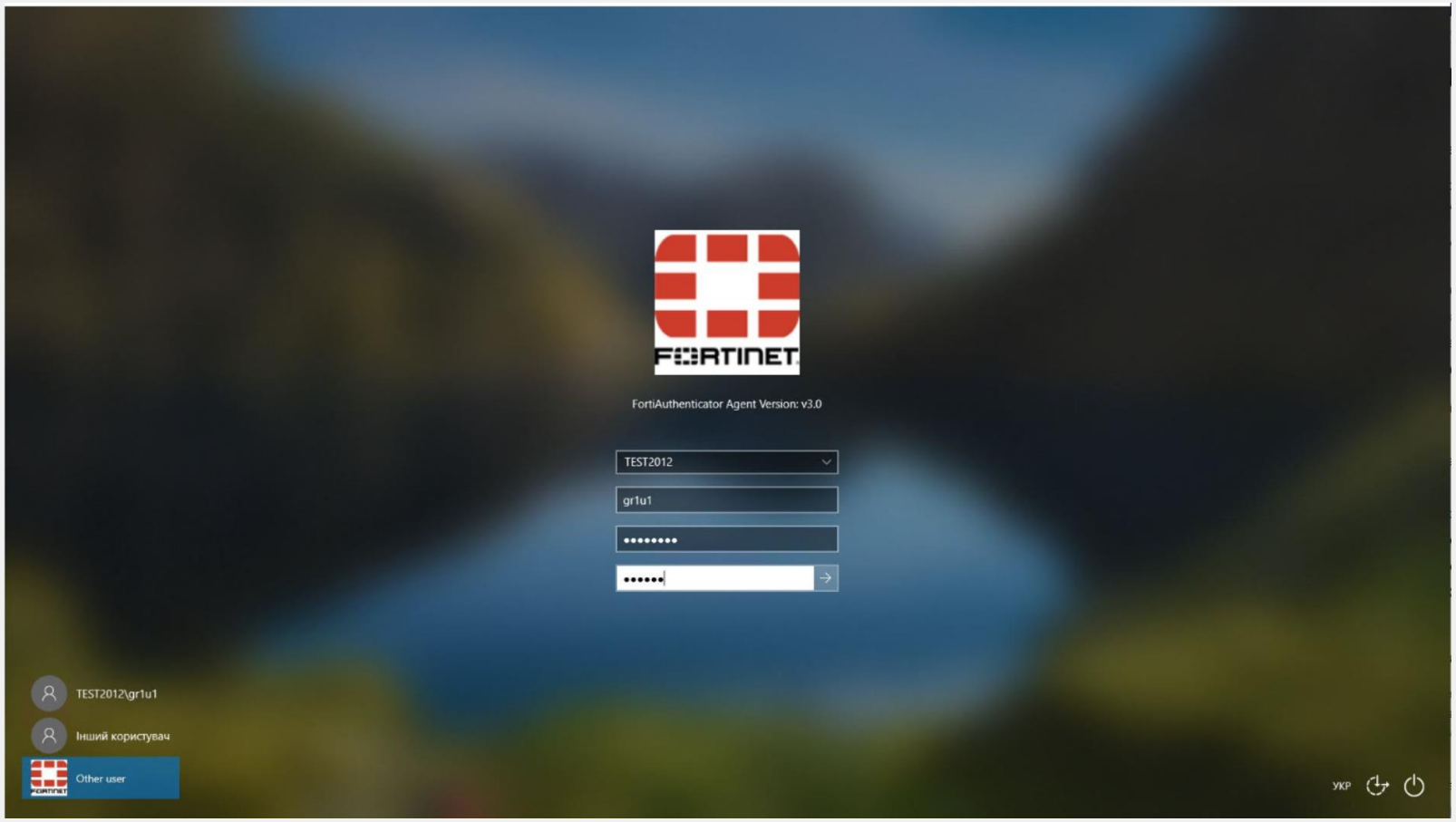
FortiToken 200B/200BCD

FortiToken 300

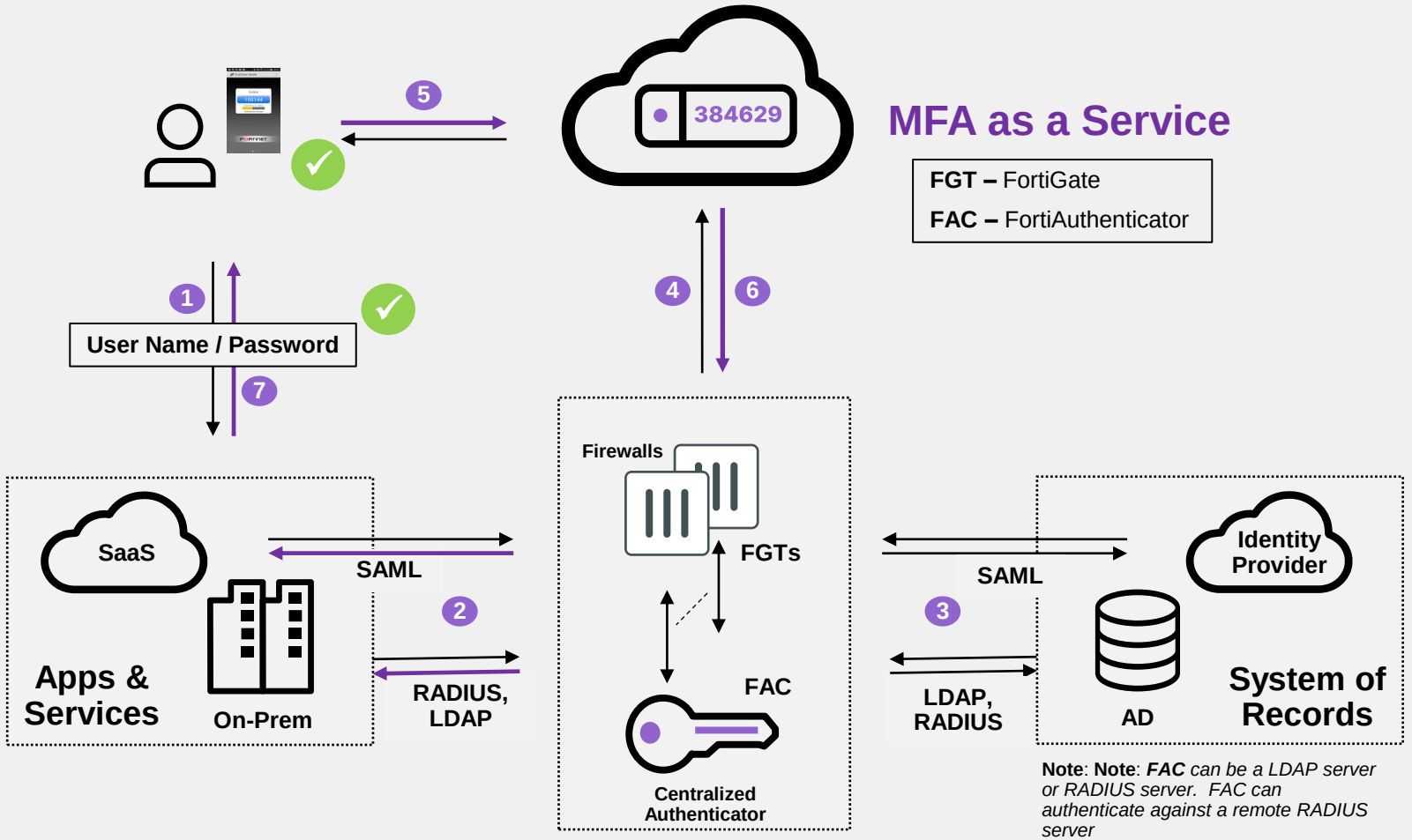
FortiToken 400 (Passwordless)

One-Time-Passcode (OTP) | Certificate | FIDO Key

FortiAuthenticator Windows Agent



FortiToken Cloud: MFA як сервіс



- Підписка на MFA as a Service
- Інтеграція FGT & FAC (без потреби додаткових HW/SW)
- Автоматизація розповсюдження токенів на iOS, Android
- Підтримка кількох варіантів OTP token:
  - FTM by default @ no cost
  - FTK HW (optional)
  - Email та SMS
- Централізоване керування, що показує події аутентифікації та використання
- Автоматичне блокування користувачів із надмірною кількістю помилок 2FA
- Підтримка MSP: можливість RBAC,окремого Realm для кожного кінцевого кілєнта для керування токенами та користувачами

FortiToken

SOLUTION BUNDLE		FORTITOKEN CLOUD
Software Tokens	Up to 25 users	FC1-10-TKCLD-445-01-DD
	Up to 100 users	FC2-10-TKCLD-445-01-DD
	Up to 500 users	FC3-10-TKCLD-445-01-DD
	Up to 2 000 users	FC4-10-TKCLD-445-01-DD
	Up to 10 000 users	FC5-10-TKCLD-445-01-DD
SMS	2 500 SMS credits	FTC-SMS-2500
	10 000 SMS credits	FTC-SMS-10K
	25 000 SMS credits	FTC-SMS-25K

See FortiToken Cloud FAQs.

SOLUTION BUNDLE		CLOUD-MANAGED FORTITOKEN CLOUD	DEVICE-MANAGED PERPETUAL LICENSE
Software Tokens	+5	Included with subscription	FTM-ELIC-5
	+10		FTM-ELIC-10
	+25		FTM-ELIC-25
	+50		FTM-ELIC-50
	+100		FTM-ELIC-100
	+200		FTM-ELIC-200
	+500		FTM-ELIC-500
	+1000		FTM-ELIC-1000
	+2000		FTM-ELIC-2000
	+5000		FTM-ELIC-5000
	+10000		FTM-ELIC-10000

SOLUTION BUNDLE		KEYCHAIN	USB	FIDO KEY
Hardware Tokens	5-pack	FTK-210B-5	FTK-310-5	FTK-410-5
	10-pack	FTK-210B-10	FTK-310-10	FTK-410-10
	20-pack		FTK-310-20	
	25-pack	FTK-210B-25		FTK-410-25
	50-pack	FTK-210B-50	FTK-310-50	FTK-410-50
	100-pack	FTK-210B-100		FTK-410-100
	200-pack	FTK-210B-200	FTK-310-200	
	500-pack	FTK-210B-500		
	1000-pack	FTK-210B-1000		
	2000-pack	FTK-210B-2000		

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortitoken.pdf

FortiTrust ID

FortiTrust ID

- Що таке FortiTrust?
  - Модель на основі підписки
  - Ліцензування по кількості користувачів (мінімальна кількість для замовлення - 100)
- **FortiTrust ID**: user-based ліцензія FAC Cloud + FortiToken Cloud
  - FortiAuthenticator Cloud (VM в хмарі Fortinet)
  - FortiToken Cloud для MFA

Identity as-a-Service

Універсальне рішення IAM для гібридного середовища

FortiTrust Identity

- Аутентифікація, MFA, та SSO
- Підписка по користувачах
- Хмарне рішення, що доступне завжди і всюди

FAC Cloud – відсутній функціонл в порівнянні з On-Prem FAC

- TACACS+ server
- LDAP server
- FSSO features
  - Event polling
  - RADIUS accounting

Ліцензування

Order Information	
100-499 Users	FC2-10-ACCLD-511-02-DD
500-1,999 Users	FC3-10-ACCLD-511-02-DD
2,000-9,999 Users	FC4-10-ACCLD-511-02-DD
10,000+ Users	FC5-10-ACCLD-511-02-DD

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortitrust.pdf

FortiPAM

Privileged Access

Привілейований доступ – це доступ до привілейованих облікових записів привілейованих користувачів (наприклад, IT-менеджерів і системних адміністраторів).

Привілейований обліковий запис

Привілейований обліковий запис – це будь-який обліковий запис, який надає доступ до ресурсів, інформації та операцій, які недоступні для стандартних непривілейованих облікових записів. Привілейовані облікові записи можуть бути пов’язані з ідентифікаторами людей або машин.

Привілейований користувач

Привілейований користувач — це будь-який користувач, який зараз має доступ до привілейованого облікового запису.

Фактор ризику

Через доступ до розширених можливостей привілейовані користувачі та привілейовані облікові записи становлять **значно більший ризик**, ніж непривілейовані облікові записи/непривілейовані користувачі.

Проблеми PAM

Один **спільний обліковий запис** адміністратора означає відсутність можливості аудиту: дії не можна відстежити до конкретної особи.

Рішення полягає в тому, щоб мати кілька облікових записів адміністратора, прив’язаних безпосередньо до окремих осіб.

Розподіл обов’язків - найкращі практики безпеки та стандарти передбачають використання двох облікових записів для кожного адміністратора. Один обліковий запис користувача, один обліковий запис адміністратора. На практиці цим часто нехтують і це призводить до вразливості, наприклад під час атак на підвищення привілеїв.

Рішення PAM - один набір облікових записів, який може використовуватися кількома особами, і аудити можуть відстежити дії та забезпечити підзвітність.

Що таке PAM?

Privileged Access Management (PAM)

це стратегія кібербезпеки, призначена для захисту та моніторингу доступу до критично важливих активів, таких як брандмауери, сервери, OT або хмарна інфраструктура. Вона гарантує, що лише авторизовані користувачі можуть виконувати конфіденційні завдання, такі як конфігурація та обслуговування, одночасно запобігаючи несанкціонованому доступу до конфіденційної інформації.

Керування привілейованим доступом
Доступ мають лише авторизовані користувачі

Моніторинг і запис сеансів
Аудит сесій та можливість завершувати сесії в режимі реального часу

Керування привілейованими обліковими даними
Безпечне зберігання облікових данних, автоматичне створення та зміна паролів

Основний функціонал FortiPAM

Сховище облікових даних

- Кінцеві користувачі не знають і не бачать облікові дані
- Зменшує ризик витоку облікових даних

На комп'ютері кінцевого користувача немає конфіденційних даних
Автоматична зміна пароля

Тільки авторизовані користувачі можуть отримати доступ до певних ресурсів

- Найменший доступ на основі ролей. (Standard User, Administrator, Custom)
- Контроль секретних дозволів
- Адміністратор визначає політику та дозволи

Ієрархічна система затвердження
Контроль ризикованих команд

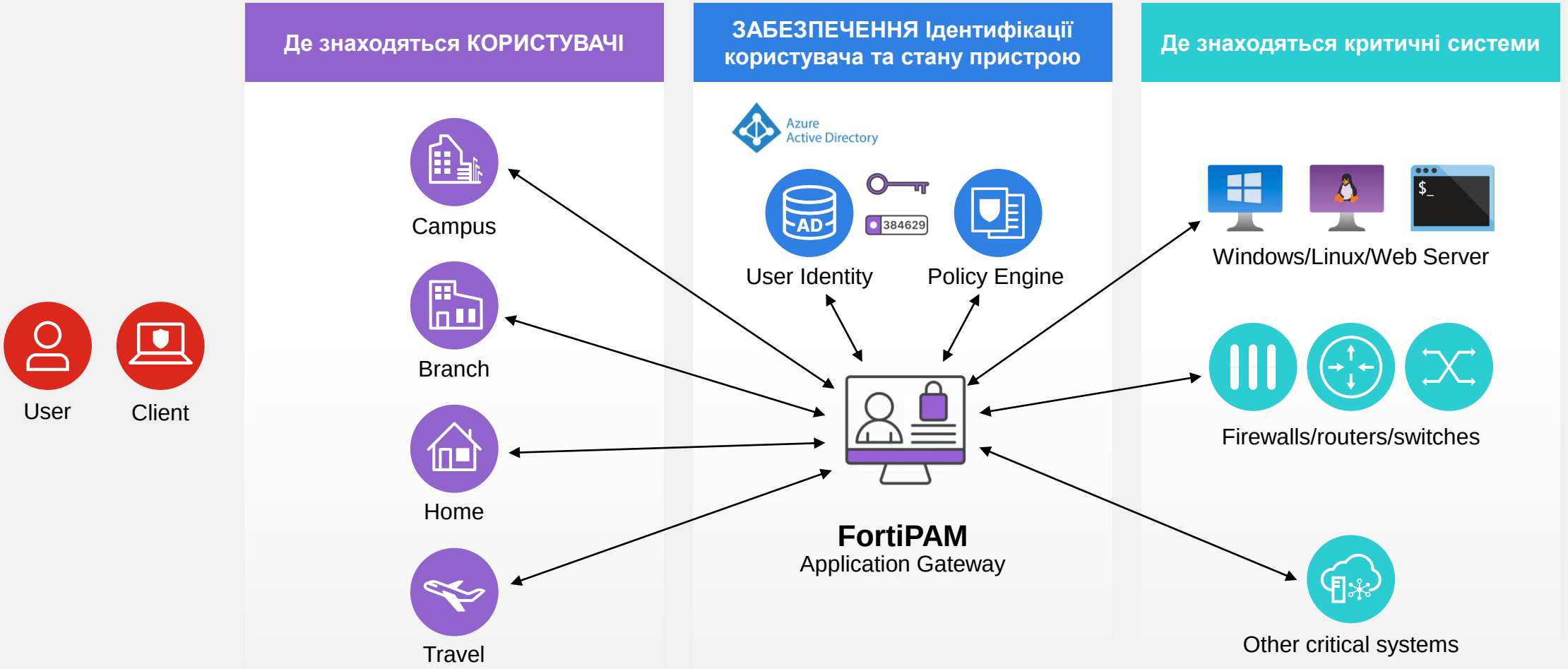
Спостереження за сеансовою активністю

- Моніторинг списку сеансів
- Моніторинг «із-за спини» (живий запис)
- Запис сеансів
- Аудит сеансів

Моніторинг натискання клавіш, подій миші
Відеозапис

FortiPAM як Application Gateway

Компоненти FortiPAM



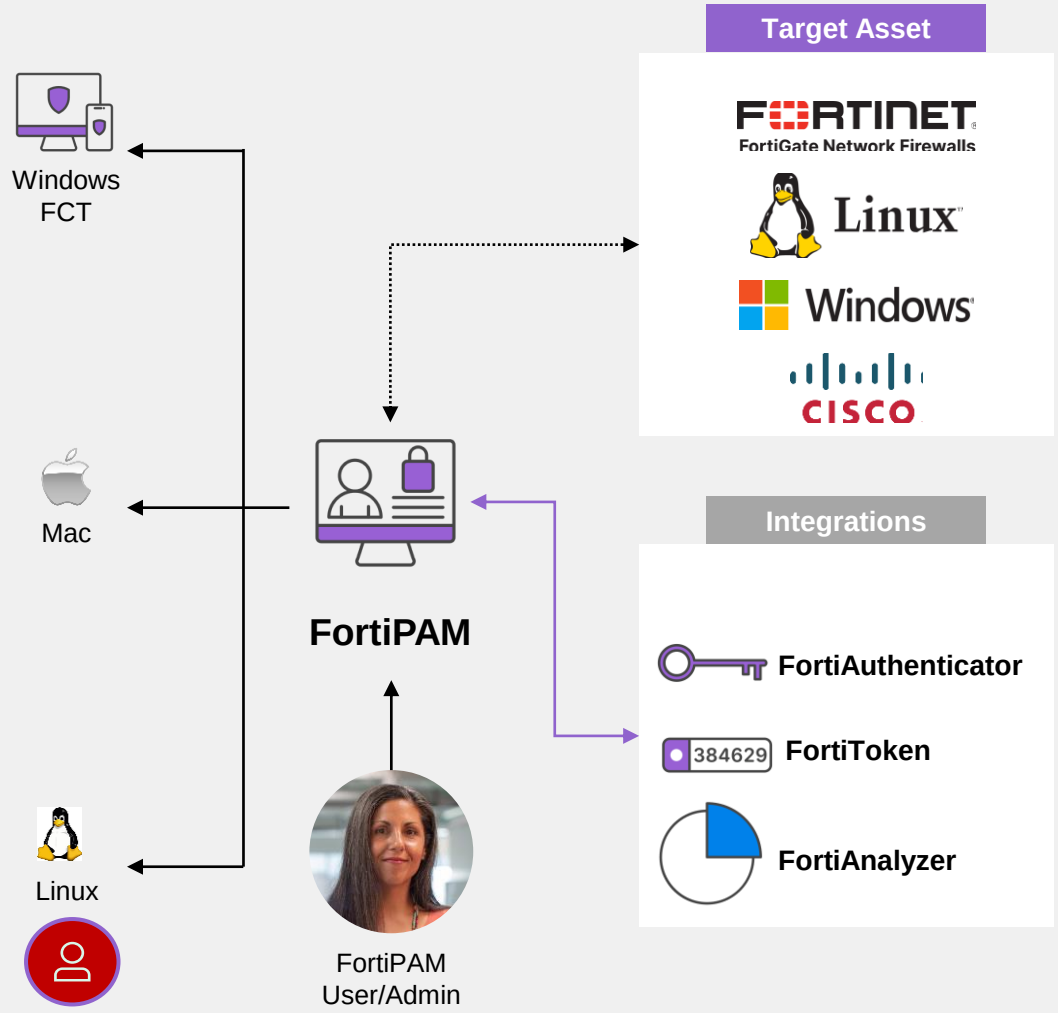
Компоненти FortiPAM

FortiPAM server (Virtual or Physical Appliance)

- FortiOS/FortiProxy platform and framework
- GUI
- Backend application

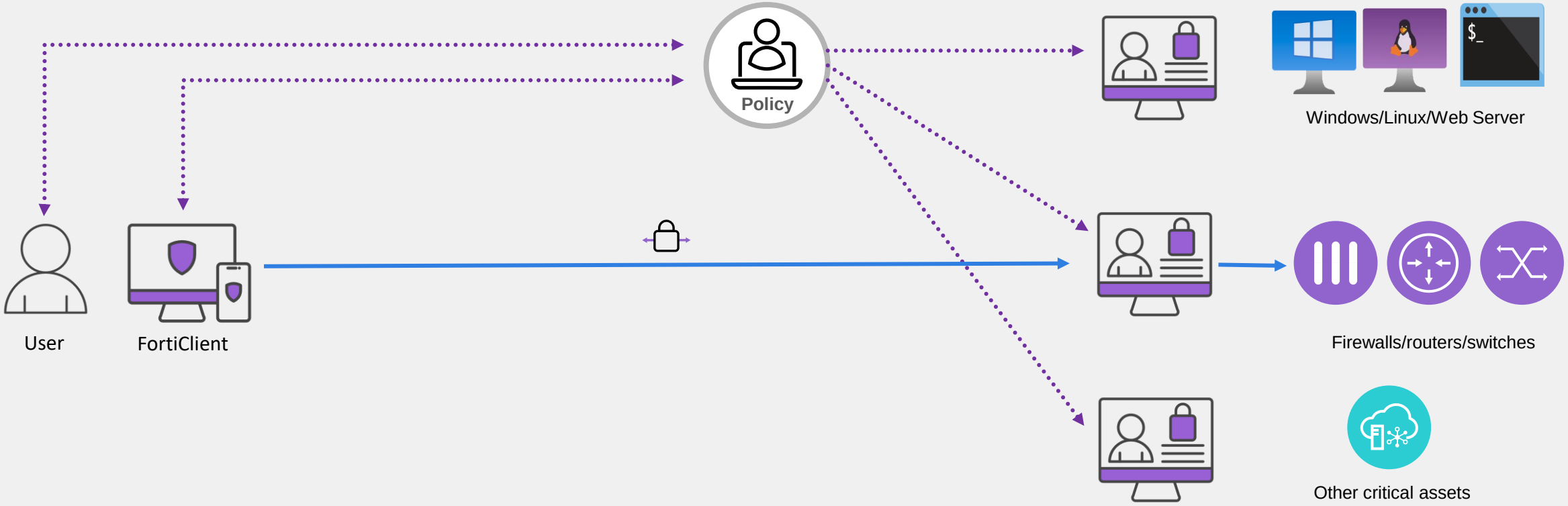
FortiClient

- FortiVRS – Video Recording Service
- FortiTCS – ZTNA Service
- Web Extension (Chrome, Edge, Firefox)



ZTNA доступ до критичних активів з FortiPAM

Додаткова безпека з FortiClient



1. Validate Device
2. Verify User
3. Device Posture
4. Application Access Only
5. Encrypted

Переваги

- Безперервна перевірка привілейованого користувача/пристрою
- Перевірка безпеки на наявність зловмисного програмного забезпечення та порушень DLP в реальному часі
- Припинення підозрілих сеансів

Моніторинг

User Monitor

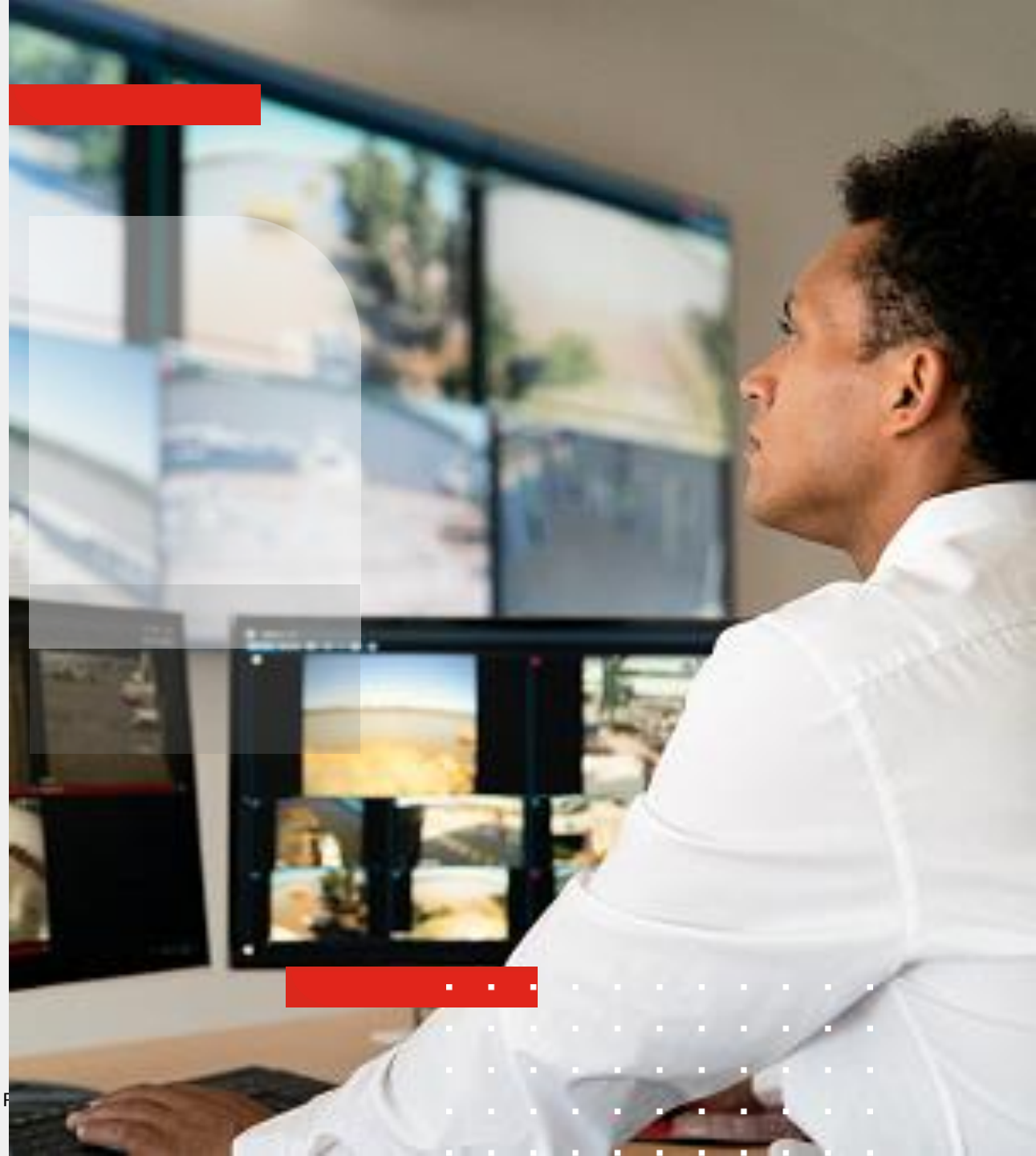
- Зареєстровані користувачі

Active Sessions

- Поточні сеанси до критичних активів
- Активний перегляд із можливістю завершення сеансу

Secret Video

- Перегляд журналів відеозаписів
- Відтворення записів із сторінки перегляду журналів



Архітектура FortiPAM

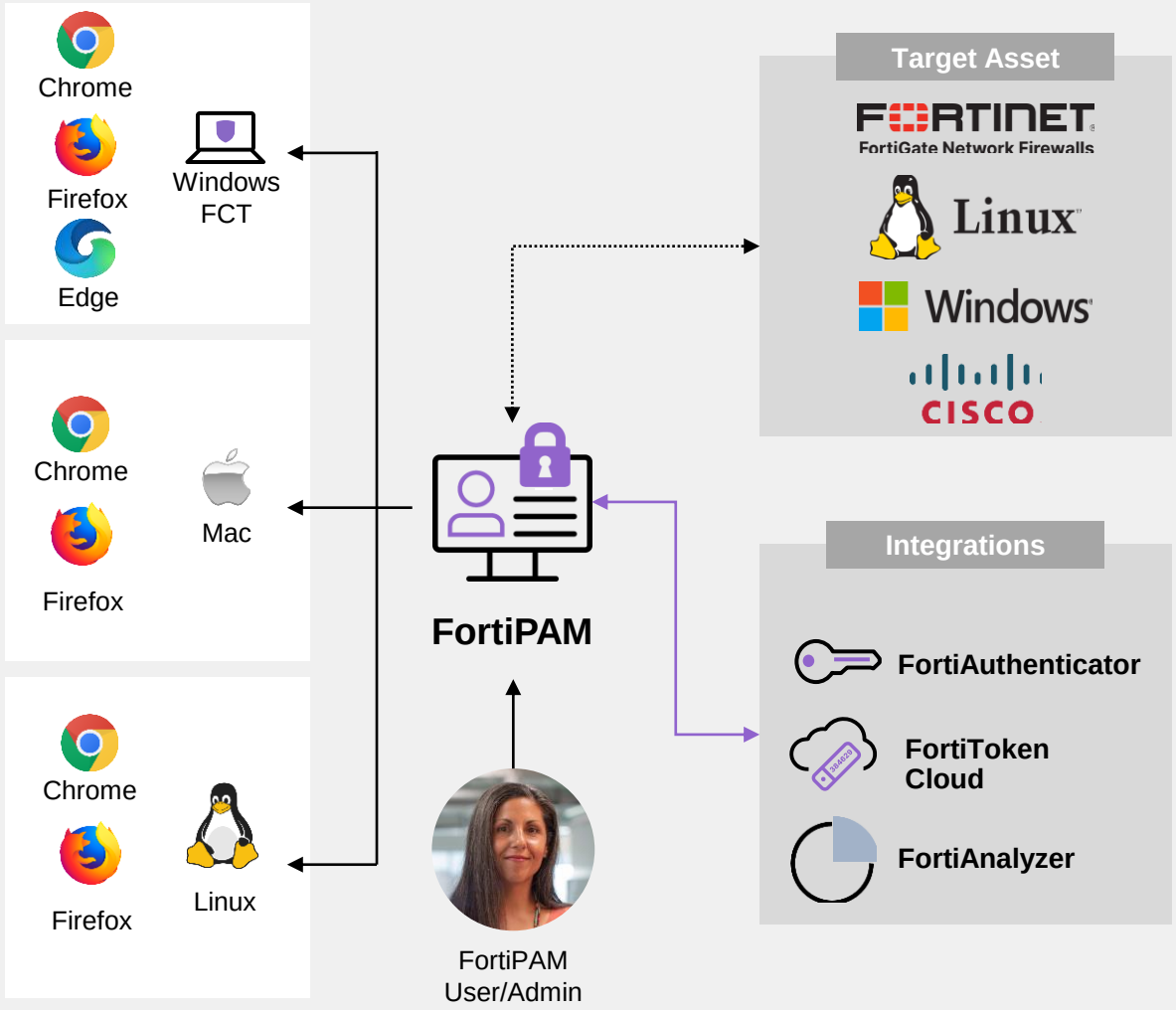
Агент користувача для підключення до цільового активу

FortiPAM application

- FortiOS/FortiProxy platform and framework
- GUI
- Backend application

FortiClient

- FortiVRS – Video Recording Service
- FortiTCS – ZTNA Service
- Chrome, Edge, Firefox extension



Ліцензування

PRODUCT	SKU	DESCRIPTION
Hardware		
FortiPAM 1000G	FPA-1000G	FortiPAM-1000G Privileged Access Management server for up to 50 users.
FortiPAM 3000G	FPA-3000G	FortiPAM-3000G Privileged Access Management for up to 100 users
Virtual Machines		
FortiPAM-VM	FC1-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 5 to 9 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC2-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 10 to 24 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC3-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 25 to 49 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC4-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 50 to 99 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC5-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 100 to 249 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC6-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for 250 or more users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
License Options		
FortiPAM License Options		Licensed FortiClient with PAM function activated. This is the recommended deployment as additional SSL VPN, ZTNA, SSOMA functions can also be activated. This uses the existing EMS licenses - no additional license required.
		Dedicated unlicensed standalone FortiClient with PAM function which does not require EMS. This standalone FortiClient can not be combined with other FCT standalone versions and can only be used for FortiPAM.

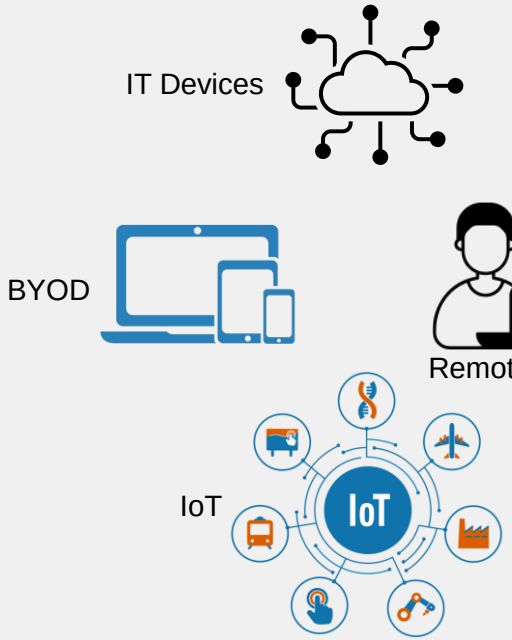
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortipam.pdf
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortipam.pdf

FortiNAC

Що стимулює впровадження NAC?

Зростання кількості користувачів, пристроїв, даних та програм

Підприємства витрачали в середньому 1,3 мільйона доларів США на відповідність до регуляторних вимог і, як очікується, вкладуть ще 1,8 мільйона доларів США



За останні 5 років кількість **віддалених працівників** зросла на 44%, і вони спричинили порушення безпеки в 20% організацій

- Виявляє, профілює та відстежує кінцеві точки
- Аутентифікація, авторизація та контроль доступу до мережі
- Поліпшення безпеки

Пристрої IoT піддаються в середньому 5200 атак на місяць

Endpoints

Digitization → Digital Transformation

Process optimization **Profitability** **Business Innovation** **Revenue Growth**

Захист усього, що підключено до мережі

Нагляд за кожним вузлом в мережі

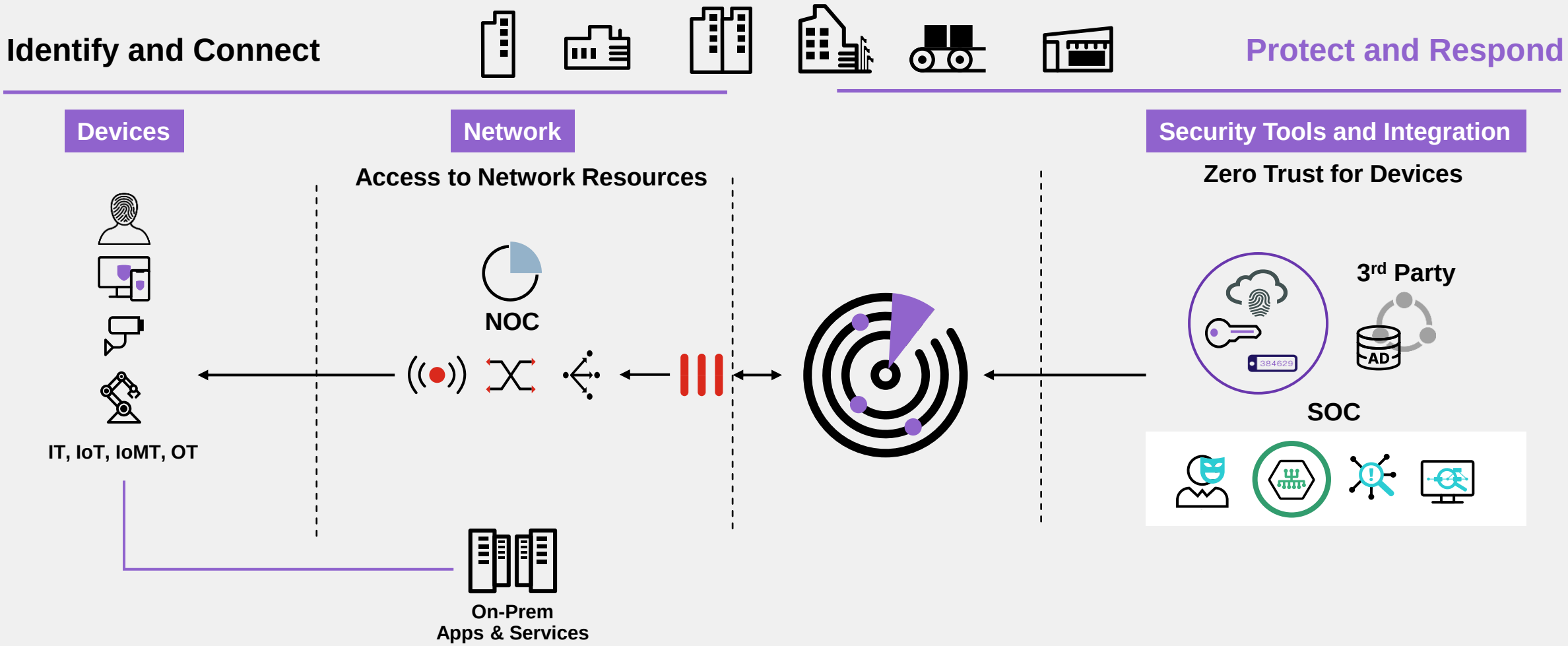
Видимість — Виявлення та ідентифікація

Контороль — Сегментація, аутентифікація та авторизація

Реагування — Детектування, реагування та знешкодження

Визначення FortiNAC

Zero Trust для пристроїв



Застосування FortiNAC

Zero Trust для пристроїв

- Найменш привілейований доступ
- Динамічні політики доступу

Інвентаризація

- Консолідована видимість
- Комплексне покриття

Реєстрація

- BYOD пристрої
- Різні типи користувачів
- Captive Portal

Мікросегментація

- Гранульована
- Динамічна
- Контекстна

Автоматизація процесів

- Виконання політики
- Стримування загрози
- Зміна дозволу

Відповідність до вимог

- Оцінка ризиків
- Аудити

Оркестрація

- Threat Intelligence insights
- Service automation
- Notification systems

IT/OT Convergence

- OT visibility
- Centralized management

Функціонал FortiNAC

Zero Trust для пристроїв

- Найменш привілейований доступ
- Динамічні політики доступу

Інвентаризація

- Консолідована видимість
- Комплексне покриття

Реєстрація

- BYOD пристрої
- Різні типи користувачів
- Captive Portal

Мікросегментація

- Гранульована
- Динамічна
- Контекстна

Автоматизація процесів

- Виконання політики
- Стримування загрози
- Зміна дозволу

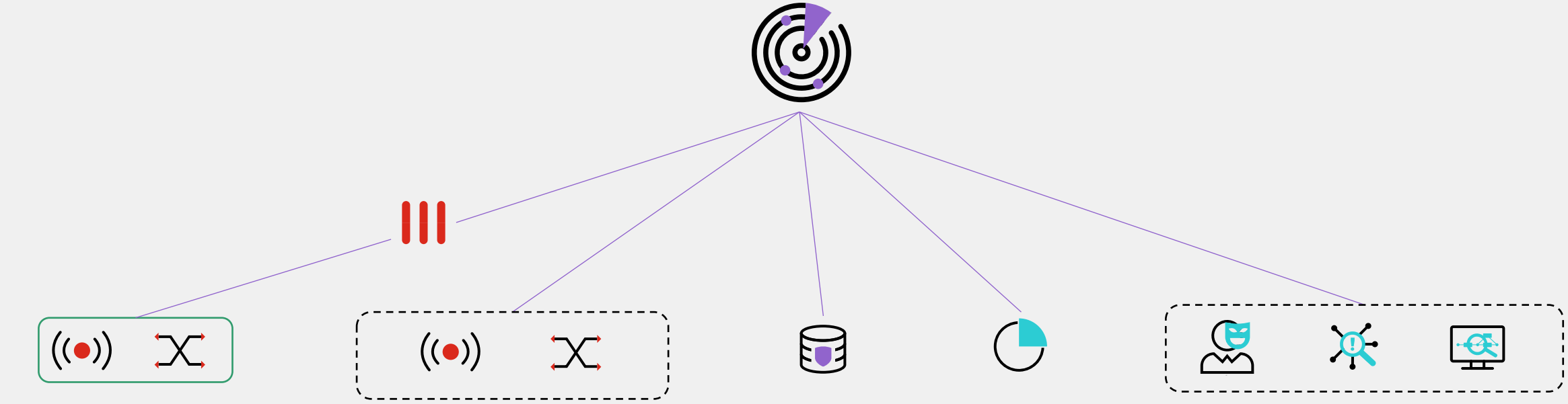
Відповідність до вимог

- Оцінка ризиків
- Аудити

Оркестрація

- Статистика та аналіз загроз
- Автоматизація захисту
- Оповіщення

FortiNAC інтеграція з Fortinet Security Fabric



Видимість мережі, конфігурація,призначення VLAN

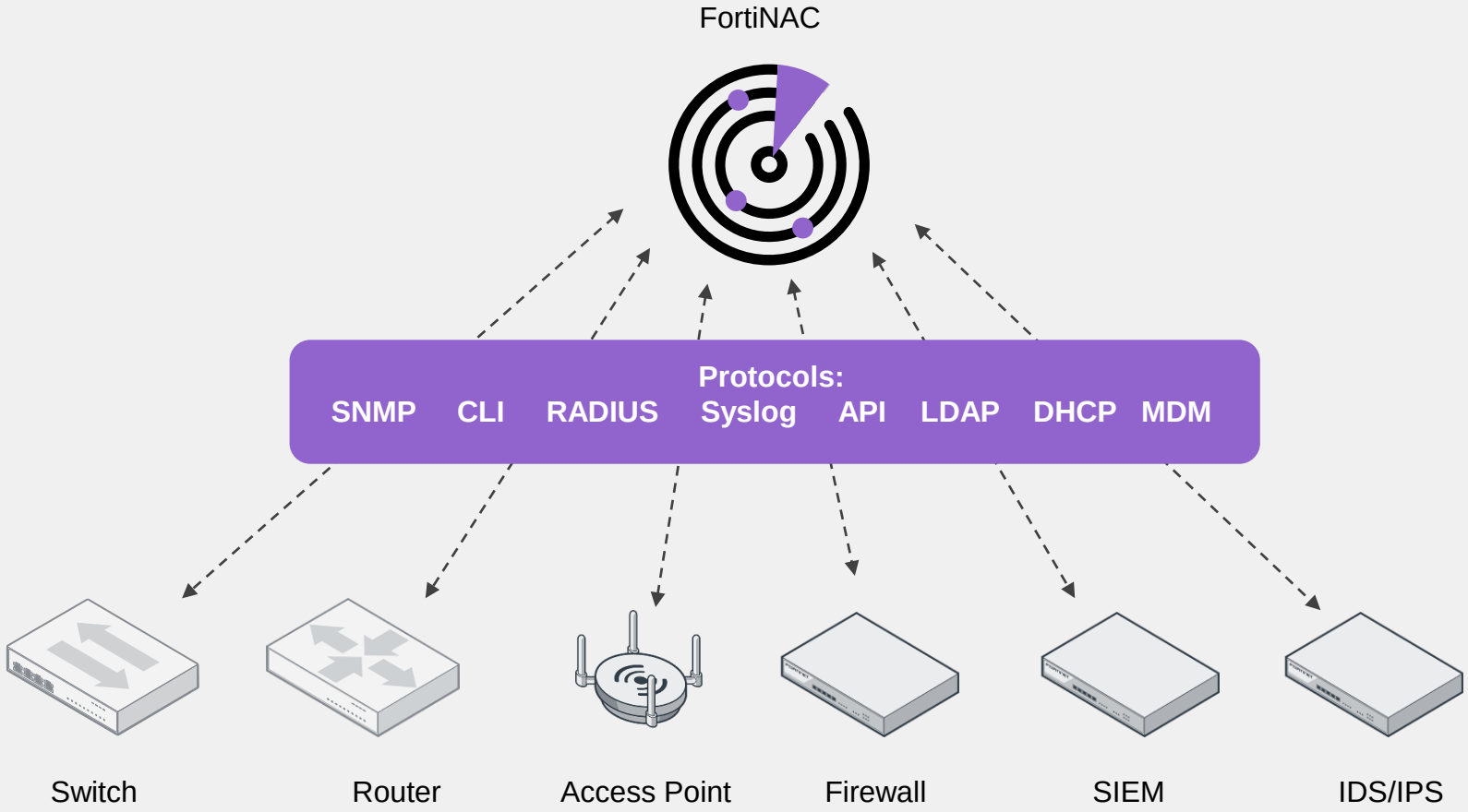
Видимість мережі, конфігурація,призначення VLAN

Реєстрація Пристроїв з FortiCleint

Звітність

Реагування на інциденти

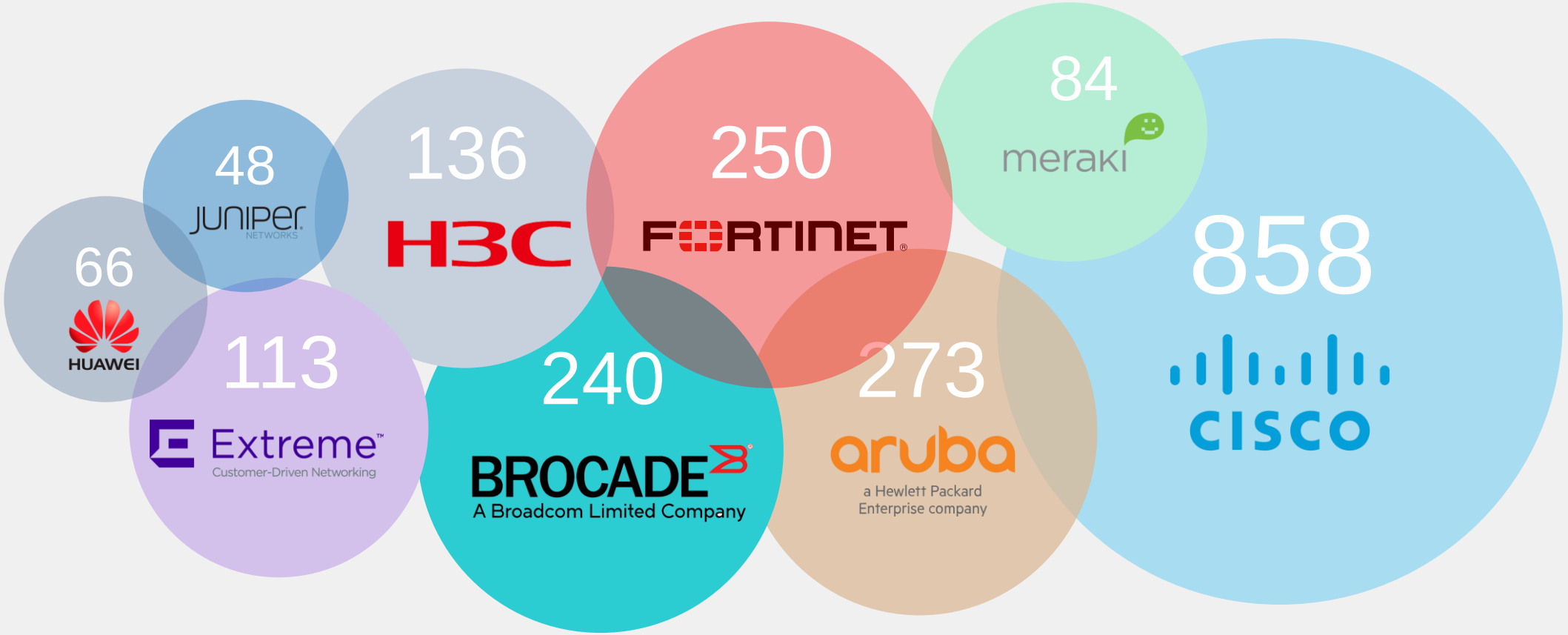
Підтримка обладнання інших виробників



Сумісність з більшістю мережевої інфраструктури корпоративного класу

Підтримка мережевого обладнання

Охоплені виробники становлять ~75% частки мережевого ринку



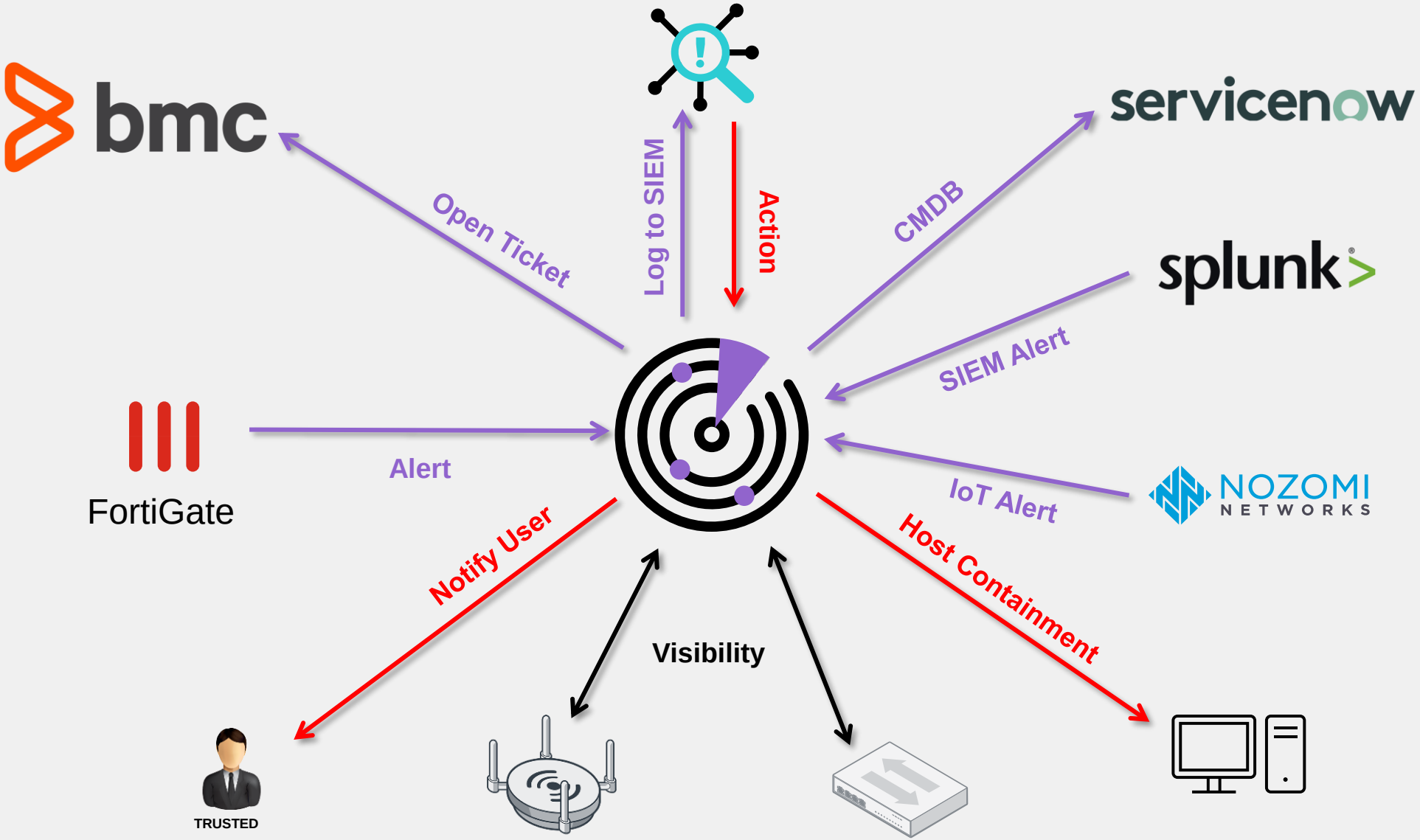
95 Виробників

- Networking
- Carrier
- Security
- Industrial

2432 Моделей

- Switches, APs, Controllers,
- Data Center, Enterprise, SMB
- Modular, 1U, Ruggedized

Автоматизація безпеки



Профілювання пристрою

Швидко, точно і безперервно

- 21 метод профілювання (10 пасивних і 11 активних)
- Правила створюються на основі методів профілювання та використовуються для оцінки виявлених пристроїв
- Правила можна ранжувати в послідовності, а інформація про пристрій містить перехресні посилання.
- Коли пристрої відповідають правилам, то встановлюються атрибути, наприклад тип пристрою, роль, група тощо.

Passive Methods

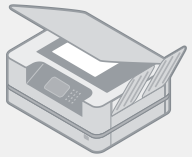
- DHCP Fingerprinting
- FortiGate
- FortiGuard
- IP Range
- Location
- Network Traffic
- Passive
- Persistent Agent
- RADIUS Request
- Vendor OUI

Action Methods

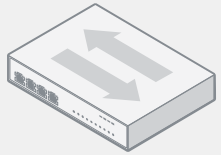
- Active
- HTTP/HTTPS
- ONVIF
- Script
- SNMP
- SSH
- TCP
- Telnet
- UDP
- WinRM
- Windows Profile

FortiNAC приклади роботи

Continuous Device Profiling

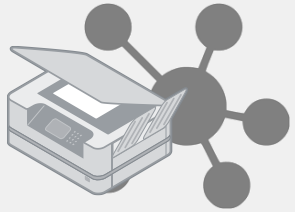


1. Printer connected to network



2. MAC notification trap triggers FortiNAC

3. FortiNAC Profiles device as printer and provide auto port configuration



4. FortiNAC allows quick deployment through Fabric and Printer-type access to network

Containment of Lateral Threats at Edge

1. Infected endpoint contacts C&C or downloads a malware

2. FGT detects and sends event to FortiNAC

3. FortiNAC quarantines the device at access layer

4. Virus contained at switch node

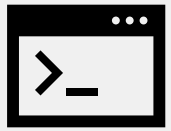
Компоненти рішення

Appliance

Hardware or VM (most popular)

- Control / Application
- Manager (concurrent license coordination)

vmware vSphere · KVM · Microsoft Hyper-V · aws · Azure



License

Subscription or Perpetual

- 3 Tiers (Base, Plus, Pro)
- Concurrent Endpoints (100- 50K)

Services and Support

- FortiCare
- Professional Services

Ліцензування

Hardware Server Sizing

Appliance

HARDWARE			
Hardware Server	**Type**	**Target Environment**	**Capacity[1]**
FortiNAC-CA-500F	Standalone Appliance (Integrated Control Server and Application Server)	Small Environments	Manages up to 5000 ports in the network
FortiNAC-CA-600F	High Performance Control and Application Server	Medium Environments	Manages up to 15 000 ports in the network
FortiNAC-CA-700F	Ultra High Performance Control and Application Server	Large Environments with few Persistent Agents	Manages up to 25 000 ports in the network
FortiNAC-M-550F	Management Appliance (Provides centralized management when multiple appliances are deployed)	Multi-site environments with multiple appliances	Can manage up to 50 CA servers with latencies up to 600ms in lab environment

1 Ports in the network = total number of switch ports + maximum number of concurrent wireless connections. FortiNAC sizes the appliance capacity based on total port counts not total number of devices.

VM Server Resource Sizing

Virtual

VIRTUAL MACHINE							
VM OS	**SKU**	**Ports in the Network[1]**	**Target Environment**	**CPU Reference**	**vCPU Qty[2]**	**Memory (GB)**	**Disk (GB)**
FortiNAC-OS	**FNC-CAX-VM**	Up to 5 000	Small	Intel Xeon E-2278 GE 3.3 GHz 8C/16T	8	16	100
		Up to 15 000	Medium	AMD Milan EPYC 7413 2.65 GHz 24C/48T	24	32	100
		Up to 25 000	Large	AMD Milan EPYC 7543P 2.8 GHz 32C/64T	32	96	100
	FNC-MX-VM	Up to 50 CA Servers	Large	AMD Milan EPYC 7413 2.65 GHz 24C/48T	24	32	100

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf

Рівні ліцензування FortiNAC

			BASE	PLUS	PRO
Visibility	Network	Network Discovery	✓	✓	✓
		Rogue Identification	✓	✓	✓
		Device Profiling and Classification	✓	✓	✓
	Endpoint	Enhanced Visibility	✓	✓	✓
		Anomaly Detection	✓	✓	✓
		MDM Integration	✓	✓	✓
		Persistent Agent		✓	✓
	User	Authentication		✓	✓
		Captive Portal		✓	✓
Automation/Control		Network Access Policies	✓	✓	✓
		IoT Onboarding with Sponsor	✓	✓	✓
		Rogue Device Detection and Restriction	✓	✓	✓
		Firewall Segmentation	✓	✓	✓
		MAC Address Bypass	✓	✓	✓
		Full RADIUS (EAP)		✓	✓
		BYOD/Onboarding		✓	✓
		Guest Management		✓	✓
		Endpoint Compliance		✓	✓
		Web and Firewall Single Sign-on		✓	✓
Incident Response		Event Correlation			✓
		Extensible Actions and Audit Trail			✓
		Alert Criticality and Routing			✓
		Guided Triage Workflows			✓
Integrations		Inbound Security Events			✓
		Outbound Security Events		✓	✓
		REST API	✓	✓	✓
Reporting		Customizable Reports	✓	✓	✓

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortinac.pdf

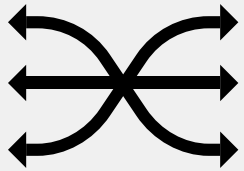
Підсумки

Чому наші замовники обирають Fortinet IAM

Надійний партнер зараз і в майбутньому

Комплексне рішення

- Комплексне рішення IAM (аутентифікація, MFA, SSO, PAM)
- Інтегроване у Fortinet Security Fabric як джерело ідентифікації
- Простота використання за допомогою SSO та порталу самообслуговування
- Екосистема Fortinet, яка дозволяє організаціям впроваджувати інновації за допомогою технологій



Централізація

- Проста і масштабована архітектура
- Об’єднання ідентифікації як з локальних, так і з хмарних джерел
- Централізоване управління та ліцензування.
- Жодних прихованих витрат на додаткові функції
- Гнучкі варіанти розгортання – пристрої, VM, хмара

Zero Trust

- Zero trust безпека ідентифікації користувача з найменш привілейованою аутентифікацією для контролю доступу для всіх користувачів, включаючи привілейованих.
- Адаптивна та надійна аутентифікація, включаючи безпарольну (FIDO), що захищає від крадіжки паролів, соціальної інженерії та фішин-атак
- Простий і легкий у повторному використанні токен OTP на різних платформах (iOS, Android)


FORTINET