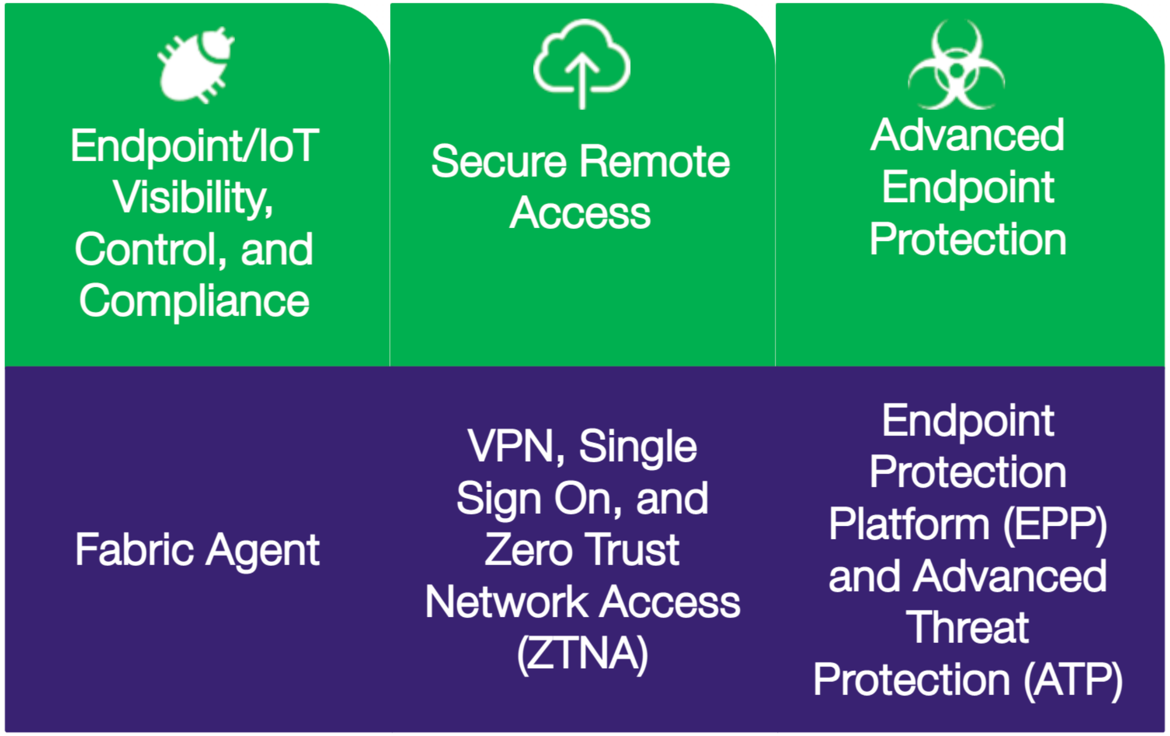
hackone

FORTICLIENT

NOME DO MENTOR: ALEXANDRE SABINO

O QUE É FORTICLIENT?



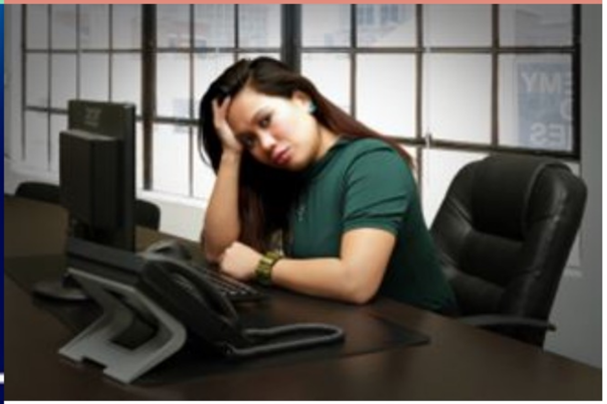
CASOS DE USO	Endpoint/IoT Visibility, Control, and Compliance	Secure Remote Access	Advanced Endpoint Protection
MÓDULOS ALINHADOS COM CASOS DE USO	Fabric Agent	VPN, Single Sign On, and Zero Trust Network Access (ZTNA)	Endpoint Protection Platform (EPP) and Advanced Threat Protection (ATP)

QUAIS PROBLEMAS O FORTICLIENT RESOLVE?

Lack of visibility

Vulnerable endpoints

Unsuspecting users



FABRIC-INTEGRATED ENDPOINT SECURITY

Visibilidade de Endpoint

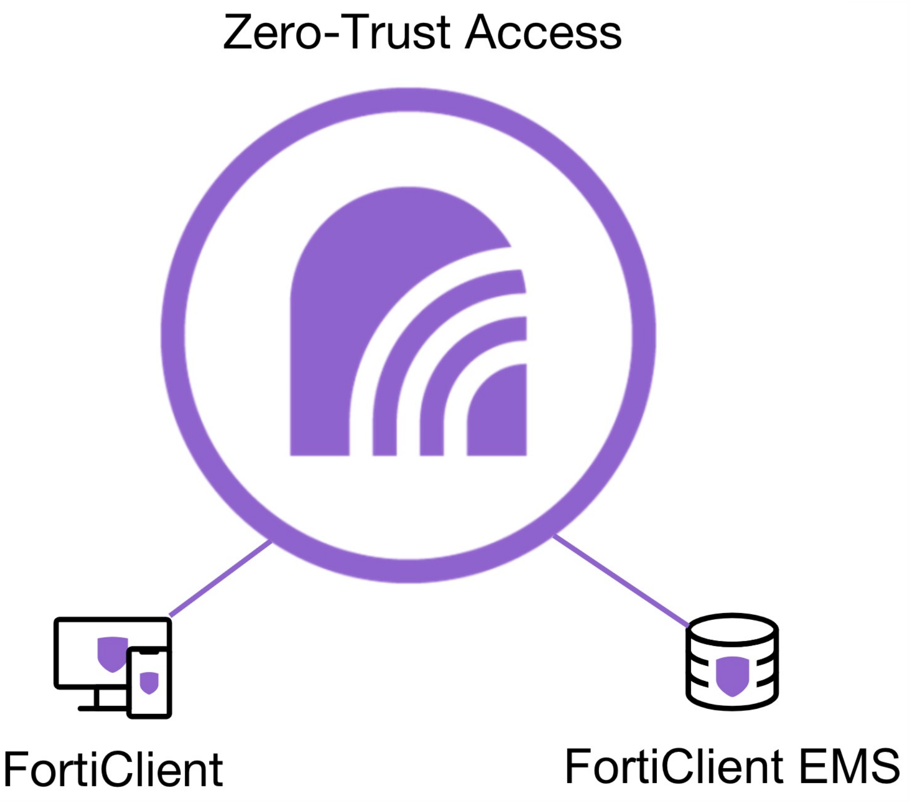
Telemetria de Endpoint
Postura de Segurança
Escaneamento de Vulnerabilidades

Control de Acesso Dinâmico

Agrupamento Dinâmico
Suporte baseado na intensão
Segmentação

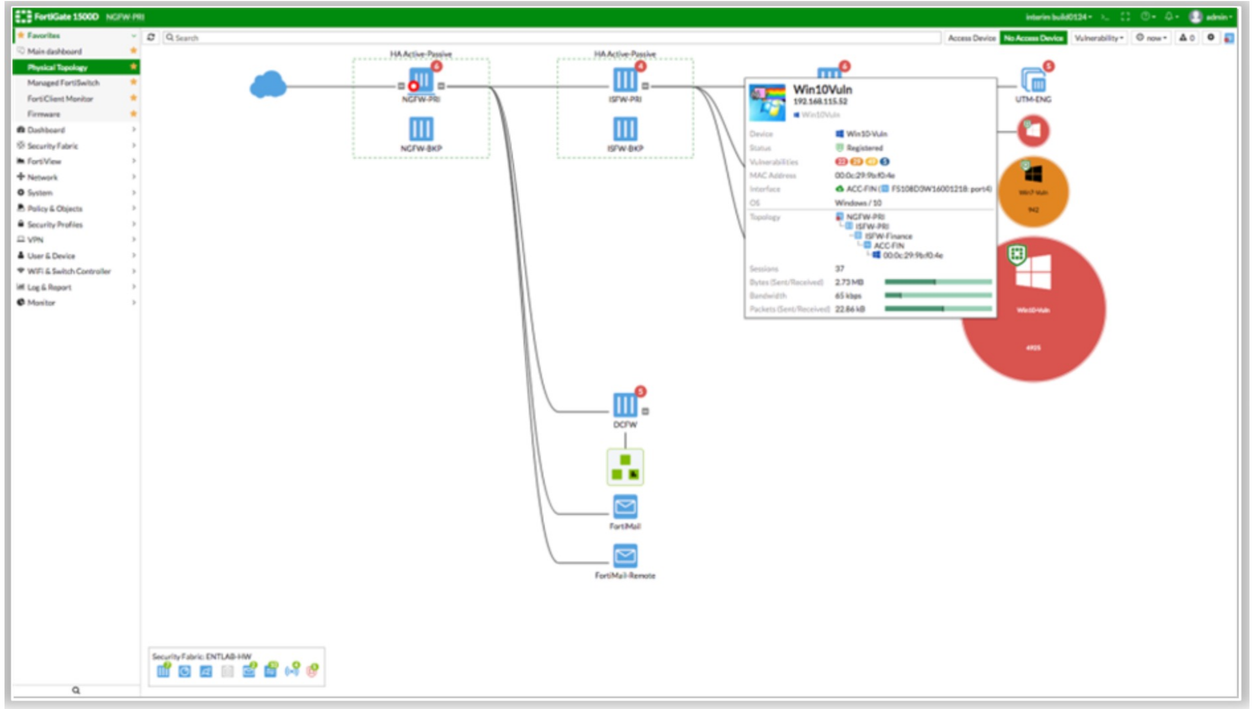
Proteção Proativa

ML-Based AV
Integração com Sandbox
Anti-exploit
Contenção Automatizada



VISIBILIDADE DO RISCO ATRAVÉS DA TELEMETRIA

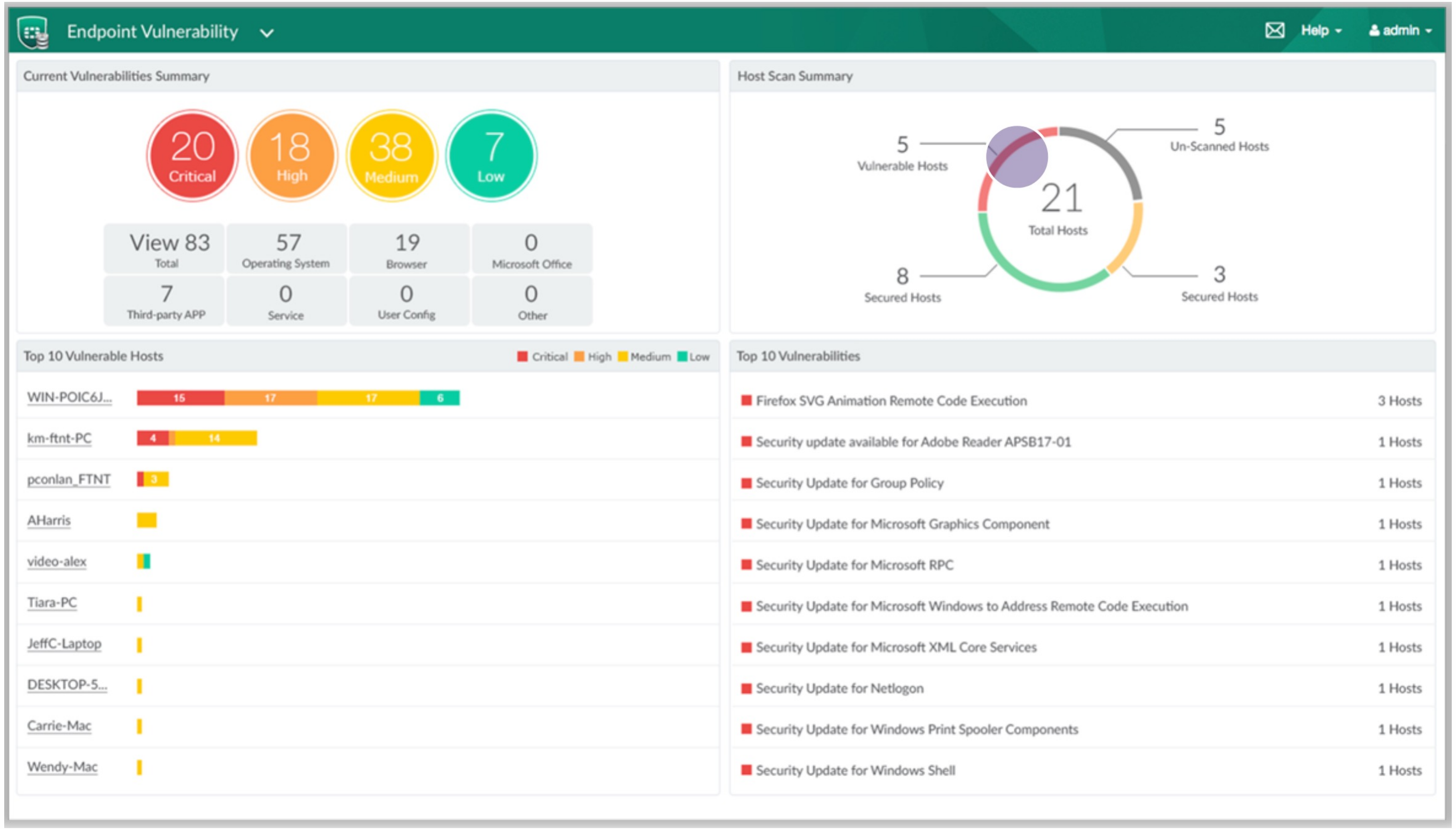
- Informação do Dispositivo
  - Sistema Operacional
  - Correlaciona múltiplos MAC
- Status do FortiClient
- Vulnerabilidades de Endpoint
- Usuários logados
- Avatar dos usuários
- Social IDs
- Online / Off-line
- Eventos e Logs dos Endpoints



Win10Vuln
192.168.115.52
Win10Vuln

Device: Win10-Vuln
Status: Registered
MAC Address: 00:0c:29:9b:f0:4e
Interface: ACC-FIN (FS108D0W16001218: port4)
OS: Windows / 10
Topology: NGFW-PRI
└ ISFW-PRI
 └ ISFW-Finance
  └ ACC-FIN
   └ 00:0c:29:9b:f0:4e
Sessions: 37
Bytes (Sent/Received): 2.73 MB
Bandwidth: 65 kbps
Packets (Sent/Received): 22.86 kB

DASHBOARD DE VULNERABILIDADES



Current Vulnerabilities Summary

View 83 Total	57 Operating System	19 Browser	0 Microsoft Office
7 Third-party APP	0 Service	0 User Config	0 Other

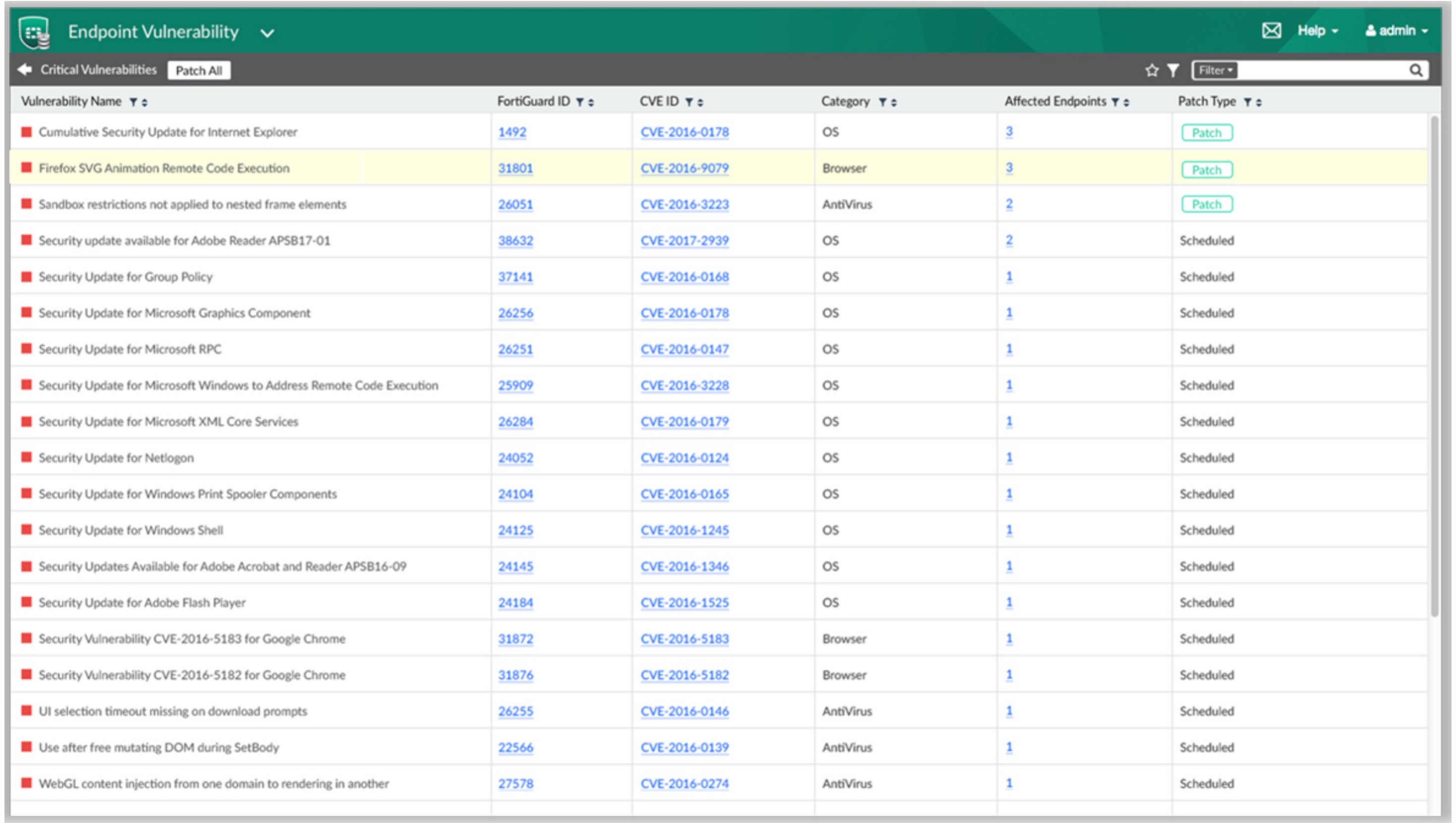
Host Scan Summary

Top 10 Vulnerable Hosts

Top 10 Vulnerabilities

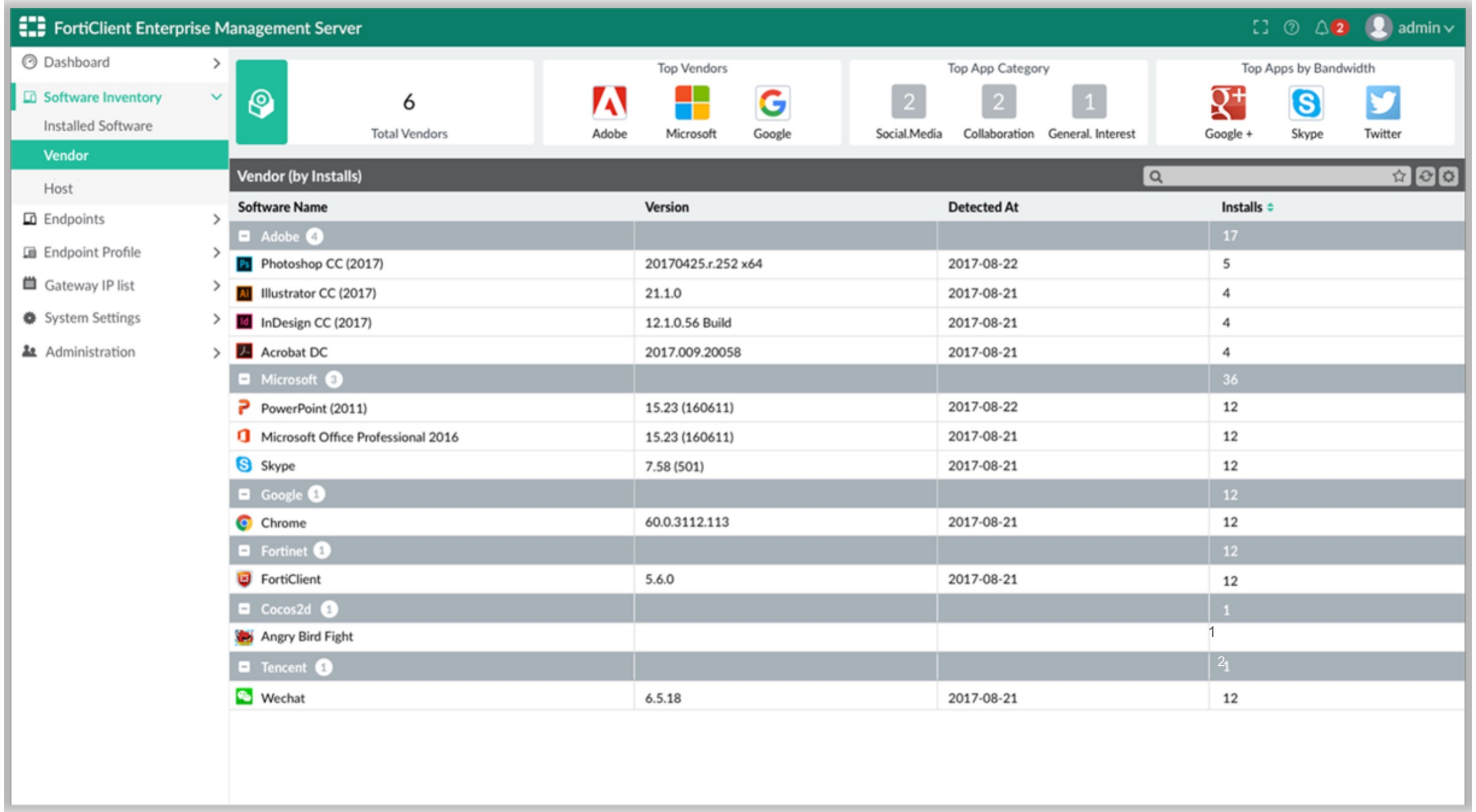
🟥 Firefox SVG Animation Remote Code Execution	3 Hosts
🟥 Security update available for Adobe Reader APSB17-01	1 Hosts
🟥 Security Update for Group Policy	1 Hosts
🟥 Security Update for Microsoft Graphics Component	1 Hosts
🟥 Security Update for Microsoft RPC	1 Hosts
🟥 Security Update for Microsoft Windows to Address Remote Code Execution	1 Hosts
🟥 Security Update for Microsoft XML Core Services	1 Hosts
🟥 Security Update for Netlogon	1 Hosts
🟥 Security Update for Windows Print Spooler Components	1 Hosts
🟥 Security Update for Windows Shell	1 Hosts

DASHBOARD DE VULNERABILIDADES



Vulnerability Name	FortiGuard ID	CVE ID	Category	Affected Endpoints	Patch Type
🟥 Cumulative Security Update for Internet Explorer	1492	CVE-2016-0178	OS	3	Patch
🟥 Firefox SVG Animation Remote Code Execution	31801	CVE-2016-9079	Browser	3	Patch
🟥 Sandbox restrictions not applied to nested frame elements	26051	CVE-2016-3223	AntiVirus	2	Patch
🟥 Security update available for Adobe Reader APSB17-01	38632	CVE-2017-2939	OS	2	Scheduled
🟥 Security Update for Group Policy	37141	CVE-2016-0168	OS	1	Scheduled
🟥 Security Update for Microsoft Graphics Component	26256	CVE-2016-0178	OS	1	Scheduled
🟥 Security Update for Microsoft RPC	26251	CVE-2016-0147	OS	1	Scheduled
🟥 Security Update for Microsoft Windows to Address Remote Code Execution	25909	CVE-2016-3228	OS	1	Scheduled
🟥 Security Update for Microsoft XML Core Services	26284	CVE-2016-0179	OS	1	Scheduled
🟥 Security Update for Netlogon	24052	CVE-2016-0124	OS	1	Scheduled
🟥 Security Update for Windows Print Spooler Components	24104	CVE-2016-0165	OS	1	Scheduled
🟥 Security Update for Windows Shell	24125	CVE-2016-1245	OS	1	Scheduled
🟥 Security Updates Available for Adobe Acrobat and Reader APSB16-09	24145	CVE-2016-1346	OS	1	Scheduled
🟥 Security Update for Adobe Flash Player	24184	CVE-2016-1525	OS	1	Scheduled
🟥 Security Vulnerability CVE-2016-5183 for Google Chrome	31872	CVE-2016-5183	Browser	1	Scheduled
🟥 Security Vulnerability CVE-2016-5182 for Google Chrome	31876	CVE-2016-5182	Browser	1	Scheduled
🟥 UI selection timeout missing on download prompts	26255	CVE-2016-0146	AntiVirus	1	Scheduled
🟥 Use after free mutating DOM during SetBody	22566	CVE-2016-0139	AntiVirus	1	Scheduled
🟥 WebGL content injection from one domain to rendering in another	27578	CVE-2016-0274	AntiVirus	1	Scheduled

INVENTÁRIO DE SOFTWARE



FortiClient Enterprise Management Server

admin

- Dashboard
- Software Inventory
  - Installed Software
  - Vendor
  - Host
- Endpoints
- Endpoint Profile
- Gateway IP list
- System Settings
- Administration

6 Total Vendors

Top Vendors: Adobe, Microsoft, Google

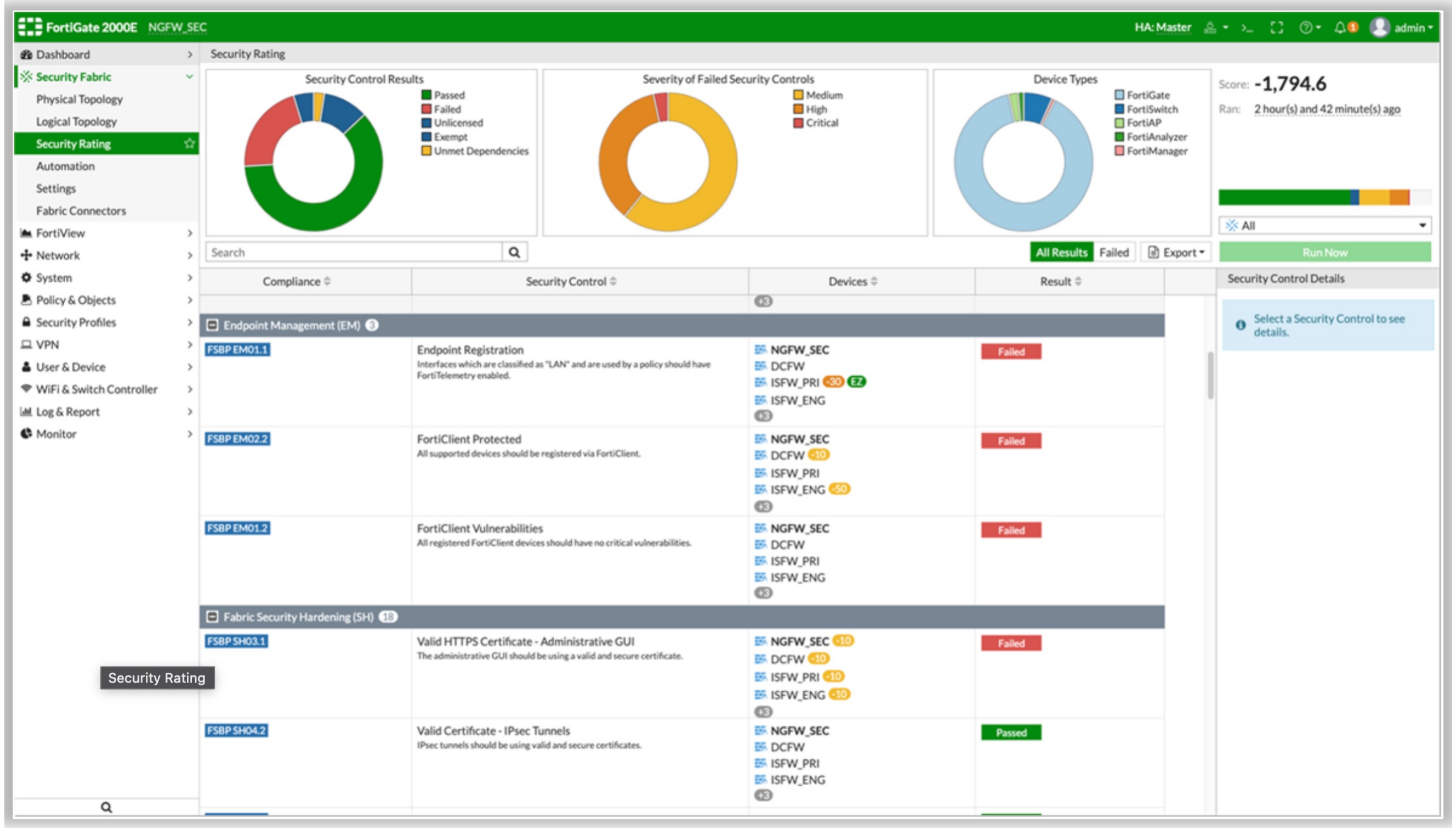
Top App Category: 2 Social.Media, 2 Collaboration, 1 General. Interest

Top Apps by Bandwidth: Google +, Skype, Twitter

Vendor (by Installs)

Software Name	Version	Detected At	Installs
Adobe 4			17
Photoshop CC (2017)	20170425.r.252 x64	2017-08-22	5
Illustrator CC (2017)	21.1.0	2017-08-21	4
InDesign CC (2017)	12.1.0.56 Build	2017-08-21	4
Acrobat DC	2017.009.20058	2017-08-21	4
Microsoft 3			36
PowerPoint (2011)	15.23 (160611)	2017-08-22	12
Microsoft Office Professional 2016	15.23 (160611)	2017-08-21	12
Skype	7.58 (501)	2017-08-21	12
Google 1			12
Chrome	60.0.3112.113	2017-08-21	12
Fortinet 1			12
FortiClient	5.6.0	2017-08-21	12
Cocos2d 1			1
Angry Bird Fight			1
Tencent 1			21
Wechat	6.5.18	2017-08-21	12

SECURITY RATING



Score: -1,794.6

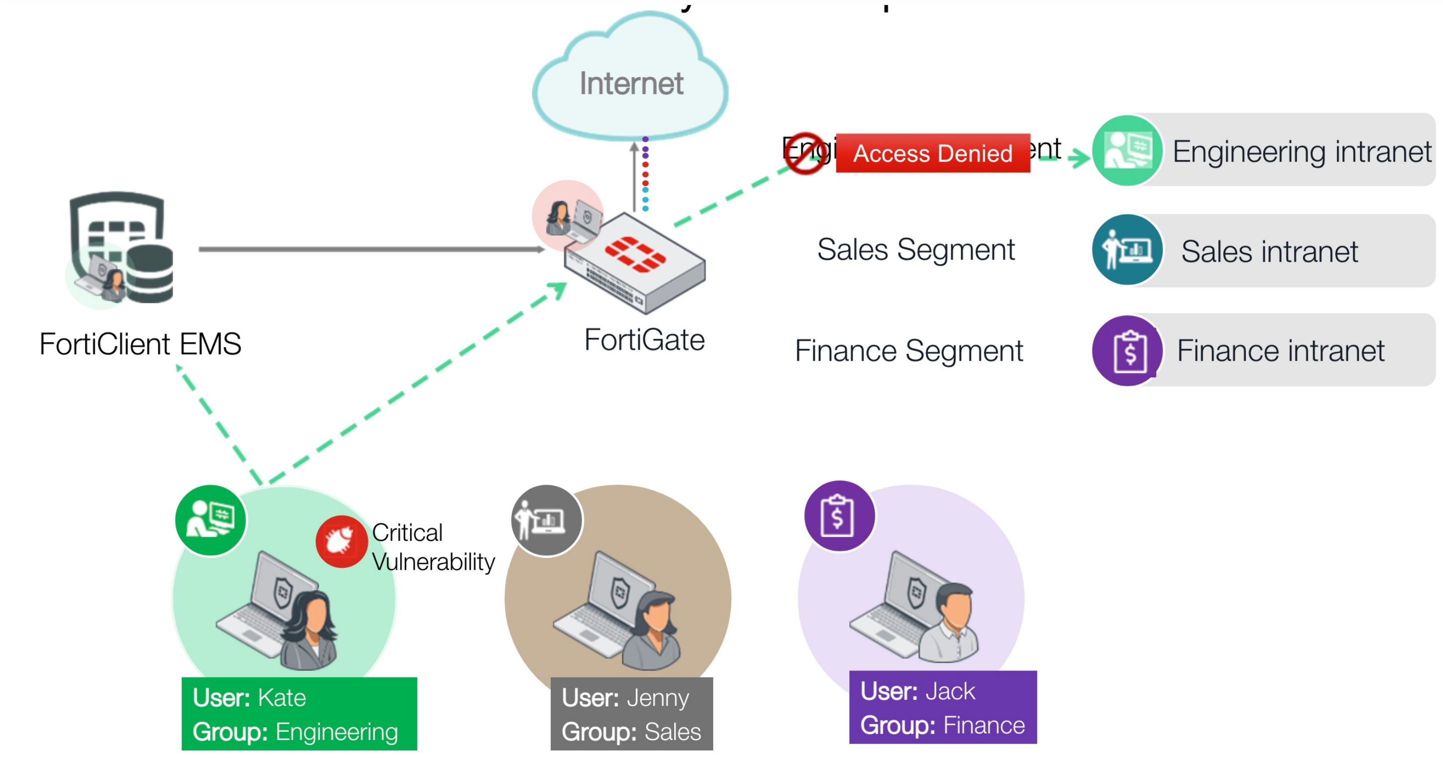
Ran: 2 hour(s) and 42 minute(s) ago

Select a Security Control to see details.

Compliance	Security Control	Devices	Result
		+3	
Endpoint Management (EM) 3			
FSBP EM01.1	Endpoint Registration Interfaces which are classified as "LAN" and are used by a policy should have FortiTelemetry enabled.	NGFW_SEC DCFW ISFW_PRI -30 EZ ISFW_ENG +3	Failed
FSBP EM02.2	FortiClient Protected All supported devices should be registered via FortiClient.	NGFW_SEC DCFW -10 ISFW_PRI ISFW_ENG -50 +3	Failed
FSBP EM01.2	FortiClient Vulnerabilities All registered FortiClient devices should have no critical vulnerabilities.	NGFW_SEC DCFW ISFW_PRI ISFW_ENG +3	Failed
Fabric Security Hardening (SH) 18			
FSBP SH03.1	Valid HTTPS Certificate - Administrative GUI The administrative GUI should be using a valid and secure certificate.	NGFW_SEC -10 DCFW -10 ISFW_PRI -10 ISFW_ENG -10 +3	Failed
FSBP SH04.2	Valid Certificate - IPsec Tunnels IPsec tunnels should be using valid and secure certificates.	NGFW_SEC DCFW ISFW_PRI ISFW_ENG +3	Passed

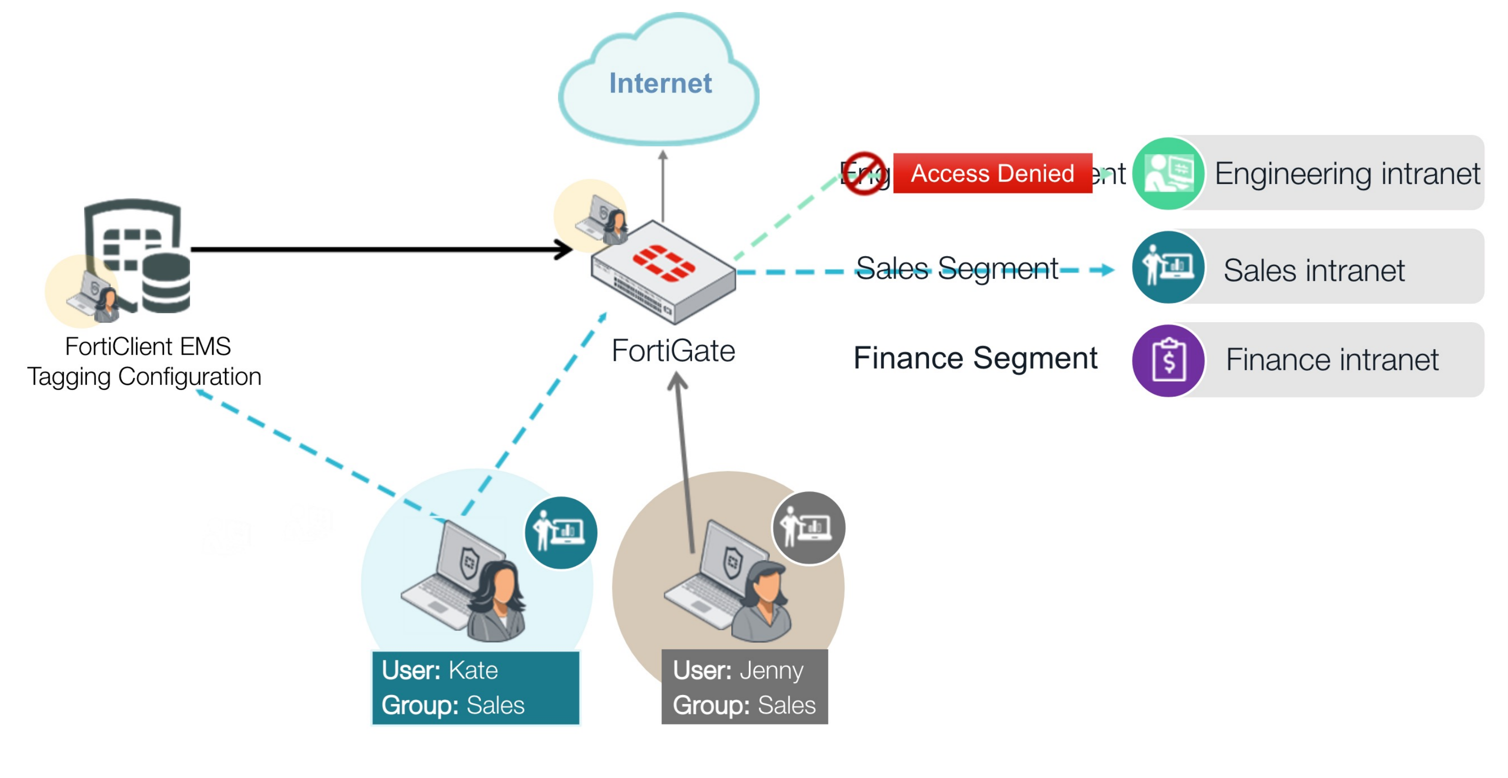
CONTROLE DE ACESSO DINÂMICO (INTENT-BASED SEGMENTATION)

CASOS DE USO: BLOQUEIA O ACESSO PELO RISCO DE SEGURANÇA DO ENDPOINT

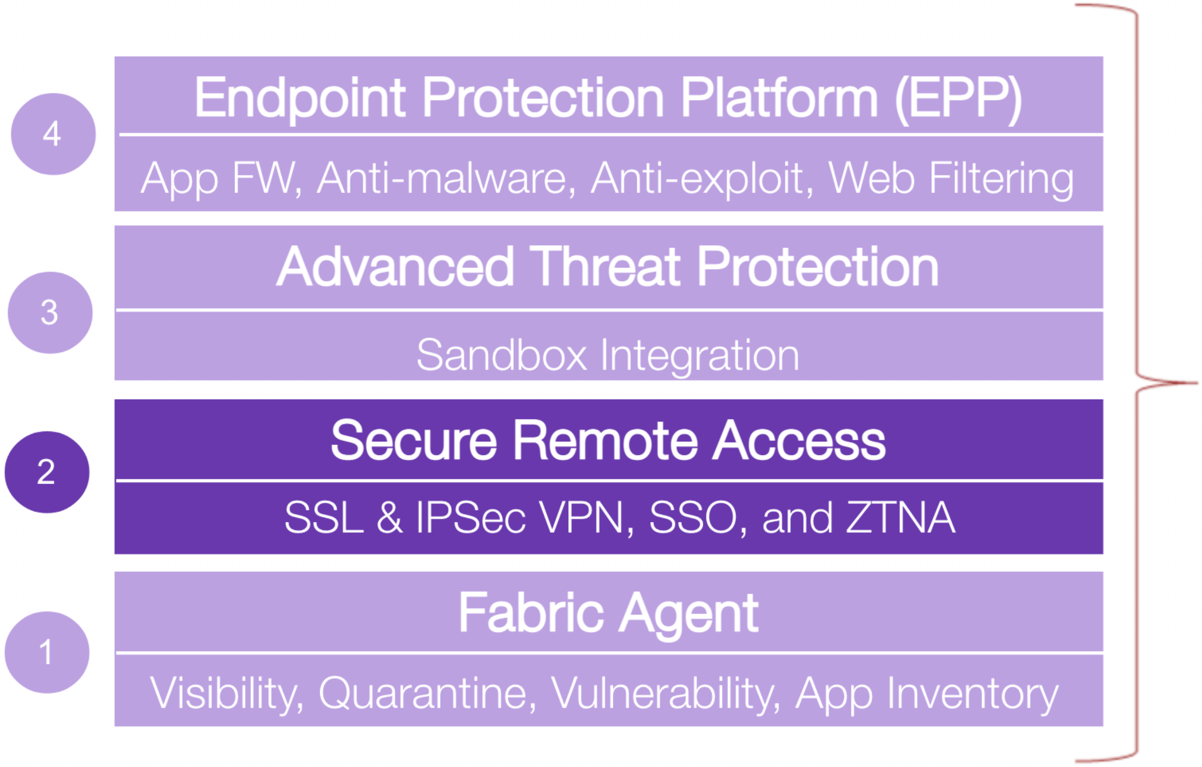


CONTROLE DE ACESSO DINÂMICO (INTENT-BASED SEGMENTATION)

CASOS DE USO: ACESSO BASEADO NOS GRUPOS DO AD



ACESSO REMOTO SEGURO



4 Endpoint Protection Platform (EPP)

App FW, Anti-malware, Anti-exploit, Web Filtering

3 Advanced Threat Protection

Sandbox Integration

2 Secure Remote Access

SSL & IPSec VPN, SSO, and ZTNA

1 Fabric Agent

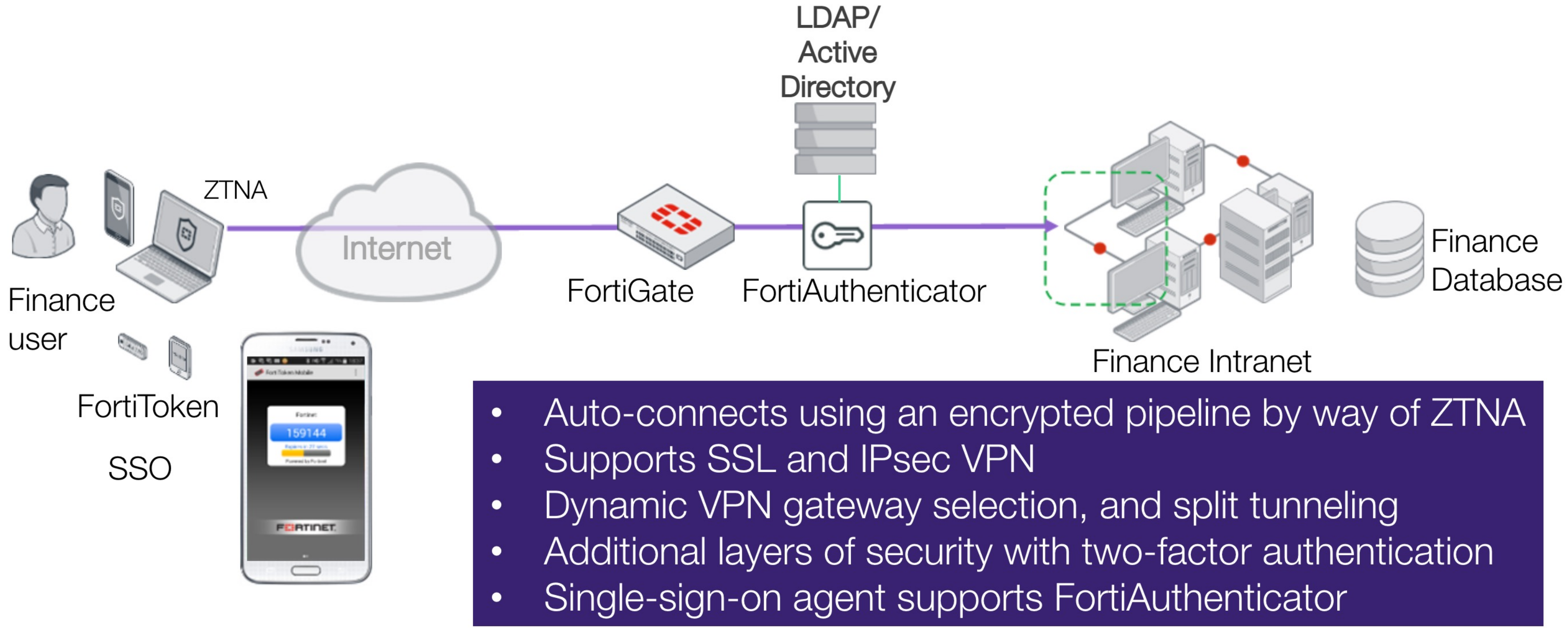
Visibility, Quarantine, Vulnerability, App Inventory

❖ **SUPORTA:**

- ➢ Secure Sockets Layer (SSL)
- ➢ Virtual Private Network (VPN)
- ➢ Single Sign-On
- ➢ Zero Trust Network Access (ZTNA)

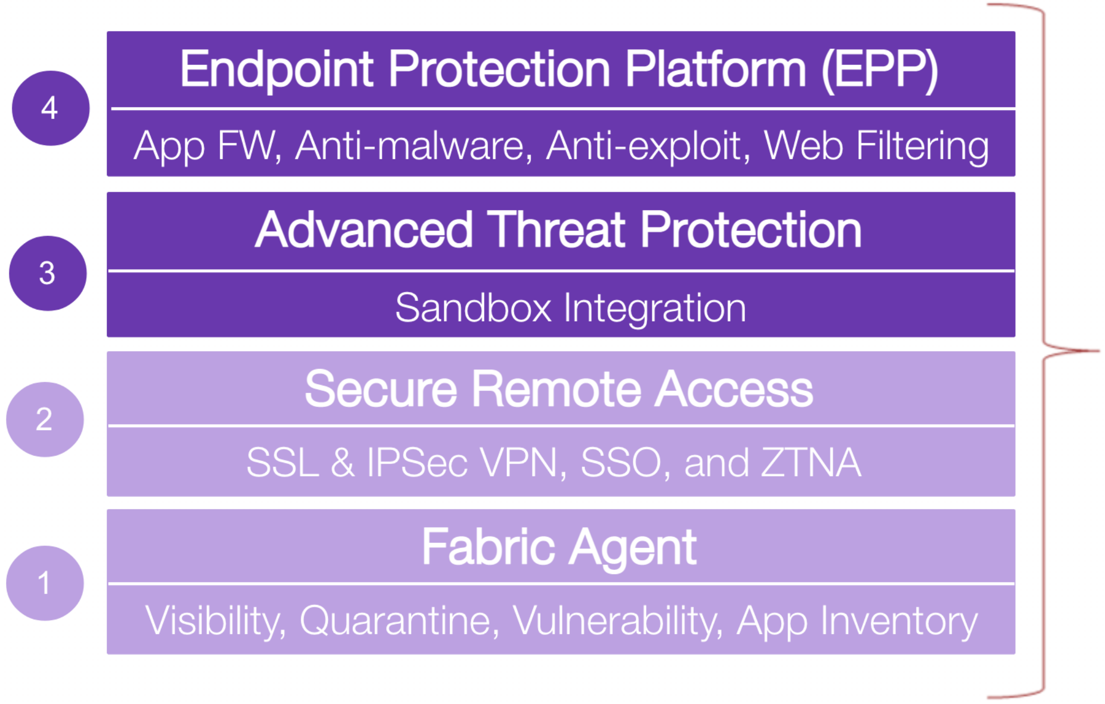
ACESSO REMOTO SECURO

ZTNA + Multi-Factor Authentication (MFA) + Single Sign On (SSO)



- Auto-connects using an encrypted pipeline by way of ZTNA
- Supports SSL and IPsec VPN
- Dynamic VPN gateway selection, and split tunneling
- Additional layers of security with two-factor authentication
- Single-sign-on agent supports FortiAuthenticator

DEFESA PROATIVA DO ENDOPOINT



4 Endpoint Protection Platform (EPP)

App FW, Anti-malware, Anti-exploit, Web Filtering

3 Advanced Threat Protection

Sandbox Integration

2 Secure Remote Access

SSL & IPSec VPN, SSO, and ZTNA

1 Fabric Agent

Visibility, Quarantine, Vulnerability, App Inventory

- ➢ Compact Pattern Recogntion Language (CPRL)
  - Uma engine anti-malware baseada em padrões
- ➢ Anti-Exploit
- ➢ Web Filtering
- ➢ Firewall de aplicação
- ➢ Integração com Sandbox

DETECTA E BLOQUEIA MALWARES E AMEAÇAS AVANÇADAS

Anti-Malware

- Engine Anti-Malware baseada em padrões
- Detecta Malware Polifórmicos
- Bloqueia canais de ataques conhecidos e websites maliciosos
- Análise Big Data, Machine Learning e inteligência artificial na nuvem

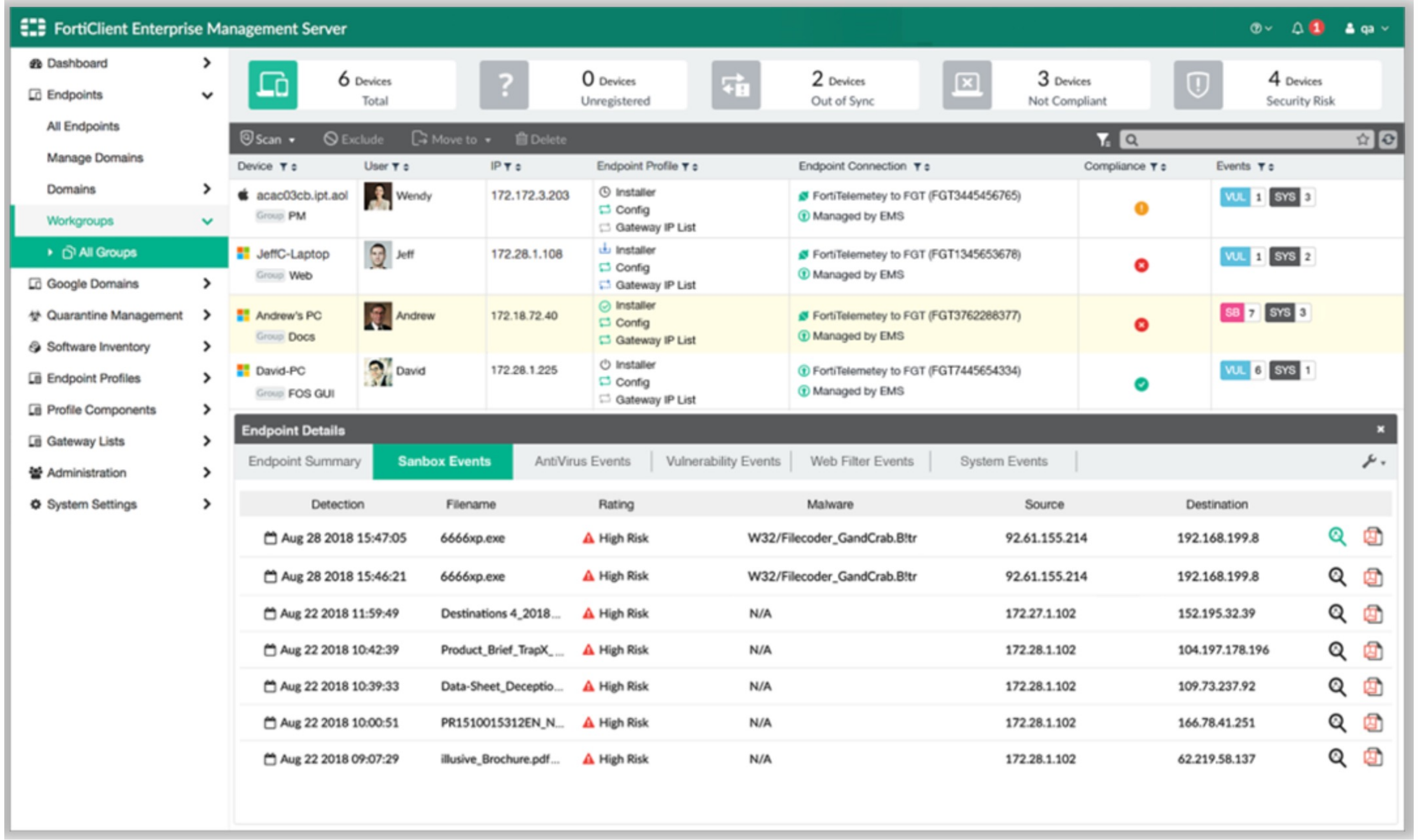
Anti-Exploits

- Detecção baseada em comportamento
- Pode detectar malware e ransomware avançados
- Prevê ataques que aproveitam PowerShell e outros scripts

Integração com Sandbox

- Detecta Malware avançado ou customizado
- Submissão automática de arquivos para análise
- Compartilhamento inteligente de ameaças

INTEGRAÇÃO AVANÇADA COM SANDBOX



Device	User	IP	Endpoint Profile	Endpoint Connection	Compliance	Events
acac03cb.ipt.aol Group PM	Wendy	172.172.3.203	Installer Config Gateway IP List	FortiTelemetey to FGT (FGT3445456765) Managed by EMS	●	VUL 1 SYS 3
JeffC-Laptop Group Web	Jeff	172.28.1.108	Installer Config Gateway IP List	FortiTelemetey to FGT (FGT1345653678) Managed by EMS	✕	VUL 1 SYS 2
Andrew's PC Group Docs	Andrew	172.18.72.40	Installer Config Gateway IP List	FortiTelemetey to FGT (FGT3762288377) Managed by EMS	✕	SB 7 SYS 3
David-PC Group FOS GUI	David	172.28.1.225	Installer Config Gateway IP List	FortiTelemetey to FGT (FGT7445654334) Managed by EMS	✓	VUL 6 SYS 1

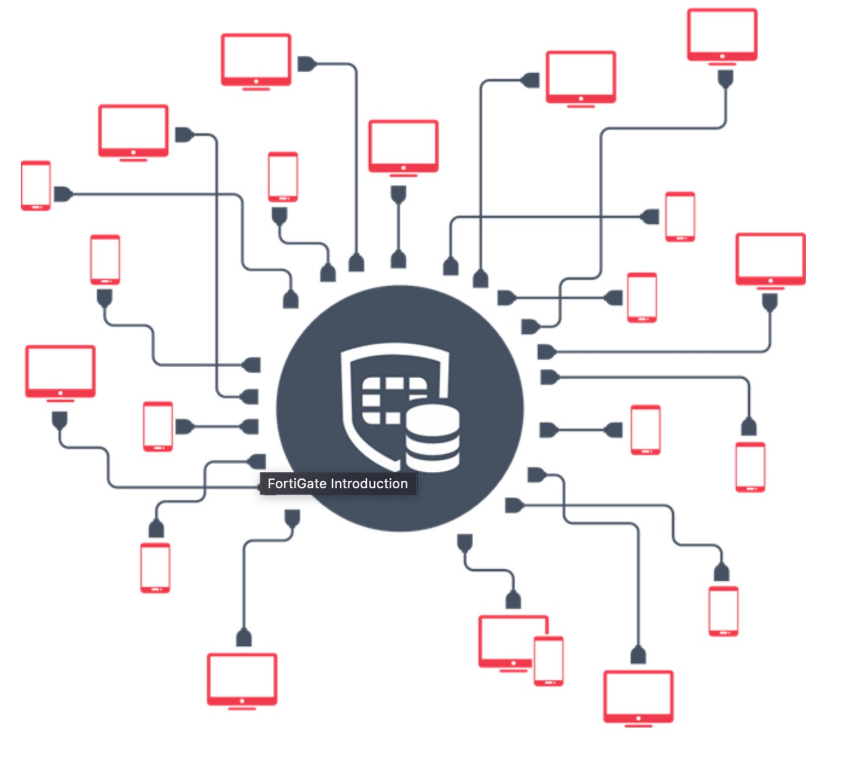
Detection	Filename	Rating	Malware	Source	Destination
Aug 28 2018 15:47:05	6666xp.exe	High Risk	W32/Filecoder_GandCrab.B!tr	92.61.155.214	192.168.199.8
Aug 28 2018 15:46:21	6666xp.exe	High Risk	W32/Filecoder_GandCrab.B!tr	92.61.155.214	192.168.199.8
Aug 22 2018 11:59:49	Destinations 4_2018...	High Risk	N/A	172.27.1.102	152.195.32.39
Aug 22 2018 10:42:39	Product_Brief_TrapX_...	High Risk	N/A	172.28.1.102	104.197.178.196
Aug 22 2018 10:39:33	Data-Sheet_Deceptio...	High Risk	N/A	172.28.1.102	109.73.237.92
Aug 22 2018 10:00:51	PR1510015312EN_N...	High Risk	N/A	172.28.1.102	166.78.41.251
Aug 22 2018 09:07:29	illusive_Brochure.pdf...	High Risk	N/A	172.28.1.102	62.219.58.137

WEB FILTERING E FIREWALL DE APLICAÇÃO

- **Web Filtering**
  - Segurança Web e Filtro de conteúdo
  - Política de uso web aceitável
  - Suportado por Windows, Mac, Chromebook, Android e IOS
  - 75+ Categorias
  - Categorias consistentes como no FortiGate

- **Firewall de Aplicação**
  - Monitora e controla o tráfego das aplicações por categoria
  - Bloqueia o tráfego de aplicações não desejadas tais como Botnet e mineração
  - Suportado por Windows, Mac, Chromebook, Android e IOS
  - 75+ Categorias
  - Controla aplicativos proxy e aplicativos de mensagens HTTPS, tais como Web Mail

GERENCIAMENTO CENTRALIZADO COM EMS



- **ENTEPRISE MANAGEMENT SERVER**
  - Configura, implanta e gerencia o FortiClient
    - Integra com LDAP e outros sistemas corporativos
  - Monitora endpoints em tempo real
  - Resumo das ameaças, notificações e alertas
  - Ações Remotas
    - Anti-malware scanning
    - Escaneamento de vulnerabilidades
    - Quarentena de Endpoints
  - Inventário de software
  - Gerenciamento de arquivos em quarentena
  - Altamente escalável

hackone