QUESTIONAMENTOS: Edital PE 1301017 000049/2018,:

1.3. A console de monitoração e configuração deverá ser feita através de uma central única, baseada em web e em nuvem, que deverá conter todas as fermentas para a monitoração e controle da proteção dos dispositivos;

R: 1.2.5. Web Console (Control Center), inicia na página 4 do manual Bitdefender_Gravityzone_Administrator_7
2. GETTING STARTED inicia na página 13

1.7. Deve permitir sincronização com o Active Directory (AD), para gestão de usuários e grupos integrados às políticas de proteção;

R:
4.2.3. Organizing Computers into Groupsm, inicia na página 41 do manual Bitdefender_Gravityzone_Administrator_7
4.2.9. Synchronizing with Active Directory , inicia na página 72 do manual Bitdefender_Gravityzone_Administrator_7

1.10. Deve a console ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando;

R: 5. SECURITY POLICIES inicia na página 159
5.1. Managing Policies inicia na página 160
Todos no manual Bitdefender_Gravityzone_Administrator_7

1.13. A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs;

R: Power User página 10
5.2.1. General inicia na página 172
Power User inicia na página 178
Todos no do manual Bitdefender_Gravityzone_Administrator_7

1.19. Permitir a exportação dos relatórios gerenciais para os formatos CSV e PDF;

R: 7. USING REPORTS inicia na página 301
7.2. Creating Reports inicia na página 313
7.8. Report Builder inicia na página 321
7.8.3 Viewing and Managing Reports inicia na página 329
Todos no do manual Bitdefender_Gravityzone_Administrator_7

1.42. Deverá permitir exportar o relatório de logs de auditoria nos formatos CSV e PDF;

R:
7. USING REPORTS inicia na página 301
7.2. Creating Reports inicia na página 313
7.8. Report Builder inicia na página 321

7.8.3 Viewing and Managing Reports inicia na página 329
Visibility inicia pagina 354
Todos no manual Bitdefender_Gravityzone_Administrator_7

1.47.2. Atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possam ser liberadas ou bloqueadas;

R:
Endpoint Events inicia na página 323
7.8.2. Managing Queries inicia na página 324
Todos no manual Bitdefender_Gravityzone_Administrator_7

1.47.3. Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;

R:
Blocked Applications inicia na página 326
Todos no manual Bitdefender_Gravityzone_Administrator_7

1.47.6. Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;

R: Firewall inicia na página 8
Content Control inicia na página 9
5.2.5. Content Control inicia na página 224
Applications inicia na página 234
5.2.6. Application Control inicia na pagina 236
Todos no manual Bitdefender_Gravityzone_Administrator_7

1.47.7. Deve possuir a opção de customizar, uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;

R:
10.4. Configuring Notification Settings inicia na página 352
Notifications inicia na página 174
Application Control inicia na página 177
5.2.6. Application Control inicia na página 236
Process Start Rules inicia pagina 237
Firewall event pagina 348
Todos no manual Bitdefender_Gravityzone_Administrator_7

1.48.1. Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;

R:
Data Protection inicia na página 232
Security for Endpoints inicia na página 1
5.2.7. Device Control inicia na pagina 241
Todos no manual Bitdefender_Gravityzone_Administrator_7

1.48.2. Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);

R:

Início na página 233 manual Bitdefender_Gravityzone_Administrator_7

1.48.3. Possibilitar o bloqueio, somente registrar o evento na Console de Administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

R:

5.2.7. Device Control inicia na pagina 241 manual Bitdefender_Gravityzone_Administrator_7

1.48.4. Deve possuir listas de CCLs pré-configuradas com no mínimo as seguintes identificações:
1.48.4.1. Números de cartões de crédito;
1.48.4.2. Números de contas bancárias;
1.48.4.3. Números de Passaportes;
1.48.4.4. Endereços;
1.48.4.5. Números de telefone;
1.48.4.6. Códigos postais definidas por países como França, Inglaterra, Alemanha, EUA, etc;
1.48.4.7. Lista de e-mails;

R:

Data Protection inicia na página 232 manual Bitdefender_Gravityzone_Administrator_7

1.48.5. Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;

R:

5.2.5. Content Control inicia na página 224 manual Bitdefender_Gravityzone_Administrator_7

1.48.6. Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo;

R:

5.2.7. Device Control inicia na página 241 manual Bitdefender_Gravityzone_Administrator_7

1.48.7. Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;

R:

Content Control
Application Control
Device Control inicia na página 9 manual Bitdefender_Gravityzone_Administrator_7

Funcionalidades não encontradas.

1.49.5. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas; (antimalware)

R:
Feito através do antimalware
Antimalware Inicia na página 7 manual Bitdefender_Gravityzone_Administrator_7

3.1.13. Windows Server 2016;
R:
Supported Operating Systems inicia pag 20 no Bitdefender_GravityZone_InstallationGuide_7_enUS

3.1.18. Amazon Linux;
Add on
https://www.bitdefender.com.br/support/how-to-set-up-the-gravityzone-integration-with-amazon-ec2-using-cross-accounts-2035.html

https://www.bitdefender.com/support/how-to-set-up-bitdefender-security-for-aws-1047.html

3.1.26. Deve possuir integração com as nuvens da Microsoft Azure (SOMENTE NA CONSOLE) e Amazon Web Services para identificar as informações dos servidores instanciados nas nuvens;

https://www.bitdefender.com/support/installing-bitdefender-security-server-in-microsoft-azure-1839.html
add on

3.2.6. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;
R:
Security for Endpoints inicia na página 1
Advanced Threat Control inicia na página 8 manual Bitdefender_Gravityzone_Administrator_7