Implementação de políticas de ATP - Standard

Descrição

A Proteção Avançada contra Ameaças do Microsoft 365 (ATP) protege sua organização contra ameaças maliciosas, que são enviadas por mensagens de e-mail, links (URLs) e ferramentas de colaboração. Com o Office 365 ATP, a equipe de segurança da sua organização pode configurar as medidas de proteção definindo políticas no Centro de Conformidade e Segurança do Office 365 para proteger o ambiente de ameaças e invasões.

Público Alvo

Esse recurso se aplica para todos os clientes que possuem o Microsoft 365 Business. Há muitas maneiras de usar a Proteção de Ameaças do Office 365 para classificar e, opcionalmente, proteger os documentos e os e-mails da sua organização.

Vantagens

- Políticas de proteção contra ameaças
- Relatórios
- Recursos de investigação e resposta de ameaças
- Recursos de investigação e resposta automatizadas

Escopo do Serviço

- Anexos seguros
- Links seguros
- ATP para SharePoint, OneDrive e Microsoft Teams
- Proteção avançada

Tempo de configuração

Aproximadamente 10 horas comerciais (não havendo intervenções).

Consumo

- Plano Microsoft 365 Business

! Antes de começar valide se o cliente tem o plano certo par a implantação do serviço, este tutorial contempla recursos do plano **ATP 1.**

Todos os recursos estão listados abaixo. Quando o Exchange Online é mencionado, ele normalmente refere-se à família de serviços do Office 365 Enterprise.

Recurso	Plano ATP 1 (anteriormente ATP autônomo)	Plano ATP 2 (anteriormente inteligência de ameaças autônomo	Office 365 Enterprise E5
Configuração, proteção e detecção			
Anexos seguros	Sim	Sim	Sim
Anexos seguros no Teams	Sim	Sim	Sim
Links seguros	Sim	Sim	Sim
Links seguros no Teams	Sim	Sim	Sim
ATP para SharePoint, OneDrive e Microsoft Teams	Sim	Sim	Sim
Políticas anti-phishing	Sim	Sim	Sim
Relatórios em tempo real	Sim	Sim	Sim
Automação, investigação, correção e educação			
Rastreadores de ameaças	Não	Sim	Sim
Investigação de ameaças (investigação avançada de ameaças)	Detecção em tempo real	Explorer	Explorer
Resposta de incidente automatizada	Não	Sim	Sim
Simulador de ataque	Não	Sim	Sim