Como consultor de segurança em nuvem, eu destacaria os seguintes recursos de segurança da AWS como fundamentais para proteger os dados sensíveis da empresa durante a migração para a nuvem:

1. **AWS Identity and Access Management (IAM)**: O IAM é um recurso de segurança essencial que permite controlar o acesso aos recursos da AWS. Ele permite criar usuários e grupos, atribuir permissões e políticas de acesso, e gerenciar chaves de acesso. Isso garante que apenas os usuários autorizados tenham acesso aos dados sensíveis.
2. **AWS Key Management Service (KMS)**: O KMS é um serviço de gerenciamento de chaves que permite criar, gerenciar e usar chaves de criptografia para proteger os dados sensíveis. Ele oferece uma solução de criptografia robusta e escalável para proteger os dados em repouso e em trânsito.
3. **AWS Security Groups**: Os Security Groups são uma forma de controlar o tráfego de rede para e desde as instâncias EC2. Eles permitem definir regras de segurança para controlar o acesso às instâncias e aos recursos da AWS.
4. **AWS CloudTrail**: O CloudTrail é um serviço de auditoria que registra todas as atividades da AWS, incluindo as chamadas de API, as alterações de configuração e as atividades de segurança. Isso permite monitorar e auditar as atividades da AWS para detectar e responder a incidentes de segurança.
5. **AWS GuardDuty**: O GuardDuty é um serviço de detecção de ameaças que utiliza inteligência artificial e machine learning para detectar e alertar sobre atividades suspeitas e ameaças à segurança. Ele pode ajudar a identificar e responder a incidentes de segurança em tempo real.

Além disso, eu recomendaria as seguintes melhores práticas de segurança para a empresa durante a migração para a AWS:

1. **Uso de criptografia**: Utilizar criptografia para proteger os dados sensíveis em repouso e em trânsito. Isso pode ser feito utilizando o KMS para gerenciar chaves de criptografia.
2. **Monitoramento de segurança**: Utilizar o CloudTrail e o GuardDuty para monitorar e auditar as atividades da AWS e detectar incidentes de segurança.
3. **Controle de acesso**: Utilizar o IAM para controlar o acesso aos recursos da AWS e garantir que apenas os usuários autorizados tenham acesso aos dados sensíveis.
4. **Segurança de rede**: Utilizar Security Groups para controlar o tráfego de rede e garantir que apenas o tráfego autorizado tenha acesso às instâncias EC2.
5. **Treinamento e conscientização**: Treinar os funcionários sobre as melhores práticas de segurança em nuvem e conscientizá-los sobre a importância da segurança dos dados sensíveis.

Em resumo, a AWS oferece uma ampla gama de recursos de segurança para proteger os dados sensíveis da empresa durante a migração para a nuvem. Ao utilizar esses recursos e seguir as melhores práticas de segurança, a empresa pode garantir a segurança e a integridade dos seus dados sensíveis na nuvem.