Transição do Secure Cloud Analytics para o Cisco XDR

Contents

A principal mudança

A experiência do usuário do Secure Cloud Analytics não estará mais disponível em 24 de outubro de 2026. O Cisco XDR torna-se a interface operacional para detecções derivadas de SCA, investigações, contexto de ativos, notificações, exportações e fluxos de trabalho relacionados.

⚠ Caution: O programa de transição do cliente SCA para XDR dedicado está programado para ser encerrado em 30 de setembro, enquanto 24 de outubro de 2026 continua sendo a data prevista para a reprovação planejada da interface do usuário do SCA. Ative o Cisco XDR agora para que sua equipe possa concluir as ações de preparação descritas abaixo.

Ações imediatas e datas críticas

O que está acontecendo e o que devo fazer agora?

Status	Ação exigida
Detalhes	A Cisco está encerrando a experiência do usuário do SCA e movendo os recursos derivados do SCA para o Cisco XDR. A telemetria e a análise se tornam parte de fluxos de trabalho XDR mais amplos para atividades, detecções, incidentes, investigação, contexto de ativos, resposta e automação.
Ação do cliente	Ative o XDR, conecte o locatário SCA, valide o acesso, use Detecções e Incidentes XDR para operações diárias, use Atividades para transferências de telemetria de origem, teste fluxos de trabalho XDR e exporte informações históricas antes de 24 de outubro de 2026.

Quais datas devo planejar?

Data	Etapa	O que isso significa
15 de setembro de 2026	Configuração do AWS e do Azure para clientes selecionados	Os clientes afetados dos EUA e EMEA migram para o método de configuração XDR recomendado.
30 de setembro de 2026	O programa dedicado de transição do cliente SCA para XDR é fechado	Conclua as ações de qualificação, provisionamento e preparação antes do encerramento do programa.
7 de outubro de 2026	Detecções de AWS CloudTrail, Log de Atividades do Azure e Log de Auditoria do GCP interrompidas	Opere essas fontes no XDR.
14 de outubro de 2026	Detecções de eventos personalizados interrompidas; Configuração de Ajuste de Incidente, Listas de Controle e Grupos de Entidades disponível no XDR	Mover fluxos de trabalho e configurações relacionados para XDR
21 de outubro de 2026	Detecções do NetFlow interrompidas	Operar detecções do NetFlow no XDR
24 de outubro de 2026	A experiência do usuário do SCA não está mais disponível	Conclua a transferência para o XDR e exporte os dados históricos antes desta data.

O que acontece se eu não fizer nada ou não tiver provisionado o XDR?

Status	Não recomendado
Detalhes	Se você não ativar e conectar o Cisco XDR antes que a experiência do usuário do SCA seja removida, você perderá o acesso ao SCA e não terá a experiência XDR de substituição disponível para seus fluxos de trabalho, detecções, investigações, integrações ou dados históricos derivados do SCA. A espera também compacta a ativação, a configuração do usuário, a validação do fluxo de trabalho e a alteração operacional na parte final da transição.
Ação do cliente	Ative e conecte o XDR agora para que sua equipe possa concluir a configuração do usuário, a validação do fluxo de trabalho e a preparação para exportação antes de 30 de setembro de 2026. A interface SCA continua sendo alvo de depreciação

	em 24 de outubro de 2026; sem um locatário XDR conectado, não há experiência de XDR de substituição disponível quando o acesso SCA termina.

O que está sendo desativado, alterado ou não está disponível

Quais conceitos do SCA não continuam explicitamente da mesma forma?

Status	Alteração ou descontinuação
Detalhes	• Experiência do usuário SCA: removido em 24 de outubro de 2026. • Comportamento de webhook SCA legado: substituído por fluxos de trabalho XDR. • Experiência de observação SCA: não é um recurso XDR de um para um. • Sensibilidade da sub-rede: por conceitos de priorização do valor dos ativos. • Grupos de entidades: substituídos por rótulos de ativos, grupos de ativos e pontuação de valor. • Configurações de detecção adiadas: não migrado; use o Ajuste de incidentes quando disponível. • Comportamento de prioridade de alerta controlado pelo cliente: não retido. • Alguns relatórios, páginas de menor uso e funções: aposentado ou substituído por experiências nativas de XDR.

Quais itens de relatório ou integração devem ser substituídos ou movidos?

Status	Alteração esperada
Detalhes	Exemplos incluem lista de monitoramento de postura de nuvem, monitoramento Kubernetes, experiências de visualização/painel/pesquisa de sessão/pesquisa de IP da AWS, integrações de contexto Meraki e Umbrella, relatórios mensais baseados em e-mail e resumos de alertas diários. Esta lista não promete uma substituição individual para cada página herdada.

O que não está sendo solicitado de mim nesta migração?

Status	Nenhuma ação deste tipo
Detalhes	A Cisco não está pedindo aos clientes para reimplantar sensores de rede existentes, reconfigurar a inclusão de logs de nuvem exclusivamente para a migração do UX, recriar manualmente objetos de configuração de detecção padrão suportados ou reter o SCA como um console paralelo de longo prazo.

Lista de verificação de prontidão do cliente

1. Ative o Cisco XDR e conecte o locatário SCA existente antes de 30 de setembro de 2026 para que sua equipe possa concluir as ações de preparação antes do encerramento do

programa de transição.
2. Crie usuários, valide a entrada e confirme o acesso apropriado no XDR.
3. Analisar detecções, incidentes, atividades, investigação e informações sobre ativos/informações sobre dispositivos.
4. Mapeie cada webhook SCA, exportação, notificação, entrega SIEM/SOAR e automação personalizada para fluxos de trabalho XDR ou outra superfície operacional XDR.
5. Valide a telemetria de origem necessária em Atividades à medida que cada origem se torna disponível.
6. Valide as detecções necessárias e os manuais de atividades de resposta antes de cada transição de origem.
7. Analisar a sensibilidade da sub-rede, grupos de entidades, adiamento, prioridade de alerta, listas de controle, regras de scanner, redes confiáveis e priorização do valor do ativo.
8. Inventariar relatórios antigos, páginas somente SCA e dependências de API; identificar alternativas ou requisitos de exportação.
9. Exporte os alertas, observações, registros brutos, registros de configuração e relatórios necessários antes de 24 de outubro de 2026.

Encontrando seu caminho na nova experiência XDR

Os clientes SCA têm direito ao Cisco XDR?

Status	Disponível como parte da transição
Detalhes	Os clientes atuais do SCA têm direito ao Cisco XDR como parte da transição. O resultado pretendido é um valor de SCA contínuo, enquanto os fluxos de trabalho principais são transferidos para o XDR.
Ação do cliente	Ative o Cisco XDR, conecte o locatário SCA existente e use o processo de ativação do Cisco XDR se precisar de assistência.

Onde as funções do SCA chegam ao Cisco XDR?

função SCA	destino XDR
Alertas e fluxos de trabalho de alerta	Detecções e incidentes de XDR
Observações e investigação orientada para eventos	Atividades XDR e Investigação XDR
Visualizador de Eventos	Atividades e investigação de XDR
Contexto do dispositivo	Insights de ativos / Insights de dispositivos
Ganchos da Web, avisos, exportações e entrega de downstream	Fluxos de trabalho XDR
Configuração de detecção	A configuração do XDR ocorre quando cada configuração atinge seu marco

O SCA permanecerá disponível como um console de uso diário paralelo?

Status	No
Detalhes	A experiência do usuário do SCA está programada para ser removida em 24 de outubro de 2026. Use o período de sobreposição para praticar o modelo operacional XDR, validar fluxos de trabalho e atualizar runbooks.

Detecções, incidentes e casos de uso de observação

As detecções estão simplesmente se movendo um para um?

Status	Alteração de modelo
Detalhes	Não. A Cisco está desenvolvendo o conteúdo de detecção e o modelo operacional em vez de copiar cada alerta SCA legado como um objeto XDR inalterado. Nomes, lógica, evidência, correlação e resultados podem mudar.
Ação do cliente	Avaliar o resultado da detecção, as evidências e a correlação de incidentes do XDR em relação ao cenário de segurança que você precisa operar; não use a correspondência de nome sozinha como aceitação.

Devo usar Incidentes ou Detecções XDR para meu fluxo de trabalho de alerta?

Status	Escolher por resultado
Detalhes	Use Incidentes para resposta humana, notificações de analistas, triagem, escalonamento, gerenciamento de casos e resposta coordenada. Use Detecções para descobertas individuais, exportações de nível de detecção e automação de máquina para máquina. Atividades é a superfície de telemetria.
Ação do cliente	Atualizar os registros de execução para que as notificações humanas e os processos de resposta sejam acionados a partir de Incidentes, quando apropriado; use Detecções para análise detalhada, exportações e automação de localização.

Continuarão os casos de uso baseados em observação?

Status	Não um para um
Detalhes	Não presuma que o nome da observação herdada, o objeto de interface do usuário ou a condição de disparador permanecerão. A meta é cobertura equivalente ou aprimorada por meio de atividades, detecções, incidentes e correlação mais ampla.
Ação do cliente	Identificar e atualizar dependências em runbooks, painéis e automação antes de 24 de outubro de 2026.

E se eu depender principalmente do NetFlow e não puder implantar o EDR?

Status	Ainda no escopo
Detalhes	Os sensores e a inclusão de rede existentes permanecem funcionais, e a implantação de EDR não é necessária para continuar usando as detecções de rede migradas.
Ação do	Use Detecções, Descobertas, Incidentes, Ajuste de Incidentes e o contexto de

cliente	ativos disponível do XDR. Solicite orientação específica de implantação se a visibilidade do endpoint for altamente restrita.

Notificações, exportações, webhooks e automação

O que acontece com os webhooks SCA?

Status	Migrar e testar
Detalhes	Os fluxos de trabalho do XDR Automate são o ponto de controle de longo prazo para notificações, exportações e automação de downstream. O caminho de exportação de destino está alinhado ao OCSF e pode fornecer detalhes de detecção contextual mais completos do que o modelo de alertas e observações SCA legado.
Ação do cliente	Se um webhook enviar informações de detecção para pessoas, SIEM, SOAR ou outro sistema, recrie e teste esse comportamento em fluxos de trabalho XDR.

Qual é a diferença entre os fluxos de trabalho de detecção e incidente?

Status	Usar o disparador correspondente
Detalhes	Use fluxos de trabalho orientados à detecção para movimentação de dados, exportações e consumo de máquinas. Use fluxos de trabalho orientados a incidentes para atividades operacionais mais amplas e notificações humanas, como e-mail, Slack ou Webex. Ambos podem suportar exportações.

O que muda para as integrações de downstream personalizadas, SIEM ou SOAR?

Status	Revisão necessária
Detalhes	Não presuma que um webhook, payload, nome de alerta ou exportação específicos de SCA continuarão inalterados. O caminho de exportação de destino está alinhado ao OCSF e pode fornecer detalhes de detecção mais completos e contextuais.
Ação do cliente	Migre dependências para fluxos de trabalho XDR e para o modelo de dados XDR e teste o recebimento downstream e o comportamento do runbook.

Preciso alterar as notificações e exportações do NVM?

Status	transição de NVM concluída
Detalhes	As detecções de NVM foram transferidas para o XDR em maio de 2026. Clientes que dependem do padrão de webhook NVM herdado precisaram mover notificações e exportações para fluxos de trabalho XDR até a transição de 15 de maio de 2026.
Ação do cliente	Continue a usar e validar o padrão de fluxo de trabalho XDR para NVM.

O que devo testar antes de um cutover de origem?

Status	Verificação de preparação necessária
Ação do cliente	Para cada origem, teste as regras de detecção ou disparo de incidentes, notificação ou exportação de carga útil, recebimento de downstream, filtragem ou roteamento e resposta atualizada do runbook. Teste antes que a fonte saia da experiência SCA.

Fontes de telemetria e transferências fonte a fonte

Quando a telemetria estará disponível nas atividades XDR?

Data	Etapa da telemetria	Ação do cliente
19 de agosto de 2026	Telemetria de dados ONA em Atividades	Comece a revisar a telemetria ONA.
26 de agosto de 2026	Telemetria de dados CTB em Atividades	Comece a revisar a telemetria CTB.
16 de setembro de 2026	Atividades de Logs de Fluxo do AWS VPC, Logs de Fluxo do Azure e Logs de Fluxo do GCP VPC	Comece a revisar a telemetria de fluxo de nuvem.
23 de setembro de 2026	Configuração da fonte AWS no XDR	Use a experiência de configuração XDR onde aplicável.
30 de setembro de 2026	AWS CloudTrail, Logs de Atividade do Azure e Logs de Auditoria do GCP em Atividades	Iniciar revisão de telemetria do log de auditoria.

Preciso reimplantar sensores de rede ou reconfigurar a inclusão de logs na nuvem?

Status	Não, não apenas para migração de UX
Detalhes	Os sensores de rede existentes e a inclusão do registro de nuvem permanecem funcionais durante essa fase e não precisam ser reimplantados ou reconfigurados apenas porque a experiência e as detecções do usuário estão sendo transferidas para o XDR.
Exceção importante	Os endereços IP públicos ou endpoints usados por sensores e integrações podem mudar. Rever regras de firewall, listas de permissão de proxy e outros controles de rede; A Cisco fornecerá os detalhes necessários do endpoint XDR antes de uma alteração de configuração ser necessária.

Quando as detecções de origem são interrompidas?

Status	Agenda específica da origem
Detalhes	Na transição, a telemetria e as detecções para essa fonte não estarão mais

	disponíveis para uso através da experiência do usuário do SCA. • 7 de outubro de 2026: Detecções de AWS CloudTrail, Log de Atividades do Azure e Log de Auditoria do GCP. • 14 de outubro de 2026: Detecções de eventos personalizados. • 21 de outubro de 2026: Detecções do NetFlow.

Configurações, ajuste, listas de controle e contexto do ativo

Minhas configurações de detecção serão migradas?

Status	Migração em fases
Detalhes	Espera-se que os objetos de configuração padrão suportados migrem como parte da transição mais ampla do mecanismo de detecção. As configurações de detecção de NVM foram transferidas para o XDR em maio de 2026; outras configurações mudam conforme sua capacidade se torna disponível.
Ação do cliente	Não recrie manualmente as configurações padrão somente para a migração, a menos que a Cisco publique uma instrução específica para sua implantação.

O que substitui a sensibilidade da sub-rede, os grupos de entidades e o adiamento?

Status	Mudança de conceitos
Detalhes	• Sensibilidade da sub-rede: substituído pela pontuação de priorização de valor do dispositivo em Insights de ativos / Insights de dispositivos; agendado no XDR Device Insights até 30 de setembro de 2026. • Grupos de entidades: configuração programada no XDR Device Insights em 14 de outubro de 2026; os grupos existentes migram para Rótulos, com rótulos de ativos e pontuação de valor usados para priorização. • Adiar: as configurações adiadas não são migradas; O ajuste de incidentes está programado para ser disponibilizado em 14 de outubro de 2026.

Quando é que as Listas de Vigia se movem?

Status	Programado para 14 de outubro de 2026
Detalhes	A configuração da lista de observação está programada para estar disponível no XDR em 14 de outubro de 2026. As listas de controle existentes serão migradas, mas a terminologia e a apresentação de regras podem mudar enquanto a lógica é preservada.
Ação do cliente	Valide as regras, a supressão e os fluxos de trabalho dependentes da lista de controle durante a transição.

Ainda posso definir a prioridade de alerta da maneira que fiz no SCA?

Status	No
Detalhes	A prioridade de alerta é definida com base na pesquisa de ameaças da Cisco e não é um controle de supressão de falsos positivos gerenciado pelo cliente.

Sensores, integrações de nuvem e integridade operacional

As integrações FTD, ISE, AWS, Azure ou GCP permanecerão inalteradas?

Status	Validar caminhos críticos para os negócios
Detalhes	Não presuma que cada integração retém a mesma interface do usuário, fluxo de trabalho ou método de configuração. A configuração do GCP já está em XDR; A AWS e o Azure estão seguindo em frente; os itens de migração relacionados ao sensor no local serão transferidos em outubro.
Ação do cliente	Valide o FTD, a quarentena do ISE, o enriquecimento, os fluxos de trabalho conectados à SAL e outras integrações essenciais aos negócios com base nas orientações específicas do produto.

Posso monitorar a integridade, a vida, o fluxo e o volume do sensor da mesma maneira?

Status	Análise de condições técnicas
Detalhes	A Cisco mantém a operação do sensor e da inclusão durante a transição, mas nem todas as páginas de monitoramento ou fluxos de trabalho do SCA têm o compromisso de migrar um para um.
Ação do cliente	Inventariar as verificações de integridade, protocolo, volume de fluxo e entrega das quais você depende e validar seu caminho operacional XDR.

A distribuição de imagens ONA ou CTB, URLs de destino, chaves de serviço ou endereços IP públicos serão alterados?

Status	Analisar dependências de rede
Detalhes	A Cisco não está exigindo a reimplantação do sensor nesta fase, mas os destinos de telemetria podem mudar conforme as fontes fazem a transição para o XDR.
Ação do cliente	Analise as regras de firewall, as listas de permissão de proxy, os URLs de destino e as dependências de chave de serviço antes da transferência de origem relevante. Não faça alterações preventivas no sensor sem publicar instruções de migração.

Dados históricos, relatórios e administração

O que acontece com os dados SCA históricos quando a experiência do usuário do SCA é desativada?

Status	Exportação antes de 24 de outubro de 2026
Detalhes	O acesso a dados históricos através da interface SCA termina quando a experiência do usuário é removida. A telemetria bruta é inserida no XDR antes e através do caminho de migração de detecção, mas o SCA não é o local de longo prazo para recuperação histórica. • Alertas e observações podem ser exportados como CSV do console SCA. • Logs brutos, incluindo tráfego de rede e logs de nuvem, podem ser exportados como CSV, se necessário. • Defina os requisitos de auditoria, computação forense e retenção de evidências antes da exportação.

Todas as funções de relatório SCA serão movidas para o XDR?

Status	Alguns aposentados ou substituídos
Detalhes	Espera-se que algumas funções de relatório, páginas de menor uso e funções legadas sejam descontinuadas ou substituídas por experiências de Detecções, Investigação, Atividades e Informações de ativos nativas do XDR.
Ação do cliente	Faça o inventário dos relatórios necessários operacionalmente agora e identifique a experiência de XDR, exportação ou fluxo de trabalho de substituição.

Como devo demonstrar a integridade da migração?

Status	Definir artefatos de prova
Ação do cliente	Definir registros e evidências necessários, exportar o histórico do SCA necessário antes de 24 de outubro de 2026 e validar a visibilidade do XDR para cada fonte necessária. A transição não é uma reimportação em massa gerenciada pelo cliente em um sistema separado.

O que acontece com as informações do administrador armazenadas no lado do SCA?

Status	Documentar antes da descomissionamento
Detalhes	Não presuma que a configuração visível ao cliente, as informações administrativas ou o histórico armazenados no SCA permanecerão disponíveis após 24 de outubro de 2026.
Ação do cliente	Exporte ou documente qualquer item necessário para administração, auditoria ou referência histórica e use o XDR como a interface operacional de destino.

APIs e integrações personalizadas

O que substitui a API Obter observações, a API de dispositivos SCA ou outras APIs específicas de SCA?

Status	Dependências de estoque
Detalhes	A Cisco não publicou uma matriz de substituição de API individual final para cada API SCA. Planeje atividades, detecções, incidentes, fluxos de trabalho, informações sobre ativos/informações sobre dispositivos e investigação de XDR.
Ação do cliente	Faça o inventário das dependências diretas agora e não suponha que os nomes de endpoint legados permaneçam disponíveis após 24 de outubro de 2026.

O que acontece com os métodos antigos de criação de incidentes e a automação personalizada?

Status	Tratar como transitório
Detalhes	O FAQ não estabelece uma data de depreciação pública comprometida para cada método de criação de incidente legado ou API. A direção de destino são os eventos e detecções de segurança personalizados XDR, a geração de incidentes no modelo XDR e o ajuste de incidentes para o gerenciamento de resultados.
Ação do cliente	Mapeie cada automação consumindo observações SCA, nomes de alerta, dispositivos, webhooks, exportações ou relatórios para um fluxo de trabalho XDR, detecção, incidente, atividade ou caso de uso do Asset Insights. Testar o comportamento de ponta a ponta antes da transição da origem relevante.

Itens de transição concluídos

Migração de detecção de NVM

Status	✅ Concluída
Resolução	As detecções de NVM e as configurações de detecção relacionadas foram transferidas para o XDR em maio de 2026. Clientes que dependem de notificações e exportações NVM herdadas devem usar fluxos de trabalho XDR e validar o padrão de fluxo de trabalho.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.