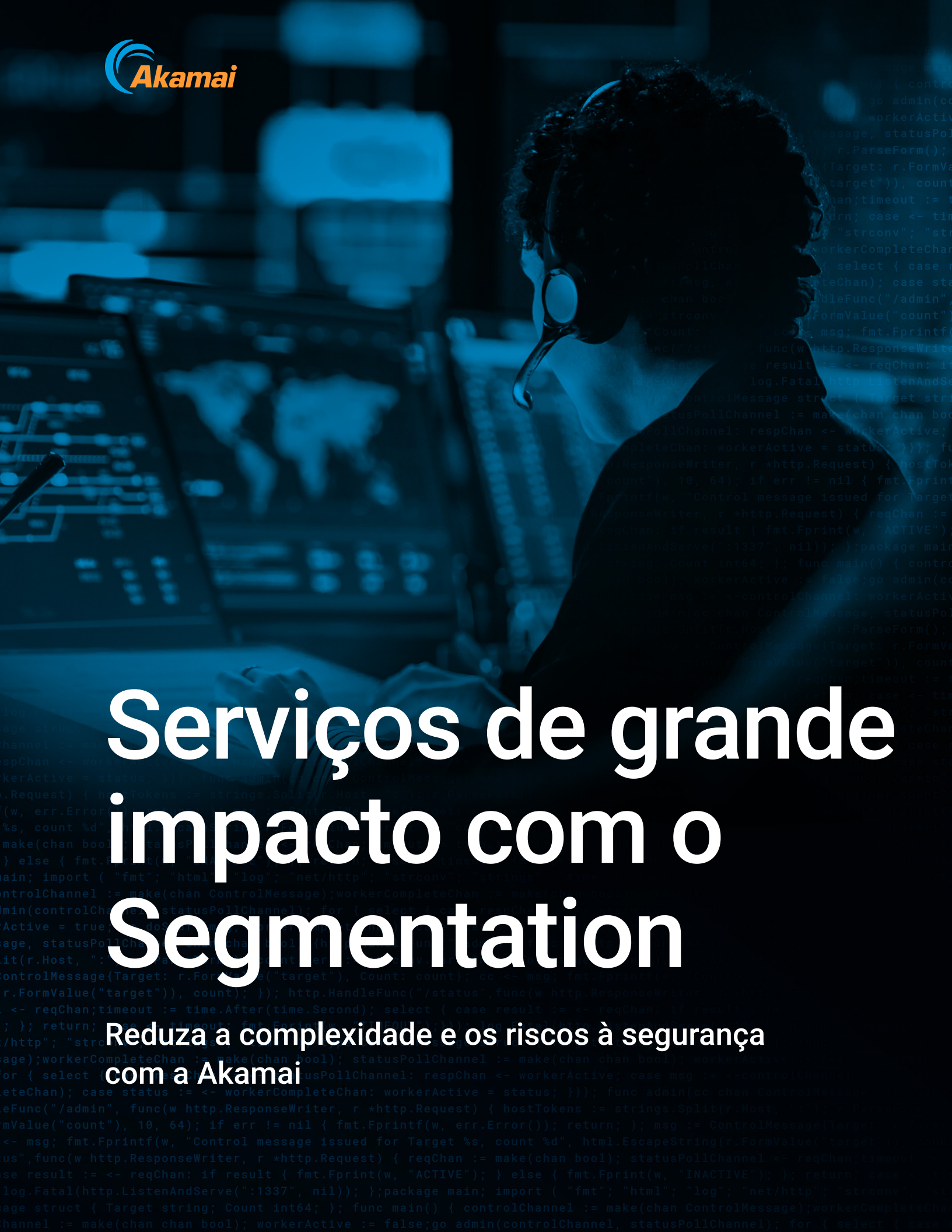


Serviços de grande impacto com o Segmentation

Reduza a complexidade e os riscos à segurança com a Akamai

Introdução

Proteger ativos essenciais em data centers locais e ambientes de nuvem pública é mais importante do que nunca. Cada vez mais, a proteção exige conhecimento especializado para acompanhar o ritmo dos novos modelos de implantação de aplicações em um cenário de ameaças em rápida evolução. O objetivo dos nossos especialistas em serviços é transformar seu investimento em nosso portfólio de segurança em resultados tangíveis e orientados aos negócios.

A equipe de serviços de microssegmentação da Akamai conta com especialistas em segurança com amplo treinamento e experiência real, tanto no setor privado quanto em organizações de inteligência militar. Nosso conjunto flexível de ofertas de serviços fornece acesso a essa experiência especializada como uma extensão de suas equipes internas de TI e segurança para implantar a melhor segurança da categoria, do data center à nuvem.

Jornada do cliente

Uma jornada típica do cliente começa com a implantação e a configuração por meio de nossa prestação de serviços profissionais: configuramos seu ambiente, definimos ativos e rótulos e implantamos a política para os primeiros casos de uso.

Em seguida, fornecemos treinamento administrativo e de engenharia para alguns dos membros da equipe que estão usando a solução.

Além disso, os Serviços operacionais Day-2 podem ser usados para continuar e melhorar a implantação (definindo mais ativos e rótulos, bem como implantando políticas para casos de uso adicionais), lidar com incidentes de segurança e melhorar a postura de segurança, fornecer controles e relatórios necessários para auditorias, e fornecer desenvolvimento personalizado para melhorar a integração com a infraestrutura do cliente.

Durante todo o ciclo de vida da solução, os extensos serviços de suporte ajudarão a resolver qualquer problema que possa ocorrer, e nossa equipe de sucesso do cliente garantirá que você obtenha o máximo valor do nosso produto.

Jornada do cliente com os serviços de microssegmentação da Akamai

Sucesso do cliente
Garantir que os clientes obtenham o valor máximo de nosso produto

Entrega de serviços profissionais	Treinamento	Serviços operacionais Day-2
Implantação do produto; implantação dos primeiros casos de uso	Treinamento detalhado e programas de certificação	Manutenção e expansões contínuas de ativos/rótulos/políticas Revisão da postura de segurança e IR, preparação para auditoria, desenvolvimento personalizado e integração Gerente de conta técnica e engenheiro residente

Serviços de suporte ao cliente
Serviços de suporte técnico: suporte 24 horas por dia, 7 dias por semana, engenheiro designado

Entrega de serviços profissionais

Uma equipe abrangente que consiste de arquitetos de segurança, gerentes de projeto e desenvolvedores trabalhará com sua equipe para implantar a plataforma Akamai Guardicore Segmentation. Dependendo das necessidades, a Akamai oferece um pacote de produtos ou um engenheiro de implantação de prazo fixo. Independentemente do pacote escolhido, nossas ofertas de serviço são personalizadas para garantir a proteção de seus ativos essenciais.

Jumpstart

O Jumpstart foi projetado para clientes que precisam acelerar sua implantação do Akamai Guardicore Segmentation, mas preferem implantar e gerenciar políticas subsequentes com orientação de nossos especialistas. Se você deseja segmentar seu ambiente de rede, delimitar aplicações ou restringir o acesso a servidores, nossos engenheiros projetarão e implantarão seu primeiro objetivo de política, ensinando você e fornecendo orientação à medida que você implantar políticas subsequentes por conta própria.

Nossa equipe também trabalhará com você para planejar a arquitetura de segurança e entender todas as considerações do projeto de aplicações. Isso inclui definir e documentar a estratégia de rotulagem, rotular seus ativos na plataforma e criar e ajustar formalmente as políticas para dar suporte ao(s) seu(s) caso(s) de uso.

Depois que a Akamai concluir a implantação da sua primeira política, nossos engenheiros continuarão a fornecer à sua equipe assistência direta em quaisquer implantações futuras de políticas e permanecerão como parte da sua equipe estendida até que os objetivos da implantação sejam atingidos.

Extended Jumpstart

Para empresas com várias metas de segmentação a serem atingidas, o Extended Jumpstart é ideal. Os especialistas da Akamai trabalharão com suas equipes para implantar várias políticas de segmentação, aumentando a proteção de seus ativos essenciais e dos mais valiosos para sua empresa.

Nossa equipe trabalhará com você para planejar a arquitetura de segurança e entender todas as considerações do projeto de aplicações. Isso inclui definir e documentar a estratégia de rotulagem, rotular seus ativos dentro da plataforma e criar e ajustar formalmente as políticas para dar suporte a várias iniciativas de segurança.

Objetivos típicos da política a serem implantados

Se você deseja segmentar seu ambiente de rede, delimitar aplicações ou restringir o acesso a servidores, nossos engenheiros trabalharão com você em cada etapa da jornada para garantir a proteção de seus ativos.

Como parte desta oferta, você pode selecionar vários objetivos de política ou se concentrar em um objetivo específico de alta prioridade. Nossos engenheiros implantarão as regras e rótulos necessários que formam nossas políticas até que seus ativos estejam protegidos de acordo com seus objetivos pré-identificados.

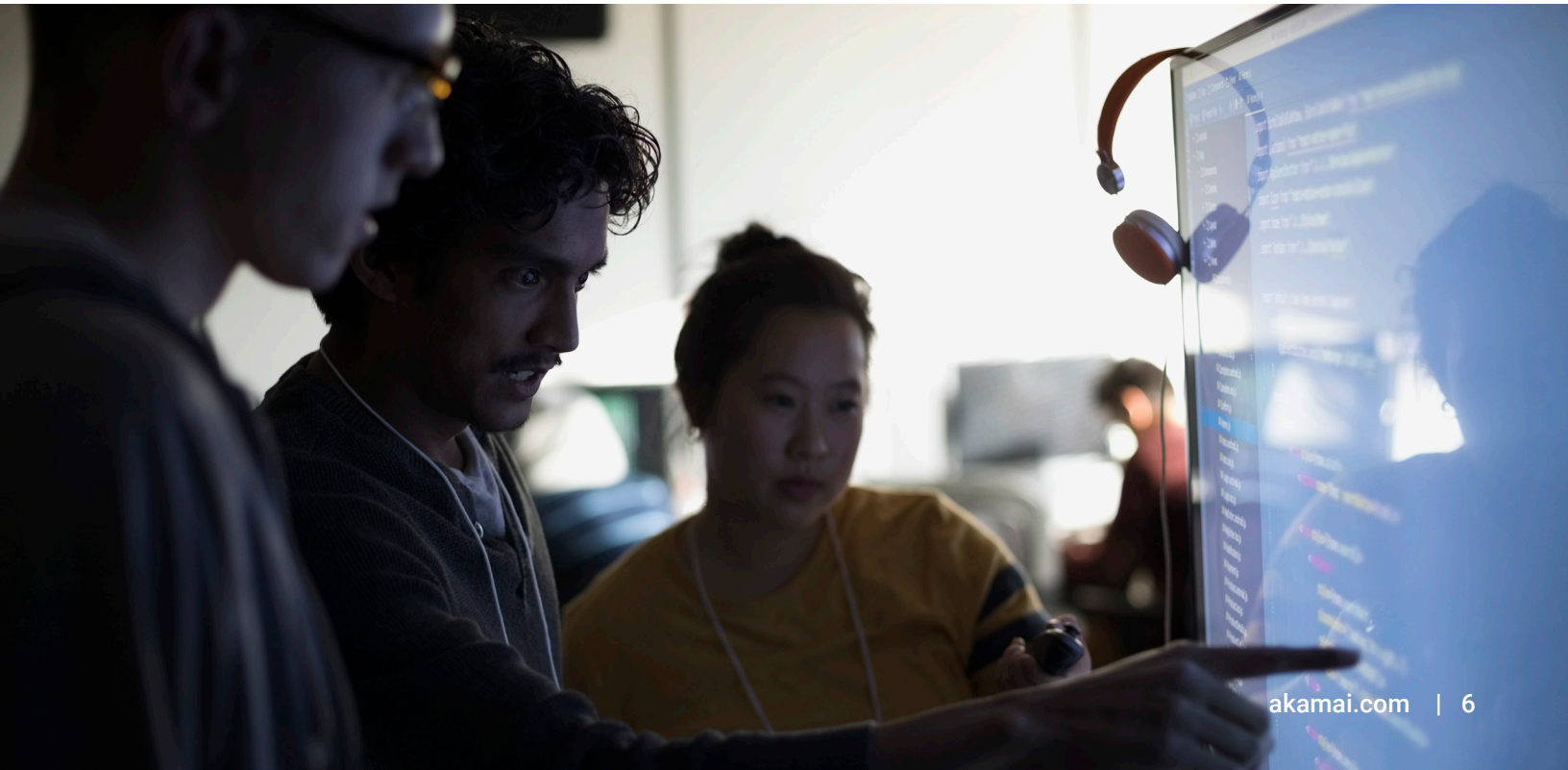
Alguns exemplos incluem:

- **Segmentação do ambiente:** servidores de diferentes ambientes não poderão se comunicar, com exceção das comunicações explicitamente permitidas.
- **Isolamento de aplicações:** aplicações essenciais só devem se comunicar com partes explicitamente permitidas. Serão permitidas comunicações internas da aplicação.
- **Microssegmentação de aplicações:** o tráfego interno e externo de aplicações críticas só será permitido se for explicitamente aprovado (Zero Trust).
- **Segmentação de endpoint "fora da empresa":** a superfície de ataque de um endpoint fora da proteção de uma rede empresarial será limitada. O Akamai Guardicore Segmentation permite conjuntos de regras diferentes para dentro e fora de sua rede corporativa.
- **Acesso privilegiado a servidores:** a política de controle de acesso a servidores pode ser implantada, por exemplo, para restringir as portas de gerenciamento apenas a jump boxes ou para impedir o acesso a servidores específicos com base na identidade do usuário da origem.
- **Aplicação das práticas recomendadas de segurança:** as regras da lista de bloqueio serão implantadas para aplicar as práticas recomendadas de segurança da rede.

Engenheiro de implantação

Quando uma empresa requer um número significativo de objetivos de política, geralmente é preferível trabalhar com um engenheiro designado por um período definido sem limites sobre o número de políticas que nosso engenheiro pode criar para garantir uma implantação bem-sucedida. Permitir que a Akamai forneça o suporte de implantação necessário para que você atinja suas metas é ideal quando sua rede precisa de uma segmentação completa.

	Jumpstart	Extended Jumpstart	Engenheiro de implantação
Instalação	✔	✔	✔
Instalação do esquema de rotulagem	✔ Limitada	✔ ✔ ✔	Recursos abrangentes de implantação por um período definido, sem limitações de casos de uso, garantindo que suas metas de sucesso sejam atendidas
Orientação sobre a postura geral da segurança	✔ Limitada	✔ ✔ ✔	
Orientação sobre criação de políticas	✔ Limitada	✔ ✔ ✔	
Implantar caso(s) de uso de política	**Política única**	**Várias políticas**	
Treinamento do usuário final	✔	✔	✔
Duração típica	**6 meses**	**12 meses**	**6 a 18 meses**
Quando escolher qual opção	O cliente ou parceiro prefere implantar principalmente internamente; a Akamai implanta apenas o primeiro caso de uso	A Akamai implanta vários casos de uso, várias políticas e orientações abrangentes	O cliente ou parceiro deseja a implantação completa (vários casos de uso), prefere explorar e definir exatamente o que e como ao longo do período



Treinamento da Akamai

O treinamento de certificação da Akamai para microssegmentação capacita os administradores (GCSA) e engenheiros operacionais (GCSE) com as habilidades e informações necessárias para obter sucesso em suas tarefas administrativas e de manutenção relacionadas.

Os métodos de formação são versáteis para satisfazer as necessidades dos clientes e dos parceiros: desde a formação básica online até à formação de certificação orientada por instrutores e até formação privada e dedicada (virtual ou presencial).

Guardicore Certified Segmentation Administrator (GCSA)

Nosso programa de cinco dias em meio período capacita os usuários da plataforma Akamai Guardicore Segmentation com a experiência necessária para operar com sucesso todos os aspectos da plataforma. Os graduados em GCSA ganharão a confiança para usar a plataforma por conta própria para implantar e manter as necessidades de segurança de sua organização.

O curso aborda o conjunto de recursos principais do Akamai Guardicore Segmentation: visibilidade, rotulagem, microssegmentação e detecção de violações. O foco está principalmente no comportamento e no uso de recursos, e o curso orientará os alunos desde a configuração inicial do Akamai Guardicore Segmentation até as operações comuns do dia a dia.

Guardicore Certified Segmentation Engineer (GCSE)

Nosso programa de três dias em meio período capacita os proprietários operacionais do sistema com as habilidades e o conhecimento necessários para executar tarefas administrativas e de manutenção relacionadas à plataforma.

Os graduados em GCSE poderão gerenciar a operação geral do ambiente do Akamai Guardicore Segmentation. O curso abrange os seguintes tópicos: configuração de plataforma e componentes, integração com ferramentas de terceiros, verificação de integridade da plataforma, solução de problemas e tarefas comuns de manutenção.

Ambos os cursos são acompanhados por um laboratório prático online disponível para todos os alunos durante o curso. Há um exame de certificação ao final de cada curso.

Suporte empresarial e sucesso do cliente

Nosso programa de suporte empresarial foi projetado para oferecer suporte a todas as possíveis consequências do uso do Akamai Guardicore Microsegmentation em sua organização. Nossa organização de suporte o atenderá 24 horas por dia, 7 dias por semana, 365 dias por ano, tratará de qualquer caso de suporte que surgir e o ajudará com atualizações e correções.

Nosso programa de sucesso do cliente ajuda você a atingir as metas de segurança de curto e longo prazo de sua organização, ao mesmo tempo em que maximiza o valor do investimento feito em nossa plataforma.

Suporte de elite

O suporte de elite da Akamai oferece à sua organização acesso prioritário a especialistas de escalonamento designados, experientes e de alto nível. Um especialista altamente qualificado, familiarizado com seu data center e processos internos, será seu único ponto de contato e ajudará você a acelerar a resposta e a resolução de qualquer problema, além de maximizar o seu investimento em segmentação baseada em software.

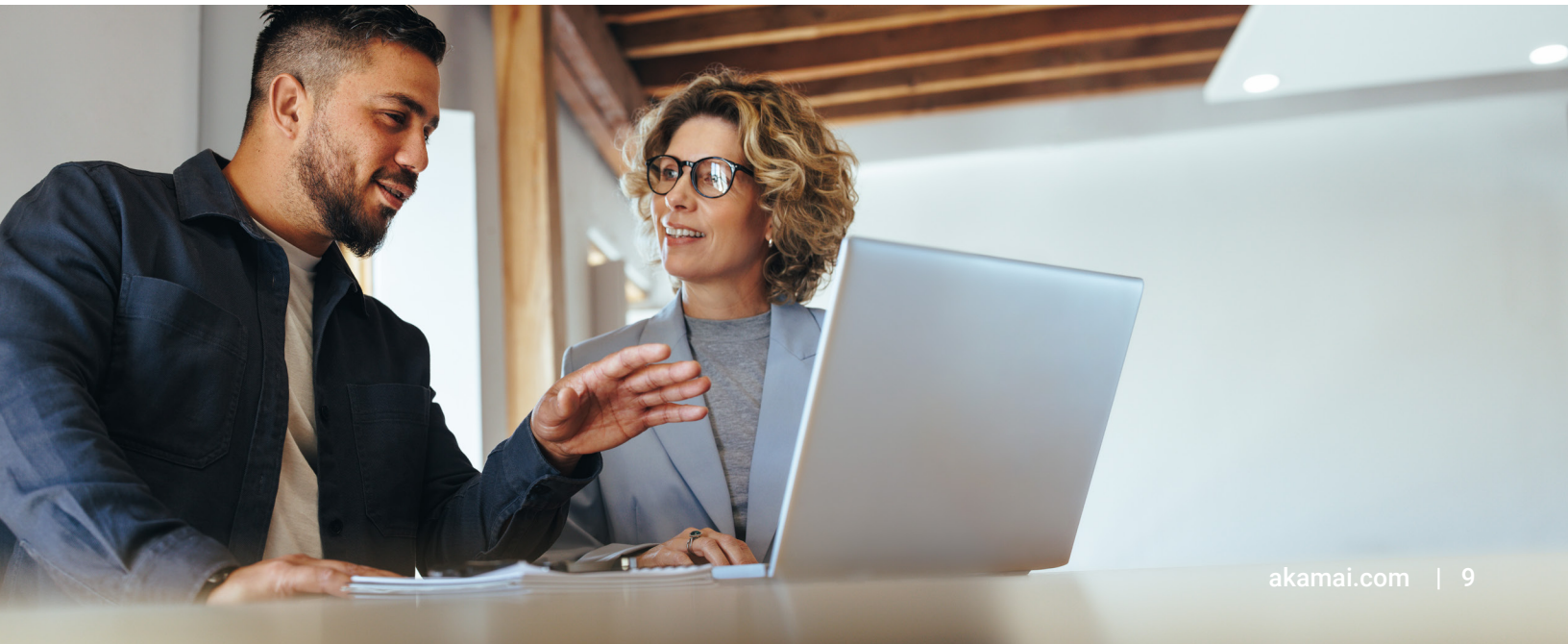
	Premium	Elite
Disponibilidade do suporte	**24 horas por dia, 7 dias por semana, 365 dias por ano**	**24 horas por dia, 7 dias por semana, 365 dias por ano**
Casos ilimitados	✔	✔
Atualizações e correções	✔	✔
Telefone, e-mail, Slack e portal	✔	✔
Análise da causa (sob demanda)	**Gravidade 1**	**Gravidade 1 e gravidade 2**
Tratamento prioritário de casos por um engenheiro designado		✔ Engenheiro designado disponível durante o horário comercial
Monitoramento proativo e contínuo da integridade do sistema		✔
Otimização personalizada		✔ Sessão de otimização trimestral
Revisão periódica de problemas e relatório de suporte		✔ Revisão semanal de problemas; relatório de suporte mensal
Dias de consulta		✔ 2, 4 ou 6 dias de consulta por ano, dependendo do tamanho (SKU)
Quando escolher qual opção	Implantação menor; precisa principalmente de suporte	Implantação maior; requer maior controle sobre problemas contínuos

Serviços operacionais Day-2

Depois de implantar os primeiros casos de uso, os clientes obtêm valor do produto Akamai Guardicore Segmentation. No entanto, há a necessidade de manutenção e atualizações contínuas para que o valor de nosso produto seja maximizado:

- Atualize a implantação (ativos, rótulos, políticas) para refletir as alterações na organização conforme elas ocorrem
- Implante casos de uso adicionais que não foram tratados durante a fase de implantação inicial (novos casos de uso identificados agora que você usa nosso produto, serviços e/ou aplicações adicionais para tratar, etc.)
- Implante o Akamai Guardicore Segmentation em departamentos adicionais de sua organização; por exemplo, redes e aplicações baseadas em nuvem. (novos ou simplesmente os restantes para a fase 2)
- Implante em endpoints adicionais, dispositivos da Internet das coisas, ambientes de infraestrutura de desktop virtual, entre outros.
- Use o Akamai Guardicore Segmentation para identificar e mitigar eventos de segurança (ou seja, interromper o movimento lateral em sua rede); você pode conectar seu ambiente ao Akamai Security Operations Command Center e obter monitoramento 24 horas por dia, 7 dias por semana, 365 dias por ano e alerta e mitigação em tempo real
- Obtenha segurança melhorada e proativa por meio do Akamai Hunt, Akamai Edge DNS (para proteção e DNS seguros contra negação de serviço distribuída) e do Akamai Enterprise Application Access (para acesso e gerenciamento de identidade)
- Use o Akamai Guardicore Segmentation para ajudar você em suas auditorias de certificação

Esses serviços devem ser fornecidos por parceiros certificados pela GcSP



Gerentes de contas técnicas e engenheiros residentes

Os gerentes técnicos de contas e engenheiros residentes da Akamai são consultores técnicos seniores para empresas com necessidades de segmentação amplas e potencialmente complexas. Depois de integrados à sua organização, nossos engenheiros rapidamente se tornam especialistas em seu ambiente, permitindo que você obtenha maior sucesso com o Akamai Guardicore Segmentation.

O engenheiro residente* atribuído à sua conta será incorporado às suas equipes e oferecerá suporte proativo a todas as suas operações para garantir que você obtenha o valor máximo do Akamai Guardicore Segmentation em todos os momentos.

O engenheiro residente pode garantir o sucesso orientando você sobre as decisões políticas, informando você sobre os recursos futuros mais recentes em nosso produto, planejando (e ajudando na execução) uma atualização e realizando análises de negócios executivas.

Seu gerente técnico de contas ou engenheiro residente também pode supervisionar e executar seus Serviços operacionais Day-2.

**O engenheiro residente pode trabalhar remotamente*

Akamai Hunt: um serviço de busca de ameaças gerenciado

O Akamai Hunt, uma extensão do Akamai Guardicore Segmentation, é nosso serviço gerenciado de busca de ameaças que pode ajudar você a se antecipar às ameaças mais evasivas e a proteger melhor sua organização.

A equipe do Akamai Hunt busca continuamente comportamentos de ataques anômalos e ameaças avançadas que contornam consistentemente até mesmo as soluções de segurança mais avançadas. Com o Hunt, você é notificado imediatamente sobre quaisquer incidentes críticos detectados em sua rede, e nossos especialistas trabalham em estreita colaboração com sua equipe para corrigir qualquer ativo comprometido para uma resposta rápida.

Independentemente de o seu objetivo ser detectar e prevenir ransomware, eliminar ameaças persistentes avançadas, se proteger contra vulnerabilidades de dia zero ou melhorar sua higiene geral de segurança de TI, o Akamai Hunt permite obter maior valor de segurança de sua implantação do Akamai Guardicore Segmentation sem qualquer software adicional, implantações de agentes ou atualizações.

O Akamai Hunt inclui:

Análise humana especializada 24 horas por dia, 7 dias por semana: nossos profissionais de cibersegurança são de várias áreas, incluindo pesquisa de segurança, segurança ofensiva, inteligência militar, red team, resposta a incidentes e ciência de dados.

Alertas sobre ameaças reais: para evitar o excesso de alerta, a equipe do Hunt notifica os clientes apenas sobre ameaças reais, evitando completamente falsos positivos.

Ferramentas de caça exclusivas: os especialistas do Akamai Hunt desenvolvem algoritmos avançados de busca de ameaças rotineiramente, como anomalias na atividade de usuários e na rede, análises executáveis, análises de log e mais, formando um poderoso conjunto de ferramentas para detecção e resposta rápidas. O Akamai Guardicore Insight, uma poderosa ferramenta baseada em consulta de sistema operacional para consultar endpoints e servidores em tempo real, está incluído no serviço sem custo adicional.

Inteligência de ameaças rica em contexto: nossa equipe do Hunt coleta indicadores de comprometimento, de IPs e domínios a processos, usuários e serviços, utilizando o Akamai Guardicore Segmentation e a enorme inteligência global da Akamai contra ameaças.

Visibilidade de rede, nuvem e endpoint: essa combinação de dados gerados a partir das implantações do Akamai Guardicore Segmentation e dos sensores globais da Akamai, incluindo mais de 7 trilhões de solicitações de DNS diárias feitas para a nuvem de DNS da Akamai, oferece à nossa equipe a visibilidade mais abrangente do seu ambiente.

Notificação imediata e insights proativos:

- As notificações por e-mail são enviadas imediatamente após a detecção de uma ameaça
- Relatórios periódicos de ameaças de nível executivo incluem análises, estatísticas e métricas para manter seus executivos ou a diretoria informados sobre as campanhas de ataque de alto nível
- O gerenciamento de incidentes é fácil com a integração do console do Akamai Guardicore Segmentation

Para saber mais sobre o Akamai Guardicore Segmentation, acesse akamai.com