Akamai

WHITE PAPER

Acabe com as barreiras de cibersegurança com a segmentação baseada em software

A Akamai Guardicore Segmentation ajuda a melhorar a segurança do acesso e a reduzir os custos de risco cibernético no setor financeiro europeu

Visão geral

O setor financeiro é uma parte crucial da economia da União Europeia, e os sistemas financeiros são considerados infraestruturas críticas por parte de alguns governos e órgãos reguladores europeus. Os produtos e serviços fornecidos pelas organizações de serviços financeiros dependem muito dos sistemas de TI altamente disponíveis e do acesso em tempo hábil às informações fornecidas por meio de vários canais e partes.

No entanto, ataques de ransomware e de criptomineração mostraram com que rapidez os agentes de ameaça podem desativar essa infraestrutura crítica por dias, ou até mesmo semanas, possivelmente se espalhando para terceiros e colegas conectados.

É vital que as instituições financeiras europeias adotem capacidades digitais de ponta na busca da competitividade, aquisição de clientes e retenção. No entanto, os requisitos normativos cada vez maiores para controles de segurança e geração de relatórios estão reduzindo significativamente a taxa de adoção da nuvem. O Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, por exemplo, pode cobrar multas de até 4% do faturamento global de empresas que não protegem seus clientes.[1]

Além disso, regulamentações recentes, como a Society for Worldwide Interbank Financial Telecommunication Customer Security Program (SWIFT CSP) e o documento Cyber Resilience Oversight Expectations (CROE) do Banco Central Europeu (ECB), exigem especificamente uma segmentação de rede mais granular.

As abordagens tradicionais de segmentação e seus procedimentos manuais associados não são uma abordagem viável para acompanhar o ritmo da inovação tecnológica, o aumento dos riscos de segurança e as regulamentações cada vez mais rigorosas.

As organizações precisam não apenas adotar novas ferramentas, mas também mudar fundamentalmente seus processos de segurança e segmentação para adotar simplicidade, transparência e automação.

Este white paper cobrirá:

- Os principais desafios de segurança cibernética que o setor financeiro europeu enfrenta hoje
- Como os bancos e as instituições financeiras podem lidar com esses riscos com uma abordagem econômica e direta da segmentação
- Como a abordagem da Akamai Guardicore Segmentation ajuda as empresas a simplificar seus processos de segurança, reduzindo significativamente os custos e acelerando a conformidade

A segurança virtual atual é complexa e cara para navegar

Embora os bancos europeus e as instituições financeiras estejam comprometidos com a segurança organizacional e a proteção dos dados dos clientes, navegar no caminho para uma postura de segurança mais forte não é uma jornada fácil no mundo atual de riscos em evolução, necessidades de acesso de terceiros e requisitos de conformidade.

O crescimento do risco cibernético aumenta as perdas monetárias

Os riscos associados a crimes cibernéticos são particularmente graves para as instituições financeiras. O setor financeiro já tem o segundo maior gasto que qualquer setor no combate a ataques, com um custo médio de US$ 5,72 milhões por violação de dados.[2]

No entanto, atingir uma postura de segurança forte também é caro. Impor controles de segurança para proteger não apenas várias plataformas, mas também o acesso de terceiros, que é essencial para a prestação de serviços comerciais, é uma tarefa complexa. Ela vem com um aumento significativo nos custos de infraestrutura e mão-de-obra.

A conformidade está custando mais

As organizações de serviços financeiros na Europa têm visto um aumento drástico nos custos, no tempo e nos recursos gerais necessários para preparar e validar a conformidade. Embora os regulamentos ajudem a garantir a estabilidade do setor financeiro, a introdução contínua de novos mandatos de segurança cibernética está afetando a lucratividade e o crescimento, retardando a transformação digital e exigindo investimentos substanciais.

Maior pressão para reforçar as políticas iniciadas com GDPR e seguidas pela Diretiva sobre Segurança de sistemas de rede e Informação (NIS), orientação do ECB CROE e, mais recentemente, a Lei de Segurança Cibernética da UE. No total, com a adição de mandatos de fornecedores, como SWIFT CSP, atingir a conformidade hoje significa abordar um grande número de requisitos técnicos e de relatórios.

Portanto, à medida que atualizam sua tecnologia, os bancos e as instituições financeiras também precisam encontrar maneiras de simplificar o gerenciamento e reduzir os custos operacionais relacionados à segurança cibernética e à conformidade.

Vulnerabilidades de segurança de interações de terceiros e do mercado financeiro

A Diretiva relativa aos Serviços de Pagamento (PSD2), revista pela UE, destinada a melhorar a conveniência e a transparência dos usuários, ampliou os riscos de acesso de terceiros e de compromisso de dados pessoais. Também há uma crescente pressão, de outras empresas do setor e órgãos reguladores de serviços financeiros, para eficiência e transparência em relação aos processos de negócios e tecnologia.

Demandas adicionais de clientes sobre segurança, mobilidade e novos serviços levaram a uma maior dependência de infraestruturas de tecnologia de informação e comunicação de terceiros, fornecedores terceirizados e suas cadeias de fornecimento.

À medida que os ambientes se tornam mais conectados do que nunca, a proteção de todos os tipos de comunicações, incluindo transações automatizadas entre bancos e intrabancárias, tornou-se um recurso intensivo.

Agora, uma única violação ao data center de uma parte poderia ter um efeito dominó, já que os invasores só precisariam explorar um único ativo para mover-se lateralmente entre as partes interconectadas, incluindo instituições financeiras pares e mercados financeiros, colocando em risco a segurança e a continuidade dos negócios de todo o ecossistema europeu de serviços financeiros.

A nuvem híbrida requer uma nova abordagem de segurança

Os mandatos de conformidade, juntamente com as diretrizes da Autoridade Bancária Europeia[3], estão moldando as tendências de adoção da nuvem no setor financeiro. Embora a adoção da nuvem esteja em ascensão na Europa, as normas aumentaram a complexidade da migração de sistemas locais para a nuvem.

Por isso, as empresas europeias têm maior probabilidade de manter as principais funções no local e adotar ambientes de nuvem híbrida em vez de ambientes de nuvem completa. Muitos bancos também avançaram para usar vários provedores de serviços de nuvem, resultando em uma infraestrutura multinuvem.

No entanto, as organizações geralmente buscam mais do que apenas mais segurança. Elas também estão procurando economia de custos e aumentando a eficiência operacional por meio da modificação do processo. A automação e a modernização de processos se tornam fundamentais para o sucesso.

Lidar com os principais desafios de segurança virtual com a visibilidade e a segmentação da rede

O tema que passa por esses desafios é a necessidade de isolar com segurança aplicações e cargas de trabalho críticas, o que é comumente chamado de segmentação. Isso permite que as instituições financeiras alcancem a segurança em escala de acordo com as necessidades comerciais e demonstrem uma abordagem baseada em risco que esteja de acordo com os requisitos normativos.

Os firewalls herdados não são a resposta

Há várias razões pelas quais a segmentação não foi mais amplamente adotada e implantada em bancos e instituições financeiras europeias.

Manutenção e intensidade dos recursos: muitos profissionais de segurança e TI hesitam em buscar iniciativas de segmentação, alegando que isso leva tempo e envolve várias equipes e enormes quantidades de recursos. Essa hesitação é compreensível, pois os métodos tradicionais tendem a ser complicados e demorados. Por exemplo, a configuração de VLANs, ACLs e firewalls em vários locais e ambientes costuma ser um processo trabalhoso, lento e sujeito a erros. Além disso, os métodos tradicionais dependem fortemente de dados de identidade não confiáveis, como IPs, que têm pouco significado e podem mudar com frequência.

Falta de visibilidade: as organizações são ainda mais impedidas pela falta de visibilidade do tráfego leste-oeste, dificultando a identificação de dependências entre segmentos e a criação de regras de segmentação que não quebrem componentes críticos. Mesmo ao usar pontos de escuta (taps) de tráfego ou tecnologias semelhantes, a visualização resultante geralmente não tem o contexto e as traduções sofisticadas necessárias entre IPs e portas. Em ambientes dinâmicos, como PaaS (plataforma como serviço), isso não é impossível.

Dependência da infraestrutura: se as cargas de trabalho se estenderem para a nuvem, o que é cada vez mais comum, o processo se tornará ainda mais complicado. Colocar um firewall físico em cada ponto de saída de dados é econômico. Outros desafios de gerenciamento surgem com as complexas configurações de rede. Essas configurações são necessárias para atender às demandas de ambientes diversos com ativos virtualizados ou legados, além de nuvem e contêineres.

> "Em algumas áreas, o regime regulatório tem lutado para acompanhar o ritmo da inovação tecnológica, assim como as estruturas de gestão e controle de risco das empresas."
>
> – Financial Markets Regulatory Outlook 2023, Centro de Estratégia Regulatória da Deloitte para a EMEA

Introduzir a mudança fundamental do processo

Até mesmo organizações de serviços financeiros de médio porte com algumas centenas de servidores podem gerar milhares de itens de linha de política de segmentação. O gerenciamento manual desses itens não é eficaz, especialmente em ambientes com entrega automatizada de aplicações, usando ferramentas como Jenkins e ciclos de CI/CD nos quais o contexto é crítico.

É por isso que a Akamai Guardicore Segmentation dá um passo além, ajudando as organizações a mudar seus ciclos de criação e atualização de políticas de um processo fundamentalmente manual para um automatizado.

Com a Akamai Guardicore Segmentation, uma vez que o perfil de uma aplicação é automatizado e todas as dependências são mapeadas, a criação de regras e as atualizações podem ser transformadas em um processo repetível em que os acionistas e proprietários de aplicações só precisam aprovar políticas geradas automaticamente. Isso praticamente elimina a necessidade de intervenção manual, o que pode diminuir significativamente os projetos e reduzir o risco de erros de configuração e erro humano.

A criação automatizada de regras mantém a consistência estrutural das regras e a escalabilidade da própria política, levando a um firewall mais otimizado.

Acelere a transformação da TI para criar um verdadeiro ambiente Zero Trust

As instituições financeiras não devem deixar que os processos manuais e recursos limitados as impeçam de atingir a segmentação em escala. O verdadeiro Zero Trust requer não só a tecnologia certa, mas também a modernização dos processos de criação, mudança e manutenção de políticas de segurança.

Os firewalls baseados em host ou software surgiram como uma abordagem simples e econômica para a segurança no nível da aplicação. Essa abordagem acelera drasticamente a implementação, simplifica a manutenção contínua e, em última análise, é mais eficaz na atenuação de ameaças. A Akamai Guardicore Segmentation foi desenvolvida desde o início para ajudar a tornar a segmentação simples, econômica e mais rápida para organizações de todos os portes.

Ela fornece um mapa visual de todas as aplicações no data center e suas dependências. Os operadores podem então criar e aplicar políticas de segurança de nível de processo individual e de rede para isolar e segmentar aplicações e ativos críticos. Essa abordagem de sobreposição definida por software é independente da infraestrutura subjacente e protege as cargas de trabalho que abrangem sistemas legados locais, VMs, contêineres, nuvens e muito mais. As políticas podem ser criadas em torno de aplicações individuais ou logicamente agrupadas, independentemente de onde residem. Essas políticas determinam quais componentes podem e não podem se comunicar entre si, criando a base para uma abordagem Zero Trust para a segurança.

Reduza de forma eficiente os riscos e custos cibernéticos

As instituições financeiras que usam a Akamai Guardicore Segmentation descobrem que podem lidar com algumas de suas preocupações de segurança mais urgentes e, ao mesmo tempo, reduzir custos em um curto período:

Reduza os custos dos riscos cibernéticos, impondo a higiene da segurança da rede e as práticas recomendadas em ambientes cada vez mais complexos e interconectados.

Simplifique o gerenciamento de conformidade por meio de visibilidade contextual granular e políticas de segmentação para mapear e isolar rapidamente ativos relacionados à conformidade e aplicações essenciais aos negócios. Ao usar uma abordagem de painel único, uma instituição financeira pode razoavelmente demonstrar que está tomando medidas para proteger ativos críticos, reduzir o risco de fraude e proteger a privacidade do cliente.

Proteja o acesso de terceiros impondo rotas para tráfego de terceiros com segmentação baseada em identidade, isolando e restringindo os usuários de viajar por uma rede. Isso fortalece a segurança em torno de interações com terceiros e mercados financeiros, impedindo que os invasores "desembarquem e se expandam" de outro sistema comprometido.

Isole os sistemas de transferência de fundos e de pagamento da TI geral para atender os requisitos dos sistemas de transferência e pagamento de fundos eletrônicos, nomeadamente a SWIFT, para uma separação rigorosa dos serviços SWIFT do ambiente geral de TI de uma instituição. A segmentação granular permite que as equipes de TI dos bancos definam limites baseados em contexto (usuário, domínio) em torno da "zona" de um provedor de serviços para restringir ainda mais o acesso não autorizado.

Migre para a nuvem com segurança e rapidez mapeando cargas de trabalho e fazendo o inventário de todas as aplicações críticas e suas dependências antes da migração. As políticas de delimitação podem usar esses mapas como base para uma segurança consistente que segue as cargas de trabalho durante todo o processo de migração. Essa abordagem permite uma migração de nuvem mais rápida e segura, mantendo os mesmos controles de segurança em vigor, independentemente das mudanças de aplicações ou de infraestrutura.

Garanta a continuidade dos negócios com atenuação eficiente de violações por meio da visibilidade granular do tráfego leste-oeste e dos indicadores de violação para alertar sobre movimentos anormais para impedir os agentes de ameaças antes que eles extrujam dados financeiros e de clientes confidenciais.

Reduza os riscos limitando o movimento lateral. Atualmente, a maioria do tráfego do data center se move lateralmente entre aplicações (leste-oeste), em vez de entrar no data center de fora (norte-sul). Estabelecer limites internos ao delimitar aplicações e sistemas críticos para os negócios reduz efetivamente a superfície de ataque, protegendo contra a disseminação lateral de ataques e limitando os danos em caso de violação.

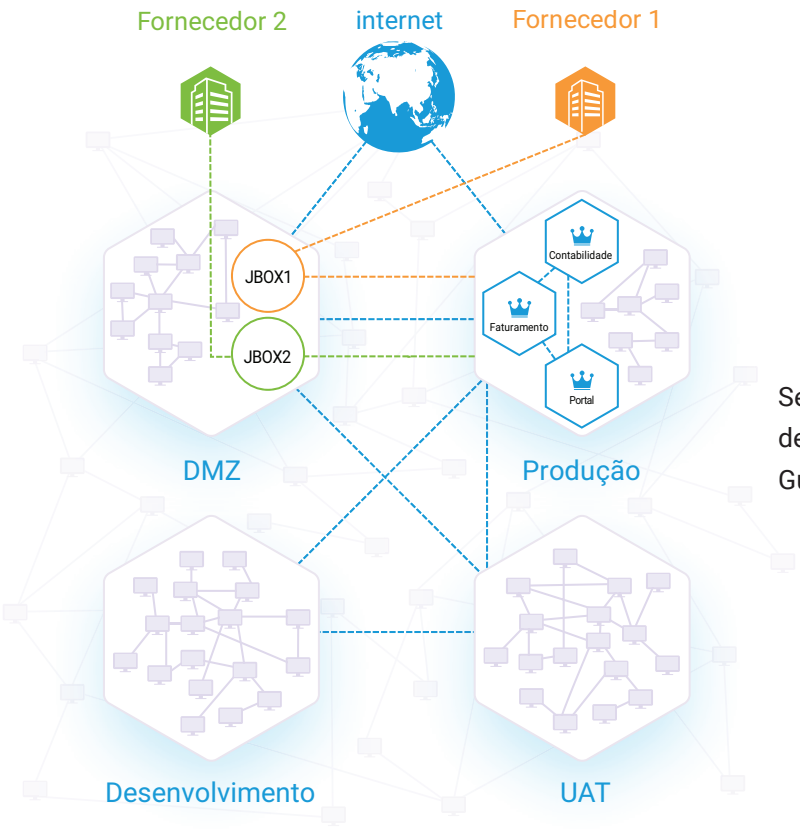
Estudo de caso: redução de custos de conformidade em um grande banco multinacional europeu

Um grande banco europeu estava à procura de uma nova e eficiente abordagem de segmentação de rede, necessária para cumprir os requisitos técnicos de várias agências reguladoras, incluindo o Federal Reserve Bank of NY (FRBNY), a Autoridade Monetária de Singapura (MAS), o BCE e outros.

O uso pelo banco de abordagens de segmentação tradicionais, regras de firewall e VLANs estava se mostrando ineficaz, resultando em altos custos anuais de não conformidade. Também estava afetando as operações de TI com tempo de inatividade significativo da produção e recursos necessários para criar e atualizar políticas.

Uma abordagem mais econômica e fácil de implementar foi necessária para atingir os objetivos de segmentação do banco. O principal requisito para uma nova solução foi o impacto mínimo sobre a infraestrutura e os recursos do banco, ao mesmo tempo em que fornece total conformidade com as regulamentações relevantes.

Após um processo de avaliação completo que incluiu vários fornecedores, os tomadores de decisão das equipes de infraestrutura e segurança de TI do banco chegaram a um consenso: A Akamai Guardicore Segmentation ofereceu o caminho mais rápido e direto para a microssegmentação.



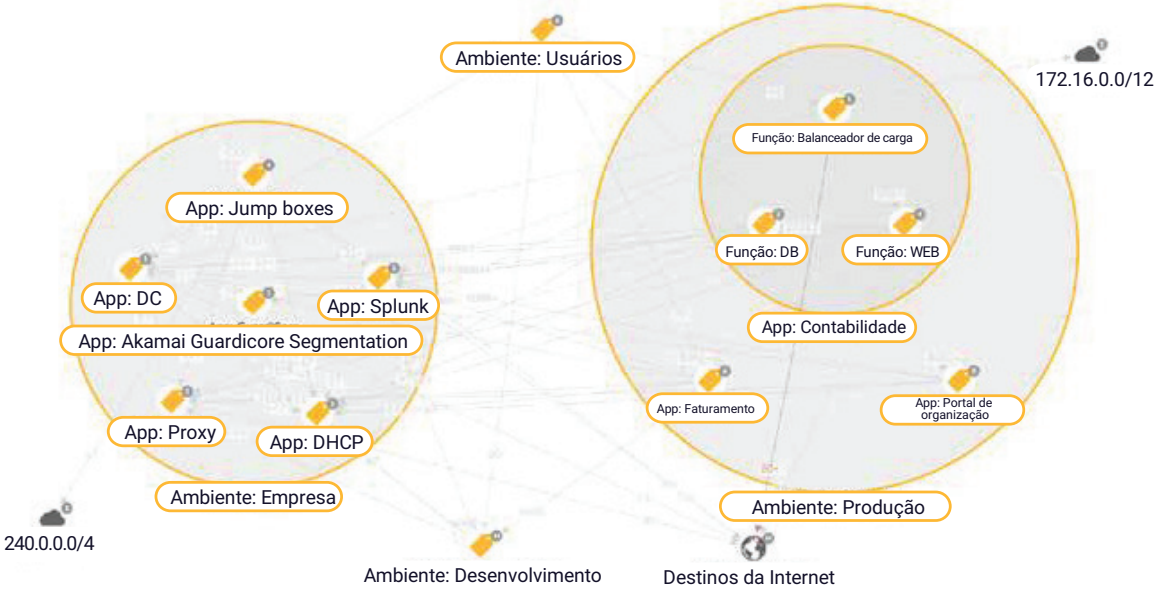
Segmentação de ambiente e controle de acesso de terceiros com Akamai Guardicore Segmentation

Simplificando e acelerando a segmentação

O banco implantou a Akamai Guardicore Segmentation em várias regiões e tipos de infraestrutura de TI, incluindo contêineres. Como não houve necessidade de alterações na aplicação, não houve tempo de inatividade no ambiente de produção. Isso também permitiu que o banco alcançasse rapidamente uma visibilidade centralizada das cargas de trabalho do data center e isolasse os ambientes de produção, teste e desenvolvimento. Com Akamai Guardicore Segmentation, o cliente também conseguiu restringir o acesso a servidores de impressoras, outros dispositivos IoT e usuários não autorizados.

Em menos de três meses, o projeto foi concluído. Foi dez vezes mais rápido do que inicialmente previsto com os métodos tradicionais de segmentação. Ao mapear o ambiente com rapidez e criar políticas baseadas nas informações coletadas, o banco melhorou sua postura de segurança e atendeu aos requisitos de conformidade de mais de 10.000 ativos. A rápida implantação resultou na redução de riscos, bem como em economia significativa de custos e recursos.

A equipe de serviços profissionais da Akamai ajudou o banco a transformar completamente os processos de segmentação. Hoje, as políticas de classificação e segmentação de ativos são totalmente automatizadas, incorporadas aos processos de desenvolvimento e implantação de aplicações. A criação de rótulo, o gerenciamento de alterações, os incidentes de segurança e as solicitações de serviço são totalmente integrados aos fluxos de trabalho do ServiceNow. O cliente ficou extremamente satisfeito com os resultados da plataforma e o valor entregue, juntamente com as equipes de serviços técnicos qualificados e dedicados da Akamai.



Saiba mais sobre a Akamai Guardicore Segmentation em akamai.com/guardicore

1 "What are the GDPR Fines? (Quais são as multas da GDPR?)" GDPR.eu, 13 de fevereiro de 2019.

2 "Cost of a data breach 2022 (Custo de uma violação de dados 2022)," IBM.

3 "A comprehensive guide to cloud adoption in Europe's banking sector (Um guia abrangente para a adoção da nuvem no setor bancário europeu)" Techerati, 31 de outubro de 2019.

A Akamai protege sua experiência do cliente, sua força de trabalho, seus sistemas e seus dados ajudando a incorporar a segurança em tudo o que você criar, em qualquer lugar que você criar e entregar. A visibilidade da nossa plataforma em relação às ameaças globais nos ajuda a adaptar e desenvolver sua postura de segurança para permitir Zero Trust, interromper ransomware, proteger aplicações e APIs ou combater ataques DDoS, dando a você a confiança para inovar, expandir e transformar continuamente o que é possível. Saiba mais sobre as soluções de segurança, computação e entrega da Akamai em akamai.com e akamai.com/blog ou Akamai Technologies no Twitter e LinkedIn. Publicado em 06/23.