

Autor:
Bryan Montany, Analista Principal,
Omdia

White Paper sobre Crescimento do Mercado de Controle de Acesso



Brought to you by Informa Tech

Solicitado por:



Conteúdo

Introdução	2
Fatores que norteiam o mercado de controle de acesso	4
Da integração à unificação	6
Arquiteturas de sistemas híbridos	7
Mitigação dos riscos de cybersecurity	9
O ambiente competitivo	11
De que forma a Genetec emergiu como líder de mercado	14
Apêndice	17

Introdução

O mercado global de sistemas eletrônicos de controle de acesso já foi dominado pelas vendas de hardware. O software já foi visto como uma ferramenta secundária para monitorar o desempenho dos equipamentos e validar a identidade dos visitantes. Na última década, no entanto, os sistemas de controle de acesso evoluíram para se tornarem mais centrados em software. A inteligência artificial, aprendizado de máquina e analíticos preditivos já têm sido aproveitados pelos fornecedores de software de controle de acesso para apresentar dados do sistema de forma mais eficiente, fornecer recursos automatizados de help desk e oferecer suporte a consultas de pesquisa em linguagem natural.

Novos casos de uso estão surgindo rapidamente para algoritmos avançados para identificar com precisão violações de segurança, informar partes interessadas sobre falhas de equipamentos, prever flutuações nas taxas de ocupação de edifícios e alterar automaticamente as credenciais. Essa evolução acelerou a tendência preexistente de expansão da base de usuários do software de controle de acesso, indo além dos profissionais de segurança para incluir gestores de instalações, especialistas em TI, profissionais de RH e administradores de empresas que podem utilizar dados de ocupação predial e ferramentas para aprimorar suas operações e negócios.



À medida que a importância dessas aplicações cresceu, o software se tornou o tipo de produto de crescimento mais rápido para sistemas de controle de acesso em todas as regiões do mundo em 2023. A Omdia espera que a demanda do mercado global por software atinja uma taxa de crescimento anual composta (CAGR) de 9,1% entre 2023 e 2028. A receita total de vendas de software será de US\$ 847 milhões até 2028. O software representará mais de 10% do mercado global de equipamentos de controle de acesso até o ano de 2030.

Essa alta taxa de crescimento, combinada com menores barreiras à entrada no mercado, encorajou novos entrantes e disruptores a introduzir novas plataformas e competir com os fornecedores convencionais. Os integradores de sistemas e usuários finais que se mantêm atualizados sobre a evolução das capacidades do software estarão melhor posicionados para investir em plataformas superiores que não apenas otimizam seus sistemas de controle de acesso, mas também são inovadoras o suficiente para oferecer suporte a uma visão mais ampla de segurança e gestão de instalações, indo além do monitoramento de acessos eletrônicos.

Este white paper explora tendências recentes e dinâmicas de mercado que impactarão a demanda por software de controle de acesso nos próximos cinco anos. O estudo também se concentra na Genetec Inc., um dos fornecedores de software de controle de acesso que mais cresce no mundo e extrai lições fundamentais de suas altas taxas de crescimento nesse setor. O estudo também aborda várias tendências importantes:

-
- O estado do mercado de controle de acesso após as inovações tecnológicas relacionadas à automação inteligente e à IA generativa com foco em enxergar a IA como um recurso complementar para facilitar decisões informadas pelas partes interessadas.
 - A transição de uma estrutura de conectividade de integrações de sistemas entre sistemas de controle de acesso e outros domínios de segurança para uma abordagem de unificação de sistemas por meio de soluções holísticas de gerenciamento de instalações.
 - A tendência em rápido crescimento de uma abordagem híbrida para arquiteturas de sistemas de controle de acesso, aproveitando as vantagens tanto das capacidades de processamento de dados in loco quanto na nuvem.
 - Ênfase contínua nas vulnerabilidades de cybersecurity como a preocupação mais premente para fornecedores de software, integradores de sistemas e usuários finais abordarem coletivamente.
 - A evolução do ambiente competitivo para vendas de software de controle de acesso, incluindo o surgimento da demanda por soluções de Controle de Acesso como Serviço (ACaaS) hospedadas na nuvem.

Os proprietários de edifícios começaram a reconhecer o papel fundamental que o software de controle de acesso pode desempenhar na agregação e fornecimento de dados de ocupação que formam a base das arquiteturas de edifícios inteligentes. A Omdia está confiante que o mercado de controle de acesso continuará a transição para uma estrutura ainda mais centrada em software na próxima década.

Fatores que norteiam o mercado de controle de acesso

Muitos proprietários de edifícios antes se contentavam em investir em upgrades de software apenas quando seus sistemas de controle de acesso começavam a falhar, e um ciclo de substituição de software de 15 a 20 anos era comum antes da pandemia de COVID-19. No entanto, os recentes desenvolvimentos da indústria levaram os usuários finais a adotar novos avanços de software e investir de forma mais proativa nas últimas inovações. Fornecedores e integradores de sistemas identificaram o software como o tipo de produto de controle de acesso que mais efetivamente diferencia sua marca e seus serviços da concorrência.

Várias tendências notáveis continuarão impulsionando as receitas de software em 2024 e nos anos seguintes:

- **As inovações tecnológicas relacionadas aos modelos de IA generativa facilitarão a acessibilidade ao software de controle de acesso entre uma base de usuários mais ampla de partes interessadas.** Os desenvolvimentos em IA incentivarão a crescente demanda por pesquisas de consulta em linguagem natural, helpdesks habilitados para IA generativa e análise de sistemas por meio de algoritmos avançados. No entanto, os usuários finais devem ser devidamente instruídos sobre os riscos associados à IA e implementar proteções contra depender exclusivamente da tecnologia para orientar suas decisões críticas de segurança. Apesar do hype em relação a possíveis casos de uso, a IA é melhor vista não como uma superinteligência revolucionária, mas como um meio adicional de criar conjuntos de dados, gráficos e análises que podem ser adaptados e apresentados às partes interessadas humanas.
- **O escopo crescente dos stakeholders do software de controle de acesso, indo além dos profissionais dedicados à segurança, levou a um foco maior na experiência do usuário (UX).** Essa tendência incentivará os fornecedores a investirem em interfaces e painéis de controle utilizáveis, intuitivos e visualmente atraentes, que atendam a uma ampla variedade de usuários com diferentes perfis. Antes do surgimento dessa tendência, o software de controle de acesso era projetado principalmente para gerentes de segurança experientes e frequentemente priorizava a exibição de dados de uma maneira que valorizava a proficiência técnica em detrimento da facilidade e simplicidade. O crescente uso de software de controle de acesso entre profissionais dos setores de TI, RH, instalações e gestão financeira levou a uma maior demanda por plataformas unificadas com displays acessíveis e facilmente customizáveis. Muitos dos primeiros casos de uso da IA se concentraram na acessibilidade do usuário final por meio de melhorias simplificadas nas interfaces do usuário.

-
- **Os fornecedores começaram a adaptar suas ofertas de software para alcançar mercados verticais específicos.** Por exemplo, projetos no setor de educação, que representaram mais de US\$ 585 milhões em vendas de controle de acesso em 2023, crescerão a uma taxa composta de 8,2% ao ano (CAGR) nos próximos cinco anos (2023-2028), ficando atrás apenas dos data centers como o mercado de crescimento mais rápido do mundo. O crescimento na educação será impulsionado pelas vendas no mercado dos EUA que cresceram 13% e representaram mais de 47% da receita global na vertical em 2023. A frequência de tiroteios em escolas nos EUA continuou a exercer pressão sobre os usuários finais para investir em sistemas de segurança escolar de alta qualidade. A expansão dos sistemas de controle de acesso para validar a entrada pelas portas internas das salas de aula tem impulsionado oportunidades de vendas para soluções de software mais complexas, capazes de rastrear com eficácia os dados em tempo real de visitantes, docentes e alunos em diferentes salas e áreas das instalações escolares.

Da integração à unificação

O mercado de software de controle de acesso foi impactado por uma demanda crescente por sistemas de segurança interconectados desde a introdução de equipamentos de segurança habilitados para IP há quase 20 anos. Desde então, equipamentos e softwares em sistemas eletrônicos de controle de acesso têm sido frequentemente integrados a outros produtos de segurança nos domínios de videomonitoramento, detecção de intrusão, notificação em massa e segurança de vida. Essas integrações de sistemas de segurança continuaram a crescer em popularidade na última década, mas uma tendência emergente viu os dados de rastreamento de ocupação do software de controle de acesso como um componente essencial para casos de uso além da segurança.

A tendência de integrar equipamentos de controle de acesso com outros domínios se expandiu nos últimos anos, pois os casos de uso de dados de ocupação suportaram a conectividade com produtos como equipamentos HVAC, equipamentos de iluminação, elevadores e bancos de dados de RH. As informações relacionadas às credenciais dos ocupantes dos edifícios podem fornecer aos domínios conectados dados atualizados em tempo real sobre a ocupação, permitindo que as partes interessadas tomem decisões informadas sobre a melhor forma de utilizar os espaços, salas e zonas designadas nos edifícios.

Fornecedores de software de controle de acesso, como a Genetec, têm impulsionado a inovação ao enxergar suas aplicações não apenas como componentes de um sistema de segurança, mas como motores holísticos de soluções de gerenciamento de instalações. Para alcançar essa visão, o software de controle de acesso deve ser projetado para ser flexível, aberto e totalmente interoperável com produtos de terceiros. Essa tendência afastou a indústria da dependência de soluções proprietárias e favoreceu parcerias com uma gama cada vez maior de fornecedores. Os fornecedores de software mais prolíficos e de crescimento mais rápido unificaram suas plataformas com sistemas de acesso móvel, leitores biométricos, câmeras de videomonitoramento, alarmes de intrusão, sistemas de controle de clima e iluminação conectada, software de controle de ponto e diversas outras aplicações.

O software de controle de acesso também pode constituir uma base crucial para arquiteturas de sistemas de edifícios inteligentes. A Omdia define um edifício inteligente como aquele com domínios totalmente integrados e processos analíticos automatizados para controlar as operações do edifício por meio de plataformas centralizadas ou distribuídas. O software de controle de acesso é ideal para fornecer às plataformas de sistemas de gestão de edifícios (BMS) atualizações em tempo real sobre a ocupação do edifício. De acordo com a Omdia, o controle de acesso permaneceu como o domínio de segurança mais comum a ser integrado a outros sistemas por meio de uma plataforma BMS, com uma taxa de adesão global de 33%. Espera-se que a demanda por recursos e funcionalidades de edifícios inteligentes cresça significativamente entre os usuários finais na próxima década. O aumento das integrações entre o software de controle de acesso e outras plataformas de gestão de edifícios incentivará os fornecedores a se tornarem mais flexíveis para atender aos requisitos de terceiros na criação de sistemas unificados.

Arquiteturas de sistemas híbridos

Credenciais mais complexas, biometria mais precisa e a transição para sistemas de acesso móvel estão entre uma infinidade de tendências que alimentaram a necessidade de sistemas de controle de acesso para capturar e interpretar mais dados. Historicamente, essa necessidade de analisar mais dados criou um problema de design de sistema para os fornecedores de equipamentos, com as opções sendo o uso da nuvem ou de software hospedado localmente em dispositivos de borda como ponto central para os analíticos do sistema. Tanto a nuvem quanto a borda oferecem aos usuários finais vantagens significativas e distintas. Uma arquitetura de sistema na nuvem pode reduzir a necessidade de grandes investimentos em infraestrutura de TI local, viabilizar o processamento de analíticos de big data e oferecer um monitoramento remoto aprimorado para instalações multi-site. No entanto, o software carregado em dispositivos de borda é menos afetado por problemas de latência de rede e é mais capaz de reagir em tempo real às mudanças nas condições em instalações individuais.

No entanto, à medida que a necessidade de os sistemas de controle de acesso processarem mais analíticos aumentou, uma terceira opção se tornou a escolha preferida entre os integradores de sistemas e os usuários finais. Em vez de fazer a transição para modelos de arquitetura apenas na nuvem ou borda, a preferência emergente tem sido a adoção de ambas as tecnologias em um único sistema de controle de acesso coeso. Nesses sistemas híbridos, os dispositivos de borda contêm software capaz de processar dados em tempo real e lidar com problemas imediatos em pontos de entrada individuais, mas também estão conectados diretamente à nuvem. O software no âmbito da nuvem é responsável pelo processamento de 'big data' envolvendo análises mais avançadas. Essa abordagem híbrida oferece aos usuários finais os melhores elementos dos modelos arquiteturais de borda e nuvem em um único pacote unificado, dando a flexibilidade de evoluir seu sistema de controle de acesso para atender às suas necessidades específicas no seu próprio ritmo.

O crescimento dinâmico dos sistemas híbridos de controle de acesso está intimamente ligado à tendência de soluções de controle de acesso como serviço (ACaaS) na nuvem. Nessas soluções, um provedor de serviço ACaaS assume a responsabilidade de manter um ecossistema na nuvem de aplicações web, ferramentas, analíticos de "big data" e proteções de segurança cibernética para dar suporte às operações dos sistemas de controle de acesso dos usuários finais. As soluções ACaaS são totalmente escaláveis e podem se adaptar às necessidades em constante mudança das instalações sem investimentos financeiros substanciais em nova infraestrutura de TI ou hardware de controle de acesso. Esses recursos permitem que os usuários finais de instalações de pequeno e médio porte comprem sistemas de controle de acesso que, de outra forma, estariam fora de seus orçamentos.

A Omdia determinou que o mercado global de software ACaaS cresceu 21,5% em 2023, uma taxa quase três vezes maior que o crescimento do software tradicional in loco. A maior parte desse mercado estava concentrada na América do Norte, mas a demanda por soluções ACaaS está

crescendo significativamente na Europa, Oriente Médio, Oceania e Sudeste Asiático. O mercado global de soluções ACaaS deve alcançar o equivalente a 18% das vendas de equipamentos convencionais de controle de acesso até 2028. A adoção em larga escala de soluções ACaaS será liderada por fornecedores como a Genetec que lançou em 2024 sua nova plataforma unificada de software como serviço para segurança física, o Security Center SaaS.

Mitigação dos riscos de cybersecurity

A tendência de unificação do software de controle de acesso com outros domínios das instalações levou a maioria dos sistemas de controle de acesso a se integrar aos sistemas de TI e redes virtuais dos usuários finais. Essa dinâmica trouxe benefícios imensos para os gestores de instalações, mas também abriu uma brecha para que agentes mal-intencionados invadam os equipamentos de controle de acesso e obtenham um acesso mais amplo à infraestrutura de TI da organização. Os sistemas de controle de acesso têm sido cada vez mais visados por ataques cibernéticos remotos e in loco. De acordo com um relatório sobre segurança cibernética publicado pela IBM em 2024, uma violação de dados típica realizada naquele ano custou aos usuários finais quase US\$ 4,9 milhões.

Hackers in loco ocasionalmente atacam credenciais e leitores, mas muitos dos ataques cibernéticos contra controle de acesso são iniciados remotamente e direcionados ao software de controle de acesso. À medida que os ataques cibernéticos continuam a aumentar e o mundo se compromete com a transformação digital, será ainda mais crítico para os provedores de software desenvolver seu produto com proteções de ponta contra ameaças cibernéticas e criptografar adequadamente as transmissões para que não possam ser usadas como pontos de entrada para hackers. Todo fornecedor de software corre o risco de perder negócios significativos se vulnerabilidades em sua plataforma forem expostas através de ameaças cibernéticas. A conscientização sobre vulnerabilidades de segurança cibernética continua a crescer entre os usuários finais. Essa compreensão mudou os diálogos entre usuários finais e provedores de sistemas de segurança para exigir mais garantias de proteção contra ransomware e mais recursos, como testes de validação de segurança cibernética.

Um método que os fornecedores de software utilizam com frequência para garantir a conformidade com os padrões de segurança cibernética aplicáveis, como a ISO/IEC 27001, é a contratação de auditores externos de segurança cibernética. Esses auditores independentes avaliam e verificam se o software atende aos padrões aplicáveis para segurança da informação. Os auditores externos podem garantir que os fornecedores sigam os mais altos padrões de segurança para níveis de criptografia e garantir a conformidade com os padrões de privacidade de dados, como o Regulamento Geral de Proteção de Dados (GDPR) da UE, a Diretiva NIS2 e a recém-promulgada Lei de IA da UE que impõe requisitos de transparência e segurança cibernética em modelos de IA designados.

Outro mecanismo técnico de proteção que as empresas adotam para se defender contra ataques cibernéticos é uma abordagem de proteção em várias camadas, incorporada à forma como as soluções escrevem, analisam e validam o código. Uma abordagem em várias camadas dificulta a ação de agentes mal-intencionados, garantindo que uma segunda camada independente continue funcional mesmo que a primeira seja violada. Mesmo que um hacker seja apenas temporariamente incomodado por esse revés, testes e verificações em segundo plano executados em tempo real

podem capturar o ataque cibernético enquanto o hacker está tentando contornar uma camada secundária.

Muitos fornecedores de controle de acesso se comprometeram com as “primeiras abordagens de cybersecurity” para o desenvolvimento de software, mas é efetivamente impossível para os fornecedores garantir uma plataforma invulnerável. O fator de diferenciação mais importante entre os fornecedores não é nenhuma inovação técnica para evitar ataques cibernéticos, mas sim um compromisso com a transparência na divulgação de informações quando as vulnerabilidades são identificadas. A melhor forma de mitigar os riscos de cybersecurity é através de parcerias com auditores terceirizados, fabricantes de hardware, integradores de sistemas e usuários finais.

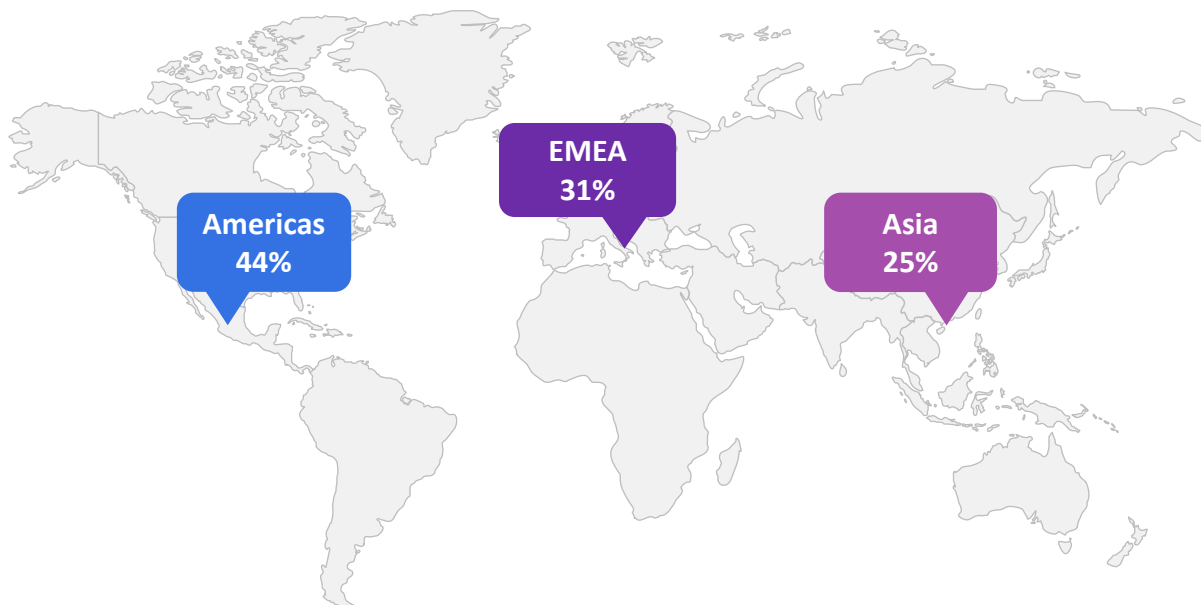
O ambiente competitivo

O nível superior do cenário competitivo para software de controle de acesso é composto por pesos pesados estabelecidos da indústria. Empresas como Honeywell, Bosch e Johnson Controls frequentemente comercializam seu software para usuários finais de nível corporativo com arquiteturas complexas de sistemas de controle de acesso. Essas empresas têm uma presença consolidada no mercado, mas tendem a registrar taxas de crescimento anual de apenas um dígito. Taxas de crescimento mais altas geralmente só são alcançadas de forma artificial por meio da aquisição de empresas inovadoras. Por exemplo, a Honeywell alcançou um crescimento substancial em 2024 por meio da aquisição da LenelS2, fornecedora líder mundial de software de controle de acesso, da Carrier.

Logo abaixo desses gigantes há um segundo nível de fornecedores especializados de software que customizam suas plataformas para atender a setores específicos de usuários finais. Por exemplo, a Identiv projetou sua plataforma de software Hirsch Velocity para integrar sistemas de controle de acesso físico com sistemas de gerenciamento de identidade e acesso (IAM). A segmentação de crescimento mais rápido neste segundo nível é com provedores ACaaS nuvem, como Brivo, Verkada e Nedap. O mercado de ACaaS está projetado para crescer cerca de duas vezes mais rápido que o mercado de soluções convencionais de controle de acesso entre 2023 e 2028.

A Genetec ocupa uma posição única no mercado em relação à concorrência, pois possui atributos de ambas as categorias de concorrência. Em termos de participação de mercado, a Genetec é um dos dez principais fornecedores globais e compete efetivamente com os líderes de mercado. No entanto, sua taxa de crescimento de receita é muito mais rápida do que esses fornecedores já bem estabelecidos. O crescimento recente se alinha mais estreitamente com os fornecedores de software especializados ativos no mercado de controle de acesso, apesar da empresa comandar uma parcela muito maior do mercado.

Divisão de receita no mercado de software de controle de acesso por região (2023)

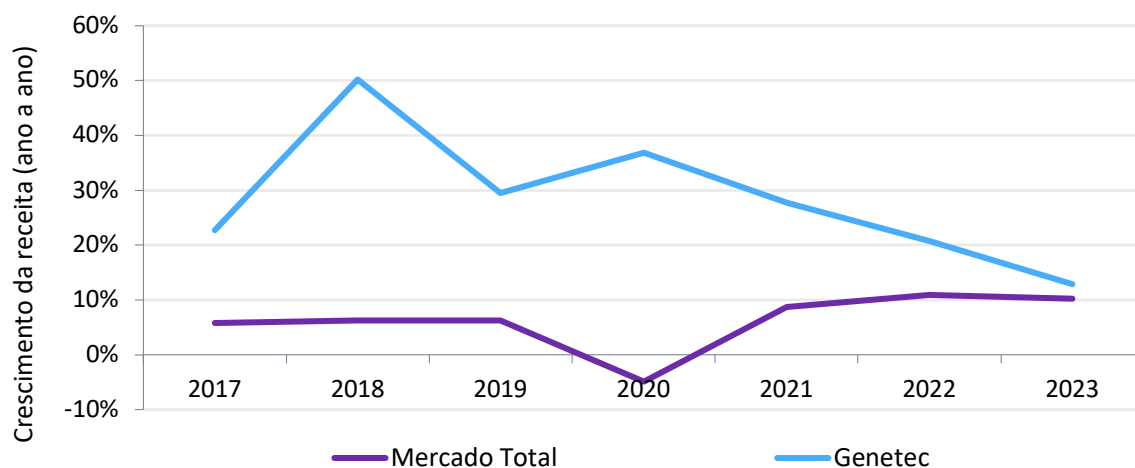


- As Américas representaram mais de 44% das vendas globais de software. No entanto, esse mercado é dominado pelos dez principais fornecedores que coletivamente representaram quase 80% das vendas totais em 2023. A maioria dos usuários finais norte-americanos compra software de marcas estabelecidas, como LenelS2, Genetec e Johnson Controls. As soluções agrupadas de controle de acesso que incluem hardware, software e serviços fornecidos por um único fabricante são comumente preferidas. Os EUA continuam sendo o maior mercado de software de controle de acesso do mundo por uma ampla margem. Inclui a maior diversidade de usuários finais do mundo e é um mercado que tem sido uma das principais prioridades da Genetec na última década.
- As condições na EMEA têm sido mais favoráveis para novos fornecedores e disruptores, já que o mercado na região é fragmentado em diferentes perfis de usuários finais que preferem investir em plataformas adaptadas localmente. A predominância de projetos de retrofit, que representaram cerca de 78% da receita de projetos na Europa Ocidental em 2023, exigiu que a maioria dos fornecedores de software projetasse suas plataformas para incluir arquiteturas de sistema abertas. Os dez principais fornecedores de software na região EMEA alcançaram coletivamente menos de 65% da participação de mercado em 2023. Exemplos de provedores líderes incluem Allegion, Nedap e Paxton Access.
- A Ásia e a Oceania representaram menos de 25% das vendas globais de software em 2023. No entanto, mercados sub-regionais específicos, como Índia e Sudeste Asiático, estarão entre os mercados de crescimento mais rápido do mundo nos próximos cinco anos. A predominância dos sistemas de videomonitoramento e do software VMS historicamente limitou as taxas de adoção de software de controle de acesso na China, embora essa dinâmica tenha começado a mudar à medida que uma porcentagem maior de fabricantes domésticos de equipamentos de controle de acesso (como Hikvision, Uniview e SenseTime) passou a lançar recentemente suas próprias

soluções de software O mercado da Ásia e Oceania ficou alguns anos atrás dos mercados das Américas e EMEA com tendências como processamento de dados na nuvem e analíticos preditivos.

De que forma a Genetec emergiu como líder de mercado

Histórico do crescimento no Mercado de Software para Controle de Acesso - Mundo



Fonte: Omdia

© 2024 Omdia

A Genetec é uma fornecedora de software e soluções de segurança física com sede em Montreal, Canadá. Nos últimos cinco anos, consolidou-se como um dos fornecedores de software de controle de acesso que mais crescem no mundo. Nenhum outro fornecedor de software classificado entre os dez principais alcançou uma trajetória de crescimento comparável na última década. As vendas globais de software da Genetec mais do que quadruplicaram entre 2016 e 2023. Em 2016, a Genetec representava apenas 2,5% das receitas globais de software de controle de acesso; em 2023, a empresa alcançou 8,7% de participação no mercado global.

Durante esse período, a Genetec passou de décimo maior fornecedor de software de controle de acesso do mundo para o segundo maior. Um aspecto notável dessa evolução é que a Genetec alcançou essa posição exclusivamente por meio de crescimento orgânico. Em vez de depender de fusões ou aquisições, a Genetec evoluiu os recursos e as capacidades do Synergis™ para conquistar fatias de mercado anteriormente dominadas por concorrentes.

A Genetec oferece aos integradores de sistemas, usuários finais e até fornecedores concorrentes um modelo de como a indústria de software de controle de acesso se desenvolveu nos últimos cinco

anos. A plataforma Security Center da Genetec incorpora características como unificação de sistemas de segurança, interoperabilidade com hardware de terceiros, experiências de usuário (UX) coesas e proteções de segurança cibernética de várias camadas.

Seu software promoveu uma visão de unificação do sistema de segurança que encaixa várias soluções de segurança em vários domínios em um única aplicação unificada. Uma plataforma integrada pode permitir a conectividade entre diferentes plataformas de segurança e incentivar o compartilhamento de dados entre elas, mas a abordagem unificada da Genetec permite que a plataforma Security Center seja construída a partir de um único sistema escalável, projetado desde o início para acomodar conjuntos de dados em diversos domínios de segurança

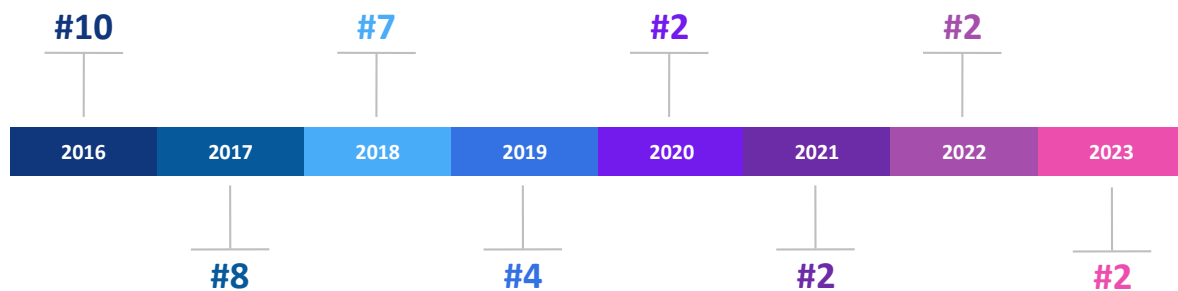
Do ponto de vista do integrador de sistemas, a unificação do sistema facilita a instalação do hardware e exige menos customização das arquiteturas dos equipamentos integrados O Security Center reforça ainda mais a unificação, pois é uma plataforma aberta totalmente interoperável com equipamentos de terceiros Esse fator facilitou oportunidades para os usuários finais investirem em projetos de retrofit econômicos para fazer upgrade em seus sistemas de controle de acesso existentes para o Security Center e o Synergis.

A Genetec também tem promovido soluções inovadoras de controle de acesso híbridas, combinando ambientes in loco e na nuvem Em 2023, a Genetec e a Axis Communications lançaram o *Axis Powered by Genetec*, uma oferta de produto combinada que reúne o software Synergis com um painel de controle IP AXIS A1210 ou AXIS A1610 O *Axis Powered by Genetec* foi a primeira iniciativa a oferecer aos integradores de sistemas um controlador de porta de borda projetado para o gerenciamento individualizado de acessos, pré-carregado com o software de controle de acesso de um fornecedor externo Esses controladores aproveitaram a arquitetura de computação na borda, mas também foram projetados com compatibilidade direta com a nuvem.

O compromisso da Genetec em oferecer soluções inovadoras de controle de acesso na nuvem e híbridas continuou com o lançamento do Security Center SaaS em 2024 que oferece gerenciamento unificado em nível corporativo de sistemas de controle de acesso, videomonitoramento e monitoramento de intrusão, com opções de processamento e armazenamento de dados tanto na nuvem quanto in loco.

Em termos de segurança cibernética, a Genetec ganhou reputação por adotar procedimentos rígidos, como o uso de uma abordagem em várias camadas, priorizar relacionamentos com fornecedores de segurança cibernética e focar em melhorias nos procedimentos de segurança dos usuários finais por meio do gerenciamento de privilégios em bancos de dados de controle de acesso baseados em funções. Esses recursos de software, juntamente com a ênfase em educar e firmar parcerias com fornecedores de hardware qualificados e integradores de sistemas, levaram a empresa a conquistar uma reputação de vigilante contra ameaças de segurança cibernética.

Ranqueamento na participação de mercado global do software de controle de acesso da Genetec (em termos de receita)



Em termos de posicionamento competitivo, mais de 75% da receita de software da Genetec em 2023 resultou de projetos nas Américas. Em 2016, a Genetec foi classificada como a sexta maior fornecedora de software (em termos de receita) na região das Américas; no entanto, a empresa cresceu e se tornou a segunda maior fornecedora de software da região em 2023, consolidando-se como um fornecedor dominante ao lado de players tradicionais como Honeywell e Johnson Controls. A Genetec foi classificada como a fornecedora de software de crescimento mais rápido com mais de 15% de participação de mercado na região em 2023.

Embora a Genetec tenha uma presença menor na Europa, Oriente Médio e África (EMEA), o Security Center obteve um crescimento significativo naquela região. Em 2016, a Genetec não era um dos vinte maiores fornecedores de software da região. A Genetec se tornou a nona maior concorrente na EMEA em 2023.

A Genetec fez um esforço concentrado para aumentar sua presença no mercado da Europa e do Oriente Médio nos últimos anos. Esse crescimento se deve em parte à sua posição como um dos principais fornecedores de software de videomonitoramento da região, já que uma porcentagem crescente de usuários finais que anteriormente investiram em seu sistema de gerenciamento de vídeo, o Omnicast™, posteriormente optaram pelo Synergis para controle de acesso, permitindo consolidar esses sistemas em uma plataforma unificada de um único fornecedor.

A Genetec também ocupa atualmente a décima posição entre os principais fornecedores de software na Ásia e Oceania. Quando as receitas do mercado chinês são excluídas da análise, a Genetec ocupa a oitava posição no restante da região. Os usuários finais na Ásia frequentemente escolhem opções de software mais em conta e preferem algo mais barato em vez de recursos avançados. No entanto, essa dinâmica começou a mudar; os usuários finais de nível corporativo na Ásia começaram a exigir software com mais recursos, mais customização, interfaces de usuário de maior qualidade e recursos de integração. A Omdia prevê que a participação de mercado da Genetec na Ásia e Oceania crescerá nos próximos cinco anos, à medida que as preferências do mercado continuarem evoluindo e a Genetec seguir priorizando oportunidades nos mercados indiano e da Oceania, que estão em rápida expansão.

Apêndice

Entre em contato

www.omnia.com
askananalyst@omnia.com

Consultoria Omdia

A Omdia é uma empresa líder de mercado em dados, pesquisa e consultoria focada em auxiliar provedores de serviços digitais, empresas de tecnologia e tomadores de decisões corporativas a prosperar na economia digital conectada. Por meio de nossa base global de analistas, oferecemos análises especializadas e insights estratégicos para a indústrias de TI, telecomunicações e mídia.

Geramos vantagem comercial para nossos clientes, fornecendo informações acionáveis para dar suporte ao planejamento de negócios, desenvolvimento de produtos e iniciativas de entrada no mercado.

Nossa combinação exclusiva de dados confiáveis, análise de mercado e expertise vertical do setor foi projetada para capacitar a tomada de decisões, ajudando nossos clientes a lucrar com novas tecnologias e capitalizar com modelos de negócios em evolução.

A Omdia faz parte da Informa Tech, uma empresa de serviços de informação B2B que atende ao setor de tecnologia, mídia e telecomunicações. O grupo Informa está listado na Bolsa de Valores de Londres.

Esperamos que esta análise ajude você a tomar decisões de negócios informadas e criativas. Caso tenha outras necessidades, a equipe de consultoria da Omdia pode ajudar sua empresa a identificar tendências e oportunidades futuras.

Aviso sobre direitos de reprodução e isenção de responsabilidade

A pesquisa, os dados e as informações da Omdia aqui mencionados (os “Materiais da Omdia”) são de propriedade da Informa Tech e suas subsidiárias ou afiliadas (juntamente com a “Informa Tech”) ou de seus provedores de dados terceirizados e representam dados, pesquisas, opiniões ou pontos de vista publicados pela Informa Tech e não são representações de fatos.

Os Materiais da Omdia refletem informações e opiniões a partir da data de publicação original e não a partir da data deste documento. As informações e opiniões expressas nos Materiais Omdia estão sujeitas a alterações sem aviso prévio e a Informa Tech não tem nenhum dever ou responsabilidade de atualizar os Materiais Omdia ou esta publicação como resultado destas alterações.

Os Materiais da Omdia são entregues “como estão” e “conforme disponíveis”. Nenhuma representação ou garantia, expressa ou implícita, é feita quanto à imparcialidade, precisão, integridade ou correção das informações, opiniões e conclusões contidas nos Materiais da Omdia.

Na extensão máxima permitida por lei, a Informa Tech e suas afiliadas, executivos, diretores, colaboradores, agentes e provedores de dados terceirizados se isentam de qualquer responsabilidade (incluindo, sem limitação, qualquer responsabilidade decorrente de falha ou negligência) quanto à precisão ou integridade ou uso dos Materiais da Omdia. A Informa Tech não será, sob nenhuma circunstância, responsável por qualquer negociação, investimento, comercial ou outras decisões feitas com base nos Materiais da Omdia.