

SureID

Ficha técnica



O que é o SureID?

Uma solução integrada de gestão de identidades e acessos em nuvem da JumpCloud, que entrega funcionalidades e configurações avançadas de integrações, protocolos de autenticação e segurança, complementada por serviços de visibilidade e suporte técnico especializado.





Desenvolvido para atender às necessidades específicas de Pequenas e Médias Empresas (PMEs), o SureID visa aprimorar a gestão de identidades e acessos, protegendo as aplicações de negócio e assegurando controle completo sobre quem acessa e o que está sendo acessado.

E por que preciso do SureID?



E por que preciso do SureID?

Imagine as pessoas, aplicações e permissões da sua empresa como passageiros, voos e assentos, onde o SureID atua como uma eficiente companhia aérea.

Ele garante a identificação de todas as pessoas, quais acessos ela possui e quais são as permissões dela nesse acesso, tudo isso de forma automatizada e dinâmica considerando diferentes contextos, garantindo assim que todos possam trabalhar de forma segura e coerente com sua função.



Controle e Segurança de Acessos

Seus negócios dependem de sistemas e dados críticos que não podem ser comprometidos, certo?

O SureID é a chave para manter esse controle e segurança contínuos. Ele vai além de simplesmente gerenciar acessos, adaptando-se em tempo real para garantir que apenas as pessoas autorizadas possam acessar os recursos necessários. Isso significa que, mesmo se houver uma tentativa de acesso não autorizado, o SureID redireciona e bloqueia automaticamente, garantindo que as operações da sua empresa permaneçam protegidas.



Monitoramento e Diagnóstico Avançado

Com o SureID, você tem um aliado tecnológico que monitora todas as atividades de acesso 24/7. Ele mantém registros detalhados de todas as tentativas, permitindo um diagnóstico preciso e intervenções rápidas e eficientes, frequentemente antes que qualquer problema seja percebido. Esta visibilidade detalhada facilita a identificação de padrões suspeitos e a ação preventiva contra possíveis pessoas e acessos não autorizados.



Segurança Robusta e Confiável

Para garantir a segurança completa, é essencial começar com uma base sólida. O SureID oferece uma gestão robusta de identidades e acessos, atuando como uma linha de defesa confiável que assegura que apenas os usuários apropriados tenham acesso às informações corretas. Isso proporciona tranquilidade ao saber que sua infraestrutura de TI está protegida contra ameaças comuns, enquanto se prepara para implementar medidas de segurança mais avançadas conforme necessário.



Base Sólida para uma Segurança Completa

O SureID estabelece uma fundação sólida para a segurança de identidades e acessos. Ele é ideal para empresas que reconhecem a importância de uma gestão eficiente de identidades e que precisam garantir segurança nos acessos às suas aplicações. Com o SureID, sua empresa poderá garantir conformidade com diversos requisitos das principais regulamentações, além de aprimorar todas as outras soluções de segurança já existentes. Isso aumentará significativamente a aderência aos padrões de segurança mais rigorosos do mercado.

Quem precisa do SureID?

Quem precisa do SureID?

Serviços de Saúde:

Clínicas médicas, laboratórios de diagnósticos e hospitais que manipulam dados sensíveis de pacientes e precisam garantir a confidencialidade e a integridade dessas informações, além de manter seus sistemas sempre online para atendimento eficaz.

Educação:

Escolas e instituições de ensino que dependem da conectividade para aulas online, gestão acadêmica e comunicação com pais e alunos, necessitando de uma rede segura que suporte essas atividades críticas.



Quem precisa do SureDevice?

Varejo e E-commerce:

Lojas físicas e virtuais que realizam transações online e gerenciam inventários em tempo real, exigindo uma rede segura e confiável para processar pagamentos e proteger informações de clientes.

Setor Financeiro e Contábil:

Empresas de contabilidade e consultoria financeira que lidam com informações financeiras sensíveis, requerendo uma camada robusta de segurança cibernética para proteger contra fraudes e vazamentos de dados.



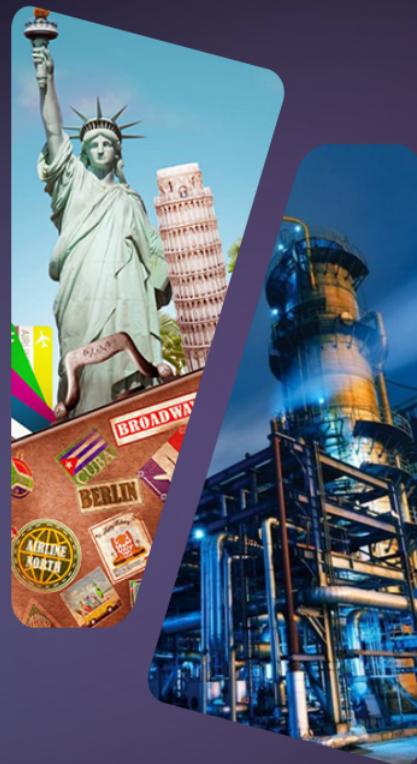
Quem precisa do SureDevice?

Turismo e Hospitalidade:

Hotéis, pousadas e agências de turismo que precisam garantir a segurança das transações online dos clientes e manter a operação de sistemas críticos para reservas e gestão hoteleira.

Produção e Indústria:

Indústrias de diversos segmentos que utilizam sistemas automatizados e precisam de uma rede segura e resiliente para manter a produção fluindo sem interrupções.



Quem precisa do SureDevice?

Serviços Profissionais:

Agências de marketing, escritórios de advocacia e empresas de TI, para quem a proteção de propriedade intelectual e dados de clientes é essencial, assim como a necessidade de conectividade constante para colaboração e entrega de projetos.

Infraestrutura e Logística:

Operadores logísticos e empresas de transporte que dependem de sistemas de rastreamento em tempo real e gestão logística, necessitando de redes seguras e sempre disponíveis.



Quais são os componentes da solução?



(A) Software:

A H1CA optou pela solução JumpCloud (SureID) como sua solução de gerenciamento de identidades e acessos, amplamente utilizada e reconhecida em todo mercado e institutos de avaliações especializados. Esta escolha demonstra o compromisso em oferecer uma gestão de identidades e acessos robusta e segura, além de possibilitar oferecer uma plataforma de unificação de outras funcionalidades além do SureID, que permitem complementar toda a oferta de produtos da H1CA.



Sobre a JumpCloud

A JumpCloud se destaca no cenário global de gerenciamento de identidades e acessos (IAM) pela sua robustez, flexibilidade e desempenho excepcional. Mais do que uma simples ferramenta de controle de acesso, a JumpCloud atua como um guardião centralizado dos recursos digitais, oferecendo tecnologia avançada para gerenciar, autenticar e proteger usuários e dispositivos.

Sua capacidade de integrar-se a diversos ambientes de TI, tanto locais quanto na nuvem, permite identificar e responder rapidamente a ameaças potenciais. Reconhecida por institutos de pesquisa independentes, a liderança da JumpCloud é evidenciada pela inovação contínua e eficácia em manter a segurança e a integridade dos ativos digitais das empresas.



(B) Serviços de Configuração e Gerenciamento H1CA:

A Hackone Consultores Associados (H1CA) eleva o padrão de serviços de configuração e gerenciamento, oferecendo uma abordagem personalizada que vai além do convencional. Cada projeto é cuidadosamente analisado para assegurar que a solução de segurança seja meticulosamente otimizada, refletindo as especificidades e exigências únicas de cada cliente. Este serviço garante que as capacidades plenas da solução JumpCloud sejam utilizadas efetivamente, transformando potencial técnico em segurança real e tangível.



(B1) Implementação:

A excelência na implementação começa muito antes da disponibilização do ambiente em nuvem da JumpCloud. Através de um levantamento técnico detalhado e uma colaboração próxima com os consultores H1CA, todas identidades e acessos que serão configurados são levantados. Um checklist pré-projeto meticuloso garante que todos os requisitos necessários sejam atendidos, assegurando uma implementação sem contratempos. A presença do consultor no local, aliada ao suporte remoto do Centro de Operações da Hackone, confere agilidade e eficácia ao processo de ativação.



(B2) Visibilidade:

Desde o momento da instalação, o SureID é integrado ao sistema de visibilidade avançada oferecida na oferta SureID, Data Ranger. Os dados analíticos de uso do SureID são coletados continuamente, sem interrupções, permitindo uma visão abrangente das suas identidades e acessos através do SureID.

A plataforma de visibilidade oferece visualizações gráficas detalhadas, disponíveis em tempo real para os clientes. Além disso, uma gama de relatórios personalizados e em tempo real são disponibilizados em uma página exclusiva no Data Ranger.



(B3) Suporte:

A Hackone disponibiliza uma equipe de suporte altamente qualificada, pronta para intervir em incidentes ou esclarecer dúvidas relacionadas ao SureID. Os serviços de suporte estão disponíveis por email e telefone, dentro dos limites de tempo de operação de suporte de cada contrato.

O suporte está disponível nos dias úteis, de segunda a sexta-feira (exceto feriados nacionais), garantindo assistência oportuna durante o horário comercial. Para clientes que necessitam de cobertura adicional, a H1CA oferece planos de suporte com atendimento estendido, disponíveis mediante consulta.



(B4) Curadoria:

Cada cliente do SureDevice beneficia-se do acompanhamento mensal realizado por um Consultor Associado Hackone, que oferece uma análise personalizada do uso dos serviços.

Através do boletim mensal digital os clientes recebem insights valiosos e informações atualizadas sobre cibersegurança e gestão de identidades e acessos, permitindo otimizar a utilização dos serviços SureDevice. A curadoria é enriquecida através de conteúdo relevante mantendo os clientes informados sobre as melhores práticas e novidades nos campos da cibersegurança e gestão de identidades e acessos.

O que compõe o SureID?



Cloud Directory

É a espinha dorsal do sistema de gerenciamento de identidades do JumpCloud, permitindo o gerenciamento centralizado de usuários, grupos e dispositivos. Atua como um diretório de usuários baseado na nuvem, substituindo ou complementando soluções tradicionais como o Active Directory (AD) ou o LDAP. Facilita o gerenciamento de autenticações, autorizações e políticas em ambientes de TI híbridos.

Funcionalidades do Cloud Directory

- Criação de Usuários de forma manual
- Importação de Usuário via CSV
- Importação e Sincronização de Usuários e grupos do Google Workspace
- Importação e Sincronização de Usuários e grupos do Microsoft 365/Azure AD
- Importação e Sincronização de Usuários e grupos a partir do Active Directory
- Adição de contas com Atualização em Tempo Real do BambooHR
- Adição de contas com Atualização em Tempo Real do bob
- Importação e Sincronização de Usuários do Namely
- Importação e Sincronização de Usuários do Personio
- Importação e Sincronização de Usuários do Workday
- Importação e Sincronização de Usuários em Tempo Real do Okta
- Adição de Usuários através de Integração Personalizada via API
- Adição de Usuários com Integração SCIM Personalizada
- Agendamento de Suspensão de Contas de Usuários
- Agendamento de Ativação de Contas de Usuários
- Geração de Arquivo CSV com Dados dos Usuários
- Geração de Arquivo JSON com Dados dos Usuários
- Personalização do Status na Etapa de Criação de Usuários



Multi-Factor Authentication (MFA)

O JumpCloud suporta vários métodos de Autenticação Multifator (MFA), reforçando a segurança ao exigir que os usuários forneçam duas ou mais evidências de sua identidade ao acessar sistemas, aplicativos e dados. Aqui estão os tipos de MFA que o JumpCloud oferece:

- **TOTP (Time-Based One-Time Password):** Utiliza senhas que são válidas por um curto período de tempo, geradas por aplicativos compatíveis com TOTP, como Google Authenticator ou Microsoft Authenticator. Os usuários inserem essa senha junto com suas credenciais normais durante o login.
- **Push Notifications via JumpCloud Protect:** O JumpCloud também oferece sua própria solução de MFA via push notifications com o aplicativo JumpCloud Protect. Os usuários recebem uma notificação em seu dispositivo móvel quando uma tentativa de login é feita, e eles podem aprovar ou negar essa tentativa com um simples toque.

Multi-Factor Authentication (MFA)

- U2F (Universal 2nd Factor): Permite o uso de dispositivos de segurança físicos, como YubiKeys, para autenticação. O usuário simplesmente insere o dispositivo em sua porta USB ou o aproxima do dispositivo para autenticar via NFC, proporcionando uma camada adicional de segurança.
- WebAuthn (Web Authentication): Uma norma para autenticação na web que permite o uso de dispositivos de segurança, como chaves de segurança FIDO2, e mecanismos de autenticação biométrica.



Directory Insights

Fornecer visibilidade detalhada e registros de auditoria sobre atividades de usuários e dispositivos dentro do ambiente do JumpCloud. Isso inclui informações sobre autenticações, modificações de diretório, atividades de SSO e MFA, permitindo aos administradores monitorar a conformidade, analisar tendências de segurança e responder a incidentes de segurança com eficácia.

Directory Insights

- Histórico de ações dos Usuários
- Histórico de ações dos Administradores
- Histórico de ações dos dispositivos
- 9 Filtros de visualizações de registros pré-definidos
- 8 filtros por tipo de serviço para geração de registros
- Mais de 80 filtros por tipo de evento para geração de registro
- Mais de 70 outros tipos de filtros adicionais para geração de registro
- Personalização do período desejado do registro
- Mais de 100 colunas para personalização de registro
- Exportação de registro em CSV
- Exportação de registro em JSON
- Registro de Usuários do Dispositivo
- Registro de Usuários do Diretório
- Registro de Usuários dos Servidores LDAP
- Registro de Usuários do RADIUS
- Registro de Usuários dos Aplicativos SSO(Single-Sign-On)
- Registro de Usuários de Grupos de Usuários
- Registro de Atualizações de Navegador
- Registro de Atualizações do Sistema Operacional



Cloud Directory Integrations

Permite a integração do diretório JumpCloud com uma ampla gama de aplicações SaaS, infraestrutura de nuvem, redes e sistemas operacionais. Essas integrações facilitam o gerenciamento unificado de identidades, permitindo o SSO, a sincronização de diretórios e a gestão de políticas de segurança em diversos ambientes de TI.

Cloud Directory Integrations

- Importação, Gerenciamento e Sincronização de Usuários e grupos do Google Workspace
- Sincronização de Atributos Específicos do Google Workspace
- Importação, Gerenciamento e Sincronização de Usuários e grupos do Microsoft 365/Azure AD
- Sincronização de Atributos Específicos do Microsoft 365/Azure AD
- Importação, Gerenciamento e Sincronização de Usuários e grupos a partir do Active Directory
- Adição de contas com Atualização em Tempo Real do BambooHR
- Adição de contas com Atualização em Tempo Real do bob
- Importação e Sincronização de Usuários do Namely
- Importação e Sincronização de Usuários do Personio
- Importação e Sincronização de Usuários do Workday
- Importação e Sincronização de Usuários em Tempo Real do Okta
- Adição de Usuários através de Integração Personalizada via API



Single Sign-On

Uma característica que permite aos usuários acessar múltiplos serviços e aplicações com uma única identidade de usuário e senha.

O JumpCloud suporta vários protocolos de Single Sign-On (SSO) para permitir que os usuários acessem múltiplos aplicativos e serviços com uma única identidade, melhorando tanto a segurança quanto a conveniência. Aqui estão os detalhes:

Single Sign-On

SAML 2.0 (Security Assertion Markup Language): Um protocolo amplamente utilizado para SSO, que permite uma troca segura de credenciais de autenticação e autorização entre diferentes domínios.

- OIDC (OpenID Connect): Baseado em OAuth 2.0, adiciona uma camada de identidade ao processo, facilitando a autenticação de usuários e a troca segura de informações de perfil.
- SCIM (System for Cross-domain Identity Management): Embora não seja um protocolo de SSO, o SCIM é relevante no contexto de gerenciamento de identidades e acessos. Ele é utilizado para automatizar o intercâmbio de informações de usuário entre sistemas, facilitando a gestão do ciclo de vida de identidades em várias plataformas e aplicativos. O SCIM ajuda as organizações a manter as informações dos usuários sincronizadas e atualizadas, complementando as capacidades de SSO ao simplificar o gerenciamento de contas e grupos em diferentes serviços.
- Permite utilizar atributos de Usuários
- Permite utilizar atributos baseados em Grupos de Usuários
- Permite a escolha se a aplicação irá aparecer no portal do Usuário
- Permite personalizar a logo da Aplicação
- Permite o Gerenciamento de Usuários via API customizável utilizando Bearer Token, chave de API ou OAuth2.0

Cloud LDAP & RADIUS

Oferece serviços de Lightweight Directory Access Protocol (LDAP) e Remote Authentication Dial-In User Service (RADIUS) baseados na nuvem, permitindo a integração segura de aplicações e recursos de rede com o JumpCloud. Isso habilita a autenticação centralizada para serviços que suportam esses protocolos, como VPNs, servidores de arquivos e mais, sem a necessidade de infraestrutura local.

Cloud LDAP & RADIUS

- **Cloud LDAP:**

- . Política Condicional - O JumpCloud suporta políticas condicionais de acesso atreladas ao Cloud LDAP, permitindo assim por exemplo exigir MFA de usuários ao acessar recursos via LDAP.

- . Push MFA - O Cloud LDAP do JumpCloud suporta autenticação MFA TOTP mas também utilizando Push, facilitando assim a implementação e adoção dos usuários ao recurso.

- . LDAP com SSL/TLS - O Cloud LDAP do JumpCloud suporta autenticação LDAP de forma criptografada e baseada em certificado digital.

- **Cloud RADIUS:**

- . Passwordless - O Cloud RADIUS do JumpCloud suporta autenticação sem senha baseada em certificados digitais.

- . Push MFA - O Cloud RADIUS do JumpCloud suporta autenticação MFA TOTP mas também utilizando Push, facilitando assim a implementação e adoção dos usuários ao recurso.

- . Múltiplos Radius Client - O Cloud RADIUS do JumpCloud suporta múltiplos clientes de RADIUS, permitindo integrar diversos equipamentos em um mesmo RADIUS Server.

- . VLAN Dinâmica e RADIUS Reply Attributes - O Cloud RADIUS do JumpCloud suporta inserção de atributos de resposta baseados em grupos de usuários, permitindo assim utilizá-los para configuração de VLAN Dinâmica para redes Wi-Fi ou LAN.



AM Dashboards & Reports (Data Ranger)

O Data Ranger é uma solução exclusiva entregue na oferta H1CA, visando apresentar dashboards e relatórios abrangentes sobre a gestão de identidades e acessos em tempo real, oferecendo uma visão geral e análises detalhadas do estado das identidades e acessos, facilitando a tomada de decisões e gestão do ambiente.

IAM Dashboards & Reports (Data Ranger)

Com o Data Ranger, o cliente obtém:

- Visualização de dashboards com informações sobre disponibilidade, número de usuários gerenciados, número de acessos
- Visualização de status MFA dos usuários separados por tipo de MFA
- Visualização de contas ativas, inativas e bloqueadas em tempo real
- Visualização de aplicações mais acessadas
- Visualização de quantos usuários possuem acesso em cada aplicação;
- Aplicação de filtros interativos diretamente na dashboard;
- Geração de diversos relatórios em tempo real de várias informações sobre os usuários e acessos gerenciados através do JumpCloud.
- Exportação dos relatórios em diversos formatos como .csv, .json, .pdf e .xls.
- Visualização em tempo real do número de licenças utilizadas;
- Conferência das funcionalidades disponíveis para uso de acordo com o SKU contratado;
- Acesso a base de conhecimento com conteúdos técnicos e exclusivos oferecidos pelo time de especialistas em português sobre a plataforma JumpCloud e suas funcionalidades;
- Alertas sobre diversos temas como novas funcionalidades, atualizações, procedimentos e avisos de segurança;



Suporte Técnico (Core)

O serviço de suporte oferece o mais alto nível de atendimento e assertividade do mercado, considerando contextos, históricos e produtos referentes ao cliente. O serviço de suporte para essa oferta inclui os atendimentos de chamados de nível 1, 2 e 3 através de um portal de chamados dedicado e customizado para a Linx.

Além de portal de chamados, será disponibilizado atendimento telefônico e através de email. Contamos com um time de profissionais certificados em JumpCloud e outras áreas de conhecimento, além de manter treinamentos constantes para que todos estejam sempre preparados para atender todas as solicitações.



Suporte Técnico (Core)

Para garantir qualidade e agilidade no atendimento, todos os chamados de suporte são classificados automaticamente, revisados e têm o SLA de atendimento e resolução adequado associado ao mesmo, garantindo assim ao cliente tempos de atendimento e resolução dentro da expectativa de acordo com a urgência da solicitação.

Todos chamados podem ser abertos por email, telefone ou via um completo portal de chamados, sendo que através do portal o cliente consegue classificar a categoria, sub-categoria, assunto e demais informações do chamado, sendo mais assertivo em sua solicitação, além de poder acompanhar de maneira transparente o status e andamento do chamado.



Suporte Técnico (Core)

Dentro do portal de chamados os clientes encontram também a nossa completa base de conhecimentos, com diversos procedimentos totalmente exclusivos desenvolvidos pelo time de especialistas.

Os procedimentos são sugeridos todas as vezes que um cliente abre um chamado baseado na descrição do chamado, podendo oferecer ao cliente uma solução para seu chamado antes mesmo dele precisar ser aberto.

Em situações em que chamados precisam envolver fabricantes, o time de especialistas fará toda intermediação entre o cliente e fabricante, não sendo necessário que o cliente fale inglês ou precise lidar com outra pessoa para ter seu chamado resolvido.