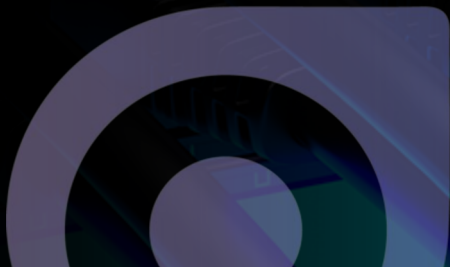




**Consultores
Associados**
Hackone ®

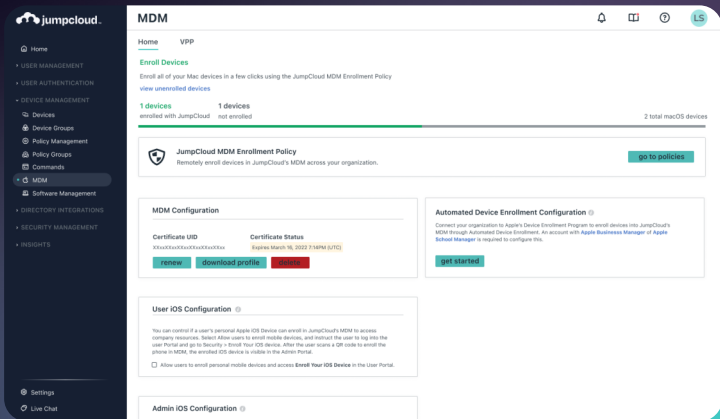
SureDevice

Ficha técnica



O que é o SureDevice?

Uma solução de gerenciamento de dispositivos móveis (MDM) em nuvem da JumpCloud que proporciona controle centralizado e segurança avançada para dispositivos em nuvem. Ela oferece funcionalidades abrangentes e configurações sofisticadas, suporte com diversos sistemas operacionais, instalações remotas, políticas de segurança e é complementada por serviços de visibilidade detalhada e suporte técnico especializado.





Desenvolvido para atender às necessidades específicas de Pequenas e Médias Empresas (PMEs), o SureDevice visa garantir a proteção e o desempenho ideal dos dispositivos da sua empresa.

E por que preciso do SureDevice?



E por que preciso do SureDevice?

O SureDevice atua como um verdadeiro maestro dentro do seu parque de dispositivos. Ele garante que todos os dispositivos estão identificados, padronizados, gerenciados e atualizados com todos os softwares e configurações necessárias para o pleno funcionamento da forma mais segura e eficiente possível, sem permitir que nenhum deles fique fora do padrão de excelência estabelecido.



Controle e Segurança de Dispositivos

Seus negócios dependem de dispositivos que acessam aplicações críticas e não podem ser comprometidos, certo?

O SureDevice é essencial para manter esse controle e segurança contínuos. Ele vai além de simplesmente gerenciar dispositivos, permitindo adequar todos os dispositivos aos padrões de segurança exigidos para a operação da sua empresa. Isso significa que, mesmo se o dispositivo for um notebook ou celular, corporativo ou pessoal, será possível gerenciá-los da maneira adequada.



Monitoramento e Diagnóstico Avançado

Com o SureDevice, você conta com uma tecnologia que monitora todas as atividades dos dispositivos 24/7. Ele mantém registros detalhados de todas as configurações, softwares instalados e políticas aplicadas, 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 ameaças.



Segurança Robusta e Confiável

Para garantir uma segurança completa, é essencial garantir que o que está sendo utilizado pelas pessoas da sua empresa esteja seguro e de fato seja um dispositivo gerenciado. O SureDevice oferece uma gestão robusta de dispositivos, atuando como uma linha de defesa confiável que assegura que todos seus dispositivos estejam no padrão de segurança correto. Isso proporciona tranquilidade, sabendo 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 SureDevice estabelece uma fundação sólida para a segurança de dispositivos. Ele é ideal para empresas que reconhecem a importância de uma gestão eficiente de dispositivos e que precisam garantir segurança dos seus dados através do controle de qual padrão de dispositivo as pessoas utilizarão para acessá-los. Com o SureDevice, sua empresa poderá garantir conformidade com diversos requisitos das principais regulamentações, estabelecendo um padrão eficiente de configuração segura dos dispositivos. Isso aumentará significativamente a aderência aos padrões de segurança mais rigorosos do mercado.

Quem precisa do SureDevice?

Quem precisa do SureDevice?

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.

Sector 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:

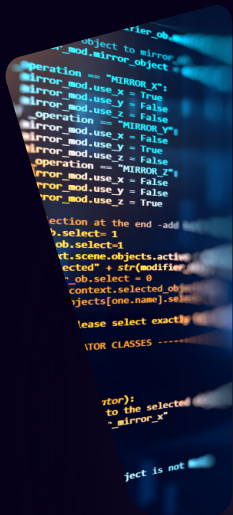
Agências de marketing, escritórios de advocacia e empresas de TI, para quem a proteção de propriedade intelectual e dados de clientes é essencial, assim como a necessidade de conectividade constante para colaboração e entrega de projetos.

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 pelo JumpCloud (SureDevice) como sua solução de gerenciamento de dispositivos móveis (MDM), amplamente utilizada e reconhecida no mercado por institutos de avaliação especializados. Esta escolha demonstra o compromisso em oferecer uma gestão de dispositivos robusta e segura, proporcionando controle centralizado, monitoramento contínuo e políticas de segurança avançadas. Além disso, o SureDevice permite complementar a oferta de produtos da H1CA, integrando funcionalidades adicionais que otimizam a proteção e o desempenho dos dispositivos móveis nas empresas.



Sobre a JumpCloud

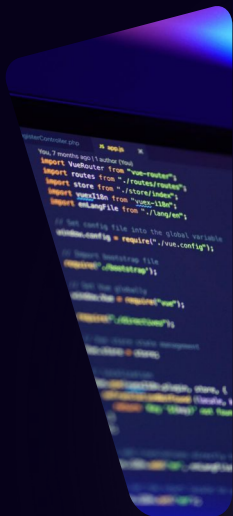
A JumpCloud se destaca no cenário global de gerenciamento de dispositivos móveis (MDM) pela sua robustez, flexibilidade e desempenho excepcional. Mais do que uma simples ferramenta de gerenciamento de dispositivos, a JumpCloud oferece uma solução abrangente para gerenciar, proteger e otimizar dispositivos móveis em ambientes corporativos.

Com funcionalidades avançadas, como monitoramento contínuo, controle remoto, e políticas de segurança personalizadas, a JumpCloud garante que todos os dispositivos estejam seguros e em conformidade com as políticas corporativas. Além disso, sua integração com soluções de gerenciamento de identidades e acessos (IAM) fortalece ainda mais a segurança e o controle sobre quem acessa quais recursos. 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, todos dispositivos 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 SureDevice é integrado ao sistema de visibilidade avançada oferecida na oferta SureDevice, Data Ranger. Os dados analíticos de uso do SureDevice são coletados continuamente, sem interrupções, permitindo uma visão abrangente das suas identidades e acessos através do SureDevice.

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 SureDevice. 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 SureDevice?



Device Management e MDM

Permite o gerenciamento centralizado de dispositivos móveis e de desktop, independentemente do sistema operacional. Inclui provisionamento de dispositivos, configurações de segurança, gestão de aplicativos e políticas de conformidade, permitindo às organizações assegurar o controle e a segurança dos dispositivos que acessam seus recursos.

Device Management e MDM

- . Gerenciamento de Dispositivos Windows
- . Gerenciamento de Dispositivos macOS
- . Gerenciamento de Dispositivos Linux
- . Gerenciamento de Dispositivos com Puppet
- . Gerenciamento de Dispositivos com Chef
- . Gerenciamento de Dispositivos iOS
- . Gerenciamento de Dispositivos Android
- . Comandos de Segurança em Dispositivos macOS
- . Comandos de Segurança em Dispositivos Windows
- . Comandos de Segurança em Dispositivos Linux
- . Comandos de Segurança em Dispositivos iOS
- . Comandos de Segurança em Dispositivos iPadOS
- . Visão Geral do Dispositivo
- . Realizar ações em massa, como habilitar o MFA no Dispositivo
- . Permite exportar para JSON ou CSV um inventário completo de Dispositivos
- . Permite a criação de filtros de pesquisa baseado em status do Dispositivo
- . Permite a criação de filtros de pesquisa baseado em status do Dispositivo
- . Permite a criação de filtros de pesquisa baseado no sistema operacional do Dispositivo
- . Permite a criação de filtros de pesquisa baseado na criptografia de disco do Dispositivo
- . Permite a criação de filtros de pesquisa baseado se o Dispositivo está integrado ao MDM JumpCloud
- . Permite a criação de filtros de pesquisa baseado se o Dispositivo não está integrado ao MDM
- . Permite a criação de filtros de pesquisa baseado se o Dispositivo está integrado ao MDM de terceiros
- . Permite ver a quais grupos de dispositivos o Dispositivo está vinculado
- . Permite ver quais políticas estão vinculadas ao Dispositivo
- . Permite ver o status de aplicação das políticas ao Dispositivo
- . Permite ver quais comandos estão vinculados ao Dispositivo
- . Permite ver quais Usuários estão vinculados ao Dispositivo



Remote Access

Facilita o acesso remoto seguro a sistemas e aplicativos, independente da localização do usuário. Essa funcionalidade suporta cenários de trabalho flexíveis, permitindo aos funcionários acessar recursos de TI necessários de qualquer lugar, mantendo altos padrões de segurança.

Remote Access

- Acesso Remoto Silencioso a dispositivos macOS
- Acesso Remoto Assistido Utilizando One-time Access Code a dispositivos macOS
- Acesso Remoto Não Assistido a dispositivos macOS
- Acesso a Pastas do Dispositivo Durante o Acesso Remoto a Dispositivos macOS
- Selecione Diferentes Monitores Durante a Sessão de Acesso Remoto a Dispositivos macOS
- Sincronia da Função "Copiar/Colar" Durante a Sessão de Acesso Remoto a Dispositivos macOS
- Colete Relatórios sobre a Sessão de Acesso Remoto a Dispositivos macOS
- Acesso Remoto Silencioso a dispositivos Windows
- Acesso Remoto Assistido Utilizando One-time Access Code a dispositivos Windows
- Acesso Remoto Não Assistido a dispositivos Windows
- Acesso a Pastas do Dispositivo Durante o Acesso Remoto a Dispositivos Windows
- Selecione Diferentes Monitores Durante a Sessão de Acesso Remoto a Dispositivos Windows

Remote Access

- Sincronia da Função "Copiar/Colar" Durante a Sessão de Acesso Remoto a Dispositivos Windows
- Uso do Atalho "Ctrl + Alt + Del" Durante a Sessão de Acesso Remoto a Dispositivos Windows
- Troque de um Usuário do Dispositivo para outro Durante a Sessão de Acesso Remoto a Dispositivos Windows
- Colete Relatórios sobre a Sessão de Acesso Remoto a Dispositivos Windows
- Acesso Remoto Silencioso a dispositivos Linux
- Acesso Remoto Assistido Utilizando One-time Access Code a dispositivos Linux
- Acesso Remoto Não Assistido a dispositivos Linux
- Acesso a Pastas do Dispositivo Durante o Acesso Remoto a Dispositivos Linux
- Selecione Diferentes Monitores Durante a Sessão de Acesso Remoto a Dispositivos Linux
- Sincronia da Função "Copiar/Colar" Durante a Sessão de Acesso Remoto a Dispositivos Linux



Background Tools

Fornecer um conjunto de ferramentas que operam em segundo plano para manutenção, diagnóstico e resolução de problemas nos dispositivos gerenciados. Isso inclui scripts personalizados e automações que podem ser aplicados sem interrupção do trabalho do usuário.

- Acesso Remoto ao Terminal em Dispositivos macOS
- Acesso à Pastas do Sistema em Dispositivos macOS
- O Acesso à Pastas do Sistema possibilita mover, deletar, subir ou baixar arquivos em Dispositivos macOS
- Acesso Remoto ao Terminal em Dispositivos Windows
- Acesso à Pastas do Sistema em Dispositivos Windows
- O Acesso à Pastas do Sistema possibilita mover, deletar, subir ou baixar arquivos em Dispositivos Windows
- Acesso Remoto ao Shell em Dispositivos Linux



Directory Insights

Oferece visibilidade detalhada e registros de auditoria sobre atividades de usuários e dispositivos, incluindo acessos, autenticações e alterações em diretórios. Essas informações ajudam a monitorar a segurança, a conformidade e a operacionalidade do ambiente de TI.

- 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 de registro
- Personalização do período desejado do registro
- Mais de 100 colunas para personalização de registro
- Exportação de registro em CSV



Directory Insights

- 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



System Insights

Fornece análises e relatórios detalhados sobre o estado dos sistemas operacionais e do hardware nos dispositivos gerenciados, incluindo informações sobre utilização de recursos, atualizações de software e configurações de sistema. Esses insights ajudam na otimização de recursos e na gestão proativa da infraestrutura de TI.



System Insights

- Informações sobre Bateria
 - Fabricante
 - Data de Fabricação
 - Modelo
 - Número de Série
 - Contagem de Ciclos
 - Saúde da Bateria
 - Condição
 - Estado de Carregamento
 - Capacidade de Fabrica
- Capacidade Máxima
- Capacidade Atual
- Porcentagem Restante
- Amperagem
- Voltagem
- Minutos até vazia
- Minutos até carga máxima
- ID do Sistema
- Data da Coleta dos Dados

System Insights

- **Informações de Certificado**
 - . Nome
 - . Data de Expiração
- **Acidentes**
 - . Tipo
 - . Processo
 - . Data e Hora
- **Criptografia de Disco**
 - . Nome
 - . Disco criptografado
- **Políticas Gerenciadas**
 - . Domínio
 - . Campo
 - . Valor
- **Armazenamento**
 - . Valor do Armazenamento
 - . Armazenamento Disponível
- **Impressoras**
- **Pastas Compartilhadas**
- **Preferências de Compartilhamento**
 - . Compartilhamento de Tela
 - . Compartilhamento de Arquivos
 - . Compartilhamento de Impressoras
 - . Login Remoto
 - . Gerenciamento Remoto
 - . Eventos Apple Remoto(macOS)
 - . Compartilhamento de Internet
 - . Compartilhamento de Bluetooth
 - . Compartilhamento de Disco
 - . ID do Sistema
 - . Data da Coleta dos Dados
- **Itens de Inicialização**

System Insights

- **Informações do Sistema**

- . Hostname
- . UUID
- . Tipo de CPU
- . Sub tipo de CPU
- . Marca da CPU
- . Quantidade Física de Núcleos de CPU
- . Quantidade Lógica de Núcles de CPU
- . Microcódigo de CPU
- . Memória Física
- . Vendedor do Hardware
- . Modelo do Hardware
- . Versão do Hardware
- . Serial do Hardware
- . Nome do Computador
- . Hostname Local
- . ID do Sistema
- . Data da Coleta de Dados

- **Dispositivos USB**

- . Modelo
- . Removível

- **Kernel**

- . Versão
- . Argumentos
- . Caminho
- . Dispositivo
- . ID do Sistema
- . Data da Coleta dos Dados

- **Controles do Sistema**

- . Nome
- . Subsistema
- . Valor Atual

- **Aplicações**

- . Nome
- . Versão
- . Última vez Iniciado

- **Plugins de Browser**

- **Extensões do Google Chrome**

- . Nome
- . Versão

- **Extensões do Firefox**

- **Extensões do Safari**

- Camada de Aplicação do Firewall

- .Permitir Assinatura habilitada
- .Descarregamento de Firewall
- .Estado Global
- .Logging Habilitado
- .Opção de Logging
- .Stealth Habilitado
- .Versão
- .ID do Sistema
- .Data da Coleta de Dados

- **ETC Hosts**

- .Hostname
- .Endereço

- **Interface de Endereços**

- .Interface
- .Endereço

- **Detalhes de Interface**

- .Interface
- .Endereço MAC
- .Status da Conexão
- .Velocidade de Banda

- **Estados das Chaves SSH de Usuários**



Patch Management

Automatiza a distribuição e aplicação de patches de segurança e atualizações de software para os dispositivos gerenciados, garantindo que estes estejam sempre atualizados e protegidos contra vulnerabilidades conhecidas.

- Controle de Atualizações para Dispositivos macOS
- Controle de Versão de OS para Dispositivos macOS
- Controle de Pequenos Pacotes de Atualizações de Dispositivos macOS
- Controle de Quantos Dias o Usuário Pode Adiar Atualizações para Dispositivos macOS
- Personalização de Notificações para Atualizações para Dispositivos macOS

Patch Management

Controle de Atualizações para Dispositivos Windows

- Instalar Automaticamente Atualizações Menores
- instalar Automaticamente Atualizações
- Comportamento das Atualizações Automáticas
- Personalizar Quais Dias da Semana Instalar Atualizações
- Personalizar Qual Hora do Dia Instalar Atualizações
- Personalizar em Qual Semana do Mês Instalar Atualizações
- Personalizar a Detecção de Novas Atualizações
- Permitir a Instalação Automática de Atualizações Durante Manutenções Automáticas
- Permitir Atualização de Produtos Microsoft
- Restringir a Atualização de Drivers no Windows Update
- Remover o Acesso a Opção de Pausar a Atualização
- Remover o Acesso a Todas as Opções do Windows Update
- Habilitar que o Gerenciador de Energia do Windows, automaticamente "acorde" o Sistema para que Atualizações Agendadas Sejam Instaladas
- Desabilitar a Ferramenta de Atualização via Windows Update
- Desabilitar o Safeguards para Atualizações
- Gerenciar o Comportamento com Versões Teste de Atualizações
- Configure qual Versão o Sistema Deverá Receber na Próxima Atualização

Patch Management

- **Configure as Notificações das Atualizações para Dispositivos Windows**
 - . Configure a Notificação de Reinicialização Automática para Atualizações
 - . Configure a Segunda Notificação de Reinicialização Automática para Atualizações
 - . Configure a Notificação de Alerta para Atualizações Agendadas
 - . Permita que Usuários Não Administradores Recebam
- . Notificações sobre Atualizações
 - . Habilite Opções para Notificações de Atualizações
- **Configure Prazos e Adiamentos de Atualizações para Dispositivos Windows**
 - . Adie Atualizações
 - . Interrompa Atualizações Iniciadas Nesta Data
 - . Adie Atualizações de Ferramentas

- . Controle qual Versão de Atualização Instalar
- . Interrompa Atualizações de Ferramentas Iniciadas

Nesta Data

- **Configurações de Reinicialização Automáticas e Obrigação de Atualização de Dispositivos Windows**
 - . Configure uma Data Limite para a Reinicialização
 - . Restrinja a Reinicialização Automática com Usuários Logados em Atualizações Agendadas
 - . Desabilite a Reinicialização Automática para Atualizações Durante Horas de Trabalho
 - . Configure as Horas de Trabalho
 - . Force a Reinicialização Automática para Atualizações Agendadas
 - . Especifique a Data Limite para Atualizações e Reinicializações

Patch Management

- **Controle de Atualizações para Dispositivos Linux**

- . Configure quais Atualizações Serão Instaladas
- . Configure a Verificação de Novas Atualizações
- . Configure o Comportamento para Atualizações de

Segurança

- . Configure o Comportamento para Outras

Atualizações

- . Restrinja Atualizações a Versões LTS
- . Defina Quanto Tempo a Atualização Poderá ser

Adiada



IAM 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.

Patch Management

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 cada cliente.

Além de portal de chamados, será disponibilizado atendimento telefônico e através de email.



Suporte Técnico (Core)

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.

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.

Quais são os requisitos do SureDevice?



Requisitos de Hardware e Conectividade para o JumpCloud Agent (Windows, macOS e Linux)

Disco: 600mb* mínimo

Memória RAM: 20mb mínimo

Internet: 2Mbps mínimo

** Em dispositivos Linux talvez seja requerido menor ou maior espaço de disco uma vez dependerá dos pacotes já instalados ou não no sistema.*



Navegadores Suportados

Recomendada versão desktop dos seguintes navegadores:

- Chrome
- Firefox
- Safari*

**Para visualização adequada no Safari, vá em View > Text Encoding, então selecione Western (ISO Latin 1).*



JumpCloud Agent para Windows

Exigida versão Windows Pro para pleno funcionamento da ferramenta

- 10 (64 bit e build acima da 1909)
- 11
- Server: 2012 R2*
- Server: 2016 (64 bit)
- Server: 2019
- Server: 2022

**Server 2012 R2 já está em End Of Support*



JumpCloud Agent para macOS

- Monterey 12.x*
- Ventura 13.x
- Sonoma 14.x
- Processadores Intel e Apple Silicon são suportados

**Monterey 12.x entrará em End Of Support em Dezembro/2024*

Para utilização das funcionalidades de Zero-Touch e ou ADE é requerido cadastro no Apple Business Manager (serviço gratuito da Apple para MDM)



JumpCloud Agent para Linux

- Ubuntu (amd64, arm64) 18.04, 20.04, 22.04 e 24.04
- Amazon Linux (amd64, arm64) 2*
- Amazon Linux 2022 e 2023
- CentOS (amd64) 7*
- Debian (amd64) 10*
- Debian (amd64, arm64) 11 e 12
- Fedora (amd64) 38*
- Fedora (amd64) 39**

- Linux Mint (Cinnamon) (amd64) 20, 21
- Pop!_OS (amd64) 22.04
- RHEL (amd64) 7 e 8
- RHEL (amd64, arm64) 9
- Rocky Linux (amd64, arm64) 8 e 9

**Já estão em End Of Support*

*** Entrará em End Of Support em
Dezembro/2024*



JumpCloud MDM para iOS, iPadOS, tvOS

- iOS 13.0 ou superior
- iPadOS 13.0 ou superior
- tvOS 13.0 ou superior

Para utilização das funcionalidades de Zero-Touch e ou ADE é requerido cadastro no Apple Business Manager (serviço gratuito da Apple para MDM)



JumpCloud EMM para Android

Para dispositivos Android pessoais, porém com perfil de trabalho (personal/employee-owned device). Nesse tipo de dispositivo, apenas o container corporativo é gerenciado e poucas configurações do dispositivo como um todo

- Android 5.1 (Lollipop) ou superior

Para dispositivos Android corporativos.

Nesse tipo de dispositivo, todo o dispositivo pode ser gerenciado, sendo utilizado ou não container corporativo.

- Android 8.0 (Oreo) ou superior
- Dispositivo formatado como Factory Reset

Para os dois modelos, é necessário que a empresa tenha um registro no Android Enterprise Mobility Management (serviço gratuito da Google para EMM).

- Conta Google (qualquer plano)