



O INTERRUPTOR DE SEGURANÇA PARA SUA VIDA DIGITAL

Latch é um produto da ElevenPaths que confere aos serviços online um nível extra de proteção

O Latch diminui a exposição dos seus serviços, permitindo que sejam bloqueados pelos seus clientes quando não estiverem em uso. Desta forma, o tempo de exposição dos serviços às ameaças é reduzido (por exemplo, durante o simples acesso à Web, pagamento com cartão, acesso dos filhos à Internet), para que as consequências de roubo de identidade ou a utilização indevida dos serviços seja minimizada.



Você encontrará mais informações sobre como proteger os seus serviços em latch.elevenpaths.com

Graças ao suporte disponível para a maioria das plataformas e linguagens de programação, utilizando SDKs e plug-ins, a integração do Latch com um serviço online é rápida, simples e totalmente independente de outros mecanismos de autenticação.

Depois de integrado, o Latch possibilita a personalização da proteção do serviço pelo usuário em um aplicativo fácil de usar instalado no dispositivo móvel. Com isso, cada usuário poderá indicar quando o serviço será utilizado. A proteção pode ser controlada e personalizada facilmente pelo usuário, de modo que todas as tentativas não autorizadas de acesso ao serviço serão bloqueadas, emitindo um alerta para que o usuário possa tomar as providências adequadas.

Somente as senhas já não é suficiente



Nem os usuários avançados que obedecem às boas práticas de uso de credenciais estão isentos de ser vítimas de phishing, watering holes e outros ataques. Apesar dos mais variados esforços das empresas para evitar fraudes relacionados com roubo de identidade, todos os anos milhões de usuários e empresas são atacados e comprometidos.

Ninguém usa seus serviços digitais 24 horas por dia, portanto, por que deixá-los disponíveis 24 x 7 tornando-os mais vulneráveis?

Latch é a solução perfeita para bloqueios temporários do serviços, aumentando a segurança sem prejuízo da facilidade de uso. Graças à sua fácil integração, a redução das consequências das ameaças pode ser conferida praticamente na hora.

Entre os casos mais comuns de uso estão:



Proteção de acesso à Web. Proteção ao acesso dos usuário a aplicativos ou a parte das suas operações na Web.



Proteção de acesso corporativo. Proteção do acesso à rede utilizando VPN, Active Directory ou Intranet.



Proteção contra o uso não autorizado de cartões de crédito. Os usuários decidirão quando um cartão estará ativo para fazer pagamentos. Isto impede fraudes em caso de roubo do cartão, clonagem, roubo de dados em operações card-not-present (CNP), etc.



Delegação do controle. O controle de determinados aplicativos pode ser transferido, para autorizar o acesso a dados confidenciais ou criar controle dos pais.

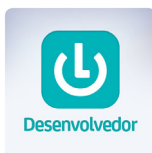


Autorização concorrente de operações. Você pode configurar a execução de uma operação para que ela exija a supervisão de mais de um usuário.



Segundo fator de autenticação. Uma implementação simples permite aumentar o nível de segurança empregando uma administração unificada.

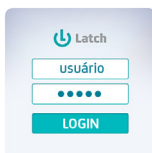
Para implementar a proteção que o Latch proporciona, bastam quatro passos



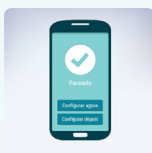
1 A solução deve ser integrada pelo prestador de serviços nos seus sistemas. O Latch fornece vários SDKs e plug-ins que irão facilitar esta tarefa.



3 Depois de parear o serviço com a conta que tem no Latch, o usuário poderá configurar a proteção do serviços diretamente no aplicativo do Latch.



2 O usuário tem que criar uma conta e instalar o aplicativo do Latch no dispositivo móvel. Atualmente, os aplicativos do Latch estão disponíveis para Android, iOS, Windows Phone e FireFox OS.



4 Quando o sistema estiver configurado, o usuário poderá receber notificações em tempo real sobre o uso e o acesso ao serviço.

Todos estes passos foram idealizados para que o nível de privacidade seja o mais alto possível, sem que o Latch obtenha, gerencie ou armazene informações sobre a identidade do usuário, do provedor ou do próprio de serviço.