



ENTRUST



Entrust ajuda a Zerto a estabelecer a integridade de seus programas empresariais

Zerto

Fundada em 2010, a Zerto foi criada com uma visão única de que a tecnologia de recuperação de desastres não deveria ser uma apólice de seguro, mas uma vantagem competitiva.

A Zerto ajuda seus clientes a acelerar a transformação de TI, eliminando o risco e a complexidade da modernização e adoção da nuvem através da resiliência de TI. Ao substituir várias soluções existentes por uma IT Resilience Platform™, a Zerto combina recuperação de desastres, backup e mobilidade na nuvem em uma solução simples e convergente. Com escala empresarial, a plataforma de software da Zerto oferece disponibilidade contínua para uma experiência sempre ativa do cliente, enquanto simplifica a mobilidade da carga de trabalho para proteger, recuperar e mover aplicações livremente através de ambientes híbridos e de multinuvens.

A Zerto transformou os mercados de TI e estendeu os limites de recuperação de desastres. A empresa desenvolveu seu produto inovador de tecnologia de proteção contínua de dados e, em um mundo onde uma tecnologia sem interrupções tem valor imensurável para as empresas, tornou-se muito mais do que apenas uma ferramenta para a recuperação de desastres.

« **Em comparação com outras empresas, a implementação e o suporte da Entrust são muito melhores. Os HSM nShield da Entrust são mais fáceis de usar e fazer backup, e também gostamos da interface gráfica de usuário (GUI).** »

- Nadav Svirsky, chefe corporativo de infraestrutura de TI da Zerto

DESAFIO DO NEGÓCIO

Como fornecedor líder de resiliência de TI, a Zerto precisava da garantia de que seus próprios sistemas comerciais não eram vulneráveis a danos. A estratégia mais eficaz para obter isso foi garantir que sua infraestrutura de chaves públicas (PKI) fosse confiável.

Uma PKI é um conjunto de hardware, software, políticas, processos e procedimentos necessários para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais e chaves públicas. As PKIs ajudam a estabelecer a identidade de pessoas, dispositivos e serviços, permitindo acesso controlado a sistemas e recursos, proteção de dados e responsabilidade por transações. Os aplicativos de negócios da próxima geração estão se tornando mais dependentes da tecnologia PKI para garantir alta segurança, pois os modelos de negócios em evolução estão se tornando mais dependentes da interação eletrônica que exige autenticação online e conformidade com regulamentos de segurança de dados mais rígidos.

Para vincular chaves públicas com o usuário associado a elas (proprietário de chave privada), as PKIs usam certificados digitais. Os certificados digitais são as credenciais que facilitam a verificação de identidades entre os usuários em uma transação. Assim como um passaporte certifica a identidade de uma pessoa como cidadão de um país, o certificado

digital estabelece a identidade dos usuários dentro do ecossistema. Como os certificados digitais são usados para identificar os usuários para os quais os dados são enviados ou para verificar a identidade do signatário das informações, proteger a autenticidade e a integridade do certificado é fundamental para manter a confiabilidade do sistema. Isto foi essencial para o modelo de negócios da Zerto como uma provedora confiável.

DESAFIO TÉCNICO

As autoridades certificadoras (CA) emitem as credenciais digitais utilizadas para certificar a identidade de usuários. As CA são os pilares de segurança de uma PKI e dos serviços que elas suportam e, portanto, podem ser o foco de sofisticados ataques direcionados. A fim de atenuar o risco de ataques contra CA, controles físicos e lógicos, bem como mecanismos de proteção, como módulos de segurança de hardware (HSM), tornaram-se necessários para garantir a integridade de uma PKI.

A Zerto usa uma plataforma da Microsoft e tecnologia da informação aprendida por trabalhar com a Microsoft que tem comprovação de que a melhor forma de proteger suas CA é usar um HSM. Oferecendo um ambiente certificado independentemente e resistente à violação, os HSM são parte integrante da segurança de chaves confidenciais e processos comerciais.

« **A implantação dos HSM nShield da Entrust para proteger nossas CA oferece tranquilidade. Nossa diretoria acha que a redução de risco vale muito o investimento.** »

- Nadav Svirsky, chefe corporativo de infraestrutura de TI da Zerto

SOLUÇÃO

A equipe de TI da Zerto tinha experiência com várias fornecedoras de HSM e escolheu os HSM Solo nShield® da Entrust para sua implantação. De acordo com Nadav Svirsky, chefe corporativo de infraestrutura de TI, a Zerto, escolheu a Entrust em vez de outras fornecedoras porque "Comparada com outras fornecedoras, a implementação e o suporte da Entrust são melhores, os HSMs Solo nShield da Entrust são mais fáceis de usar e de fazer backup, e também gostamos da interface gráfica de usuário (GUI)".

RESULTADOS

A Zerto não compartilha seus resultados quantificáveis da instalação dos HSM nShield da Entrust para proteger suas CA. Em referência a ter agora a melhor prática

de segurança de CA, que era o objetivo inicial do projeto, Svirsky disse: "Nossos clientes precisam estar confiantes de que nossos sistemas são seguros e confiáveis. Infelizmente, geralmente não é possível valorizar a segurança dos dados até que algo dê errado. Quando isso acontece, é possível ver a reputação de uma empresa, as vendas e o preço das ações caírem. Assim, a implementação dos HSM Solo nShield da Entrust para proteger nossas CA nos dá tranquilidade. Nossa diretoria acha que a redução de risco vale muito o investimento".

DESEMPENHO, CONFIABILIDADE E PROTEÇÃO

Necessidade do negócio

- Reduzir o risco de problemas internos de segurança de dados

Necessidades tecnológicas

- Ponto de confiança para servidores de CA a um custo razoável

Solução

- HSM nShield da Entrust

Resultados

- Menos riscos
- Tranquilidade para a diretoria da Zerto

SOBRE A ENTRUST

A Entrust mantém o mundo movendo-se com segurança, permitindo identidades, pagamentos e proteção de dados confiáveis. Hoje, mais do que nunca, as pessoas exigem experiências seguras e contínuas, quer estejam cruzando fronteiras, fazendo uma compra, acessando serviços de governo eletrônico ou entrando em redes corporativas. A Entrust oferece uma gama incomparável de soluções de segurança digital e emissão de credenciais no centro de todas essas interações. Com mais de 2.500 colegas, uma rede de parceiros globais e clientes em mais de 150 países, não é de admirar que as organizações mais confiáveis do mundo confiem em nós.