THALES

451 Research®

2018

RELATÓRIO DA THALES SOBRE AMEAÇAS A DADOS

Tendências em criptografia e segurança de dados

EDIÇÃO GLOBAL

RESUMO EXECUTIVO

#2018DataThreat

EM DESTAQUE

A transformação digital está provocando agitação em massa. Mude a forma como protege seus dados. Ou seja atacado. Novamente.

Atualmente, na sua 6ª edição, o Relatório da Thales sobre ameaças a dados de 2018 quantifica o alcance das violações de dados em empresas médias e grandes no mundo inteiro, identificando os riscos, detalhando os planos de gastos com segurança e oferecendo informação crítica sobre como as organizações podem evitar fazer parte das estatísticas de violações a dados.

Este ano descobrimos que as organizações estão enfrentando mudanças massivas provocadas pela mais recente onda de transformação digital. Como a transformação digital necessariamente leva às organizações para um mundo orientado aos dados, 94% das organizações estão utilizando dados sensíveis na nuvem, big data, IoT, contêineres ou dispositivos móveis, criando assim novas superfícies de ataque e novos riscos para os dados, que devem ser compensados pelos controles de segurança de dados.

A TRANSFORMAÇÃO DIGITAL EXIGE NOVA ABORDAGEM À SEGURANÇA DE DADOS

94% usa tecnologias de transformação digital com seus **dados sensíveis**

Altos níveis de adoção pioram o problema

100% das empresas agora adotaram a nuvem

99% usa Big Data

94% Implementa Internet das coisas (IoT)

91% Trabalha emou utiliza pagamentos móveis

AS ORGANIZAÇÕES DEVEM MUDAR A FORMA COMO PROTEGEM SEUS DADOS

Violados alguma vez

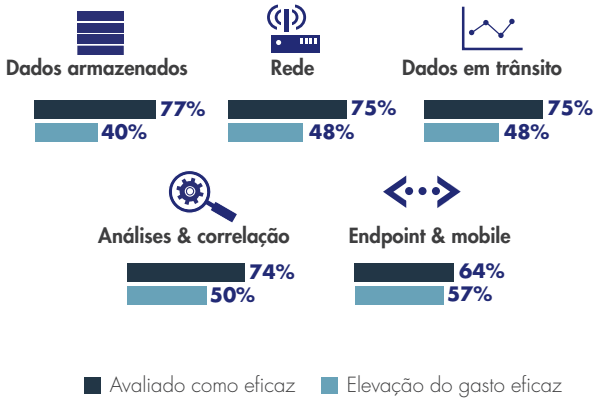
67% das empresas foram violadas alguma vez

Violados no último ano

A cada ano aumenta o número de empresas que enfrentam violações de dados

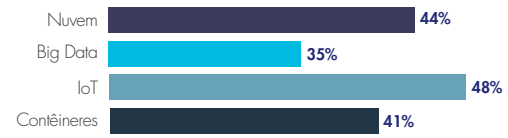
OS TEMPOS MUDARAM; AS ESTRATÉGIAS DE SEGURANÇA, NÃO

Os profissionais em segurança de TI sabem o que funciona para proteger os dados, mas não estão priorizando aumentar o orçamento para segurança dos dados armazenados



A CRIPTOGRAFIA É A SOLUÇÃO CRÍTICA

A criptografia é necessária para estimular o uso de tecnologias digitalmente transformadoras:



As ferramentas de criptografia estão no topo da lista de ferramentas de segurança de dados a serem compradas no próximo ano:

44% Tokenização

43% Criptografia com BYOK

41% Módulo de segurança de hardware para operações de criptografia seguras

OS DADOS SENSÍVEIS AGORA CORREM MAIS RISCO QUE ANTES

A transformação digital está provocando não apenas agitação em massa no setor de TI; mas também exige novos enfoques na segurança de dados.

A transformação digital leva à eficiência e escala dos produtos e serviços existentes, enquanto possibilitam novos modelos de negócios que impulsionam o crescimento e rendimento. As empresas estão aproveitando a oportunidade alavancando todas as ofertas de tecnologia digital, mas podem colocar em risco a segurança de seus dados sensíveis no esforço para se desenvolver.

Descobrimos que a adoção geral de tecnologias como a nuvem, big data, IoT, contêineres, pagamentos móveis e blockchain por parte das empresas atingiu níveis máximos históricos, impulsionando esta transformação. Algumas tecnologias (como big data) atingiram 99% de adoção e 94% planeja utilizar dados sensíveis dentro desses ambientes. A escala de adoção faz com que este problema seja hiper-crítico, pois as organizações estão utilizando muitos fornecedores e ambientes.

O alto índice de uso de tecnologias de transformação digital piora o problema de segurança de dados

94% das empresas usa **dados sensíveis** com ferramentas para a transformação digital.

Os altos níveis de adoção pioram o problema

100%
das empresas agora adotaram a nuvem

99%
usa Big Data

94%
Implementa Internet das coisas (IoT)

91%
Trabalha emou utiliza pagamentos móveis

Os ataques estão superando as defesas das empresas em velocidade recorde.

O alcance e o impacto das crescentes ameaças se evidenciam com mais claridade nos níveis de violações de dados e vulnerabilidade. Os índices de violações de dados têm atingido máximas históricas; 67% das organizações informam que foram atacadas em escala global (e 71% nosEUA). Além disso, os índices de violações de dados foram os mais altos no ano passado: 36% das empresas no mundo inteiro sofreram violação de dados só no ano passado (e quase metade das organizações, 46%, nos EUA). Em consequência, identificamos níveis recordes de vulnerabilidade nas empresas, com 44% globalmente (e 53% nos EUA) se sentindo muito ou extremamente vulneráveis às ameaças contra seus dados.

Violados alguma vez

67%
Das empresas sofreram violação de dados atualmente

Violados no último ano

2018 **2017** **2016**

A cada ano aumenta o número de empresas que sofreram violação de dados

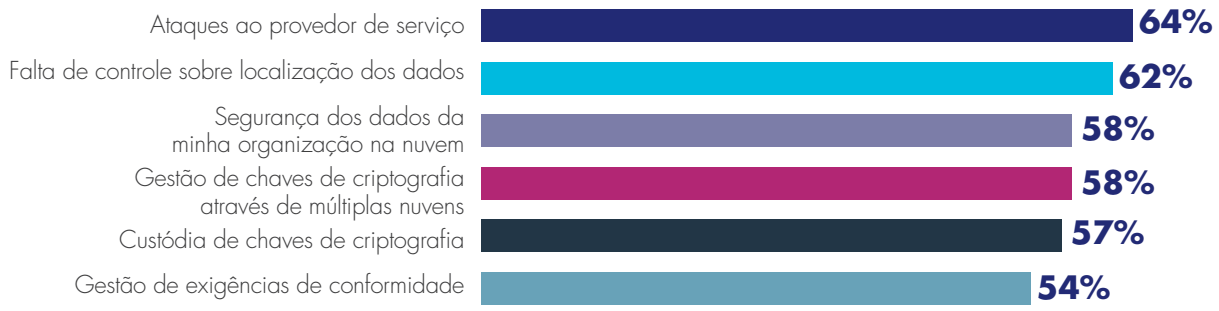
A MIGRAÇÃO PARA A NUVEM EXIGE A SEGURANÇA DE DADOS

A segurança de dados independentemente de onde sejam armazenados vira um problema crítico.

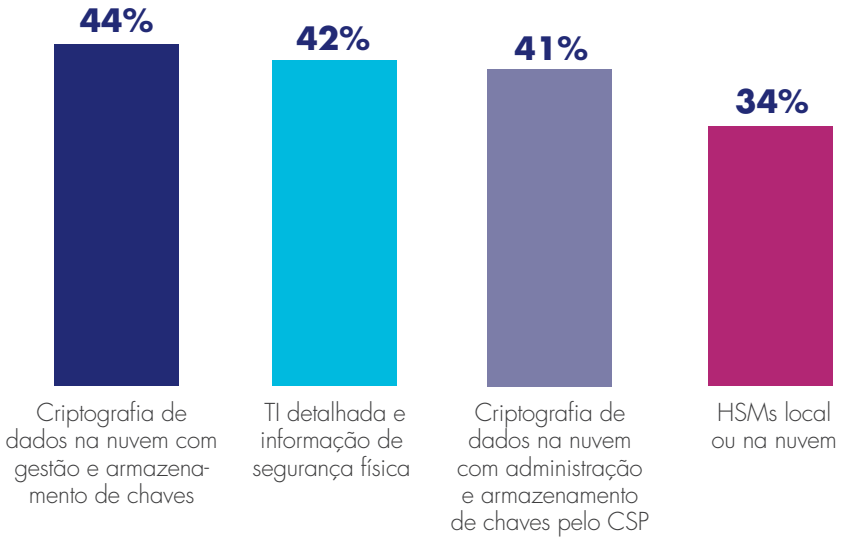
O uso da nuvem é quase universal e continua se expandindo, disparando os índices de adoção pelas empresas. A computação na nuvem (39%) agora visa evitar as punições por violação a dados (39%), seguida de perto por conformidade (37%) como a principal motivação para o gasto com segurança de TI.

A maioria das empresas está desenvolvendo estratégias de múltiplas nuvens, sendo o uso de SaaS especialmente elevado; 42% está usando 50 ou mais aplicativos de SaaS e a maioria das empresas está utilizando dois ou mais distribuidores de IaaS e PaaS. A propagação do uso da nuvem desafia o conceito tradicional do "perímetro" de uma empresa, já que a infraestrutura e o software subjacente não estão mais sob controle da empresa. O resultado é que a segurança dos dados se torna uma tecnologia essencial,dado que seu uso com soluções de criptografia na nuvem permite o máximo controle de segurança necessário (44%). A proliferação de distribuidores provoca então outro problema: a gestão, manutenção e armazenamento de chaves de criptografia para que todos esses ambientes conservem o controle dos dados. A gestão de BYOK através de múltiplas nuvens e contra um progressivo número de exigências de conformidade impõe a necessidade de soluções para as empresas gerirem de forma segura as chaves de criptografia e o acesso aos dados, e sem gastos adicionais inadmissíveis.

Principais preocupações com segurança na nuvem
(índice de muita/extrema preocupação)



Criptografia, o controle número 1 de segurança de TI necessário para ampliar a adoção da nuvem



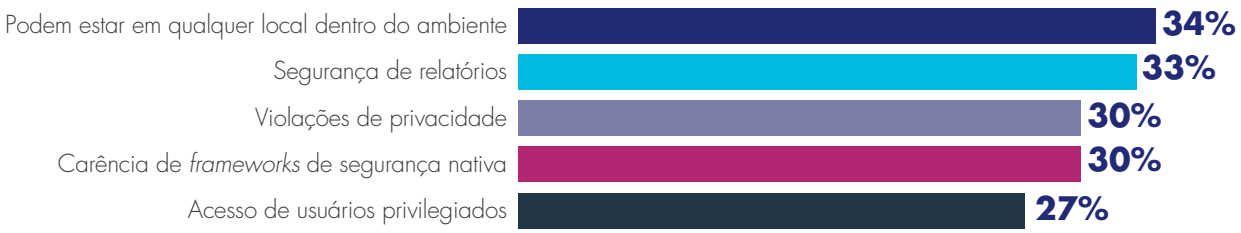
BIG DATA ESTÁ SENDO UTILIZADO PELO MUNDO INTEIRO; PRECISA-SE PROTEÇÃO DE DADOS SENSÍVEIS

Big Data é um gigante mundial: 99% das empresas agora utilizam big data (e 45% usando big data com informação sensível), estes ambientes estão cada vez mais em risco de não-conformidade, regulamentação de privacidade e violações de dados. A natureza complexa e de mudanças rápidas desses ambientes leva à possibilidade de os dados sensíveis estarem localizados em qualquer parte da estrutura, complica o problema e traz o risco de acessos indevidos. Um problema adicional é que frequentemente o big data é implementado em ambientes de nuvem, agravando a percepção de risco das empresas com o fato de que a infraestrutura e a localização de dados já não estão sob o controle da mesma.

99% das empresas agora usam big data

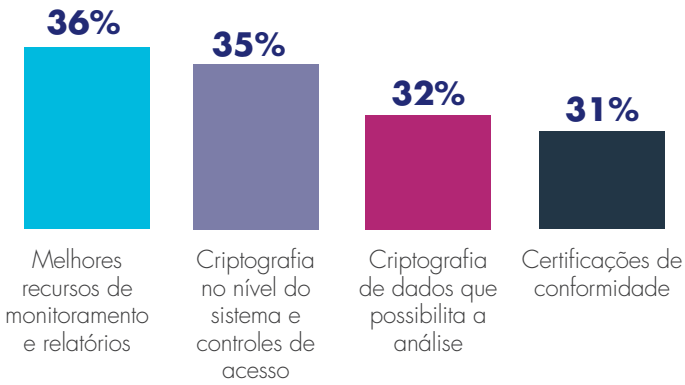
45% está usando dados sensíveis dentro de seus ambientes big data

Principais preocupações em relação a dados sensíveis dentro de ambientes big data



O que é necessário para acelerar a adoção de Big

38%
Autenticação mais forte dos usuários



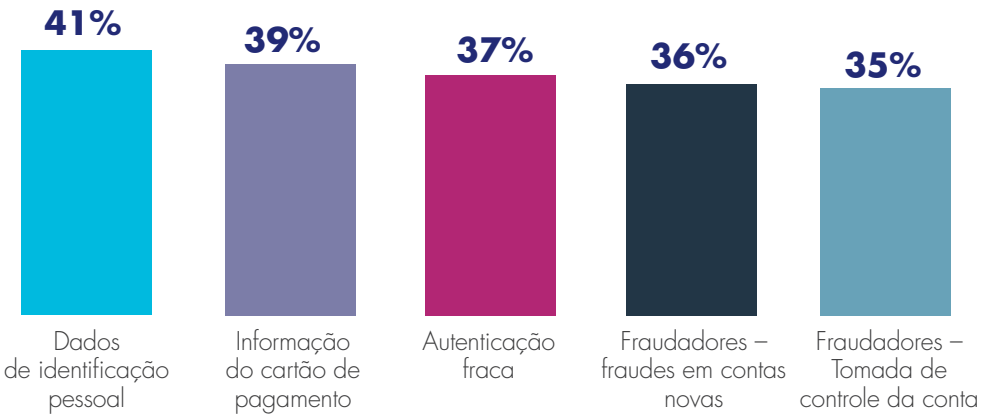
PAGAMENTOS MÓVEIS AUMENTAM; CRIPTOGRAFIA É NECESSÁRIA

Os aplicativos de pagamentos móveis estão ganhando ampla aceitação. 91% das empresas entrevistadas este ano estão desenvolvendo um aplicativo de pagamento móvel ou já implementaram. Porém, ao mesmo tampo, são muitas as preocupações pelas vulnerabilidades dentro do ecossistema de pagamentos móveis. Os pagamentos móveis possuem uma necessidade inerente de segurança de dados em todas as fases de uso, devido à perda potencial de informação pessoal e financeira inerente a seu uso. Portanto, a criptografia torna-se uma tecnologia chave necessária para garantir todo o ambiente de pagamentos móveis, bem como para cumprir as cada vez maiores regulamentações e normas da indústria.

91%
Usa ou tem planos de usar pagamentos móveis

37%
Usa atualmente dados sensíveis com aplicativos móveis

Principais preocupações com pagamentos móveis



Criptografia, ferramenta chave que possibilita o uso seguro de pagamentos móveis

- A criptografia estabelece identidade segura com certidões de nascimento digitais para os dispositivos
- A criptografia protege os dados em trânsito
- A criptografia protege os dados no dispositivo
- A criptografia e os controles de acesso auxiliam as organizações a satisfazer os requisitos de conformidade para o armazenamento de dados

"As violações bem-sucedidas atingiram máximas históricas tanto em empresas médias quanto nas grandes corporações, com mais de dois terços (67%) das organizações no mundo inteiro e quase três quartos (71%) nos EUA tendo sofrido violações em algum momento no passado. Além disso, quase metade (46%) dos entrevistados nos EUA reportaram alguma violação durante os 12 meses anteriores, o que equivale a quase o dobro dos 24% que apresentaram esta resposta no ano passado; por sua vez, mais de um terço (36%) dos entrevistados no mundo inteiro tiveram um destino parecido".

"Obviamente, fazer o que temos feito durante décadas já não está funcionando. A pergunta mais importante na mente dos líderes de TI e de negócios é mais direta: "o que fazer para parar as violações a dados?."

—Garrett Bekker, 451 Research, Analista Principal, Segurança da Informação
Autor do Relatório da Thales sobre ameaças a dados de 2018

A CRIPTOGRAFIA É A SOLUÇÃO

As tecnologias de criptografia são fundamentais para proteger os dados armazenados, em trânsito e em uso. A criptografia garante a segurança dos dados para satisfazer os requisitos de conformidade, as melhores práticas e as regulamentações de privacidade. É o único conjunto de ferramentas que garante a segurança e o controle dos dados não apenas nos data centers tradicionais, mas também com as tecnologias empregadas para impulsionar a transformação digital da empresa.

SOBRE A THALES

A Thales eSecurity é líder em soluções avançadas de segurança de dados e serviços que oferecem confiança quando a informação é criada, compartilhada ou armazenada. Garantimos que os dados de companhias e entidades governamentais estejam seguros e sejam confiáveis em qualquer ambiente: nas instalações locais, na nuvem, data centers ou ambientes big data, sem sacrificar a agilidade no negócio. A segurança não reduz somente o risco; também possibilita as iniciativas digitais que agora fazem parte da nossa vida quotidiana: dinheiro digital, identidades eletrônicas, atendimento médico, automóveis conectados e com a Internet das cosas (IoT), até os eletrodomésticos. A Thales oferece tudo o que uma organização precisa para proteger e gerir seus dados, identidades e propriedade intelectual e atingir o cumprimento das regulamentações, através da criptografia, gestão avançada de chaves, tokenização, controle de usuários privilegiados e soluções de alta segurança. Os profissionais em segurança no mundo inteiro confiam na Thales para acelerar a transformação digital da sua empresa. A Thales eSecurity faz parte da Thales Group.

CLIQUE AQUI SE QUISER LER O RELATÓRIO COMPLETO

THALES

www.thalesesecurity.com