

5 razões pelas quais você não pode impedir o ataque de ransomware



Contents

5

Compensa financeiramente

4

É barato

3

É fácil

2

Tem um ROI rápido

1

As pessoas não são confiáveis



Proteção contra ransomware de confiança zero

Dado o número de ataques de ransomware de alto escalão ao longo dos anos e as graves consequências de uma infecção, você pode pensar que os métodos de prevenção devem estar amadurecendo a ponto de que o ransomware venha ser totalmente eliminado em breve. Considere a ameaça onipresente dos kits de exploração, como o infame Angler, uma enorme dor de cabeça para qualquer equipe de segurança na época. Esses kits de exploração praticamente desapareceram da memória, graças ao esforço incansável dos pesquisadores para reprimi-los. Mas o ransomware ainda está em toda parte, e a prevenção total dessa ameaça é efetivamente impossível. Vamos contar as razões pelas quais podemos afirmar isso.

5

Compensa financeiramente

Os invasores estão mais motivados do que nunca, porque os ataques bem-sucedidos oferecem grandes recompensas. Em 2019, as demandas de resgate cresceram 184% do primeiro ao segundo trimestre, e especialistas estimam que o custo médio por incidente em 2020 foi de US\$ 283.800. Desde 2018, os incidentes relacionados a ransomware aumentaram 41%, com o custo total para as empresas em 2019 atingindo US\$ 170 bilhões, segundo algumas estimativas. Se essas tendências continuarem, o ataque de março de 2019 à Norsk Hydro, que custou à empresa pelo menos US\$ 40 milhões, pode se tornar comum. Com números como esses, é fácil ver por que o ransomware continua sendo um dos empreendimentos favoritos entre os cibercriminosos. E mesmo que as agências de aplicação da lei desaconselhem isso, as empresas continuam pagando o resgate. Afinal, é natural que elas queiram proteger os seus dados. Além disso, o custo da interrupção dos negócios geralmente eclipsa o próprio valor do resgate, o que significa que pagar é geralmente a opção mais econômica.

4

É barato

Por outro lado, os custos desembolsados para executar uma campanha de ransomware são baixos. Atualmente, um invasor pode comprar um kit de ransomware pré-fabricado por uma quantia relativamente insignificante. O kit contém tudo o que é necessário para implementar e monetizar um ataque, incluindo serviços de criptografia, dropper de carga útil e ferramentas de ofuscação. Uma assinatura típica de ransomware como serviço (RaaS) começa em pouco mais de US\$ 100 por mês. Variantes mais complexas e poderosas podem custar milhares de dólares, mas o potencial de retorno também aumenta. Planos de suporte também estão incluídos para garantir que os invasores possam extrair o máximo valor do serviço.

3

É fácil

Um dos primeiros exemplos de RaaS foi o GandCrab, que em seu auge em 2018 foi responsável por mais da metade de todas as infecções de ransomware em todo o mundo. Ao longo de sua ilustre execução, o GandCrab gerou mais de US\$ 2 bilhões em lucro, com US\$ 150 milhões indo direto para os criadores e o restante distribuído entre os seus muitos afiliados.

Alguns cibercriminosos vão ainda mais longe, e têm programas de afiliados altamente desenvolvidos, que examinam os candidatos quanto à compatibilidade. O ransomware REvil/Sodinokibi, atualmente em disseminação, foi detectado pela primeira vez em meados de 2019 e rapidamente ganhou destaque graças ao seu programa de afiliados. Por meio dele, os criadores permitem que apenas certos grupos de alto rendimento usem o seu programa RaaS. Esqueça o estereótipo de malfeitores de capuz em quartos escuros; esta é uma rede sofisticada, comparável a qualquer programa de parceria corporativo.

2

Tem um ROI rápido

Outra razão pela qual o ransomware é tão atraente é que, uma vez que entra em um sistema, normalmente por meio de anexos de e-mail, URLs maliciosos, protocolos de área de trabalho remotos inseguros ou malvertising, ele se move rapidamente. O cibercriminoso verifica a rede para localizar arquivos, depois criptografa o conteúdo e exige um resgate. Infelizmente, uma vez iniciado o processo de criptografia, não há muito o que fazer para desfazê-lo. Além disso, uma tendência alarmante é que surgiu uma nova metodologia pela qual os invasores roubam dados antes de criptografá-los. Em abril de 2020, Cognizant, o gigante de computadores da Fortune 500, foi atingido por um ataque de ransomware Maze. Esse ransomware, que está circulando desde meados de 2019, primeiro rouba dados, e depois ameaça as vítimas de que essas informações serão divulgadas publicamente, se o resgate não for pago. Essa estratégia elimina qualquer intenção de evitar o pagamento por meio de um forte plano de recuperação de desastres. Portanto, dificilmente é um choque que os invasores continuem perseguindo esse vetor. Afinal, ele é lucrativo e fácil de conseguir, e as pessoas continuam pagando.

1

As pessoas não são confiáveis

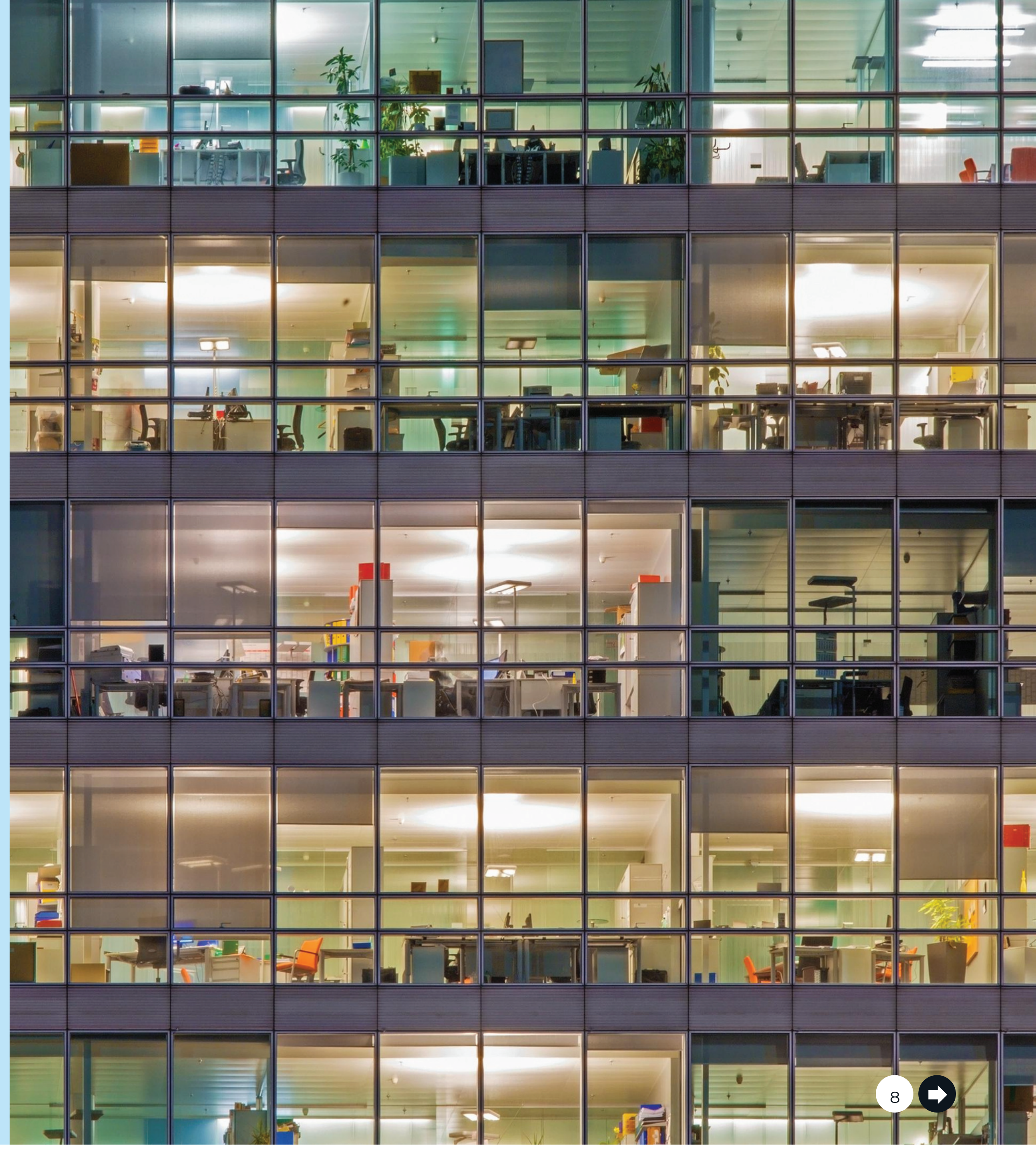
Até agora, abordamos por que o ransomware é tão onipresente, mas não dissemos nada sobre como pará-lo. Embora seja verdade que um grande número de ataques poderia ser evitado com uma melhor higiene dos patches, há uma razão acima de todas para que a prevenção total seja impossível: as pessoas. Você confia que os seus funcionários nunca prejudicariam intencionalmente a sua empresa. Mas as infecções por ransomware ainda acontecem porque os funcionários não estão sempre alertas para os perigos de links e e-mails maliciosos ou tentativas de phishing.

Tenho certeza de que muitos leitores estão familiarizados com o treinamento regular obrigatório baseado na conscientização de segurança. O treinamento certamente não faz mal, mas mesmo seus funcionários mais conscientes sobre a segurança podem ter um lapso momentâneo de julgamento ao clicar em um link ou abrir um e-mail. E sem políticas de segurança super restritivas que atrapalhem o trabalho das pessoas, basta esse lapso de julgamento.

Proteção contra ransomware de confiança zero

Se você não pode impedir o ransomware, o que pode fazer para se proteger? Os seus funcionários precisam de acesso a dados para fazer o seu trabalho. Do mesmo modo, o ransomware precisa de acesso para que os seus funcionários se tornem o vetor de ataque.

As políticas e funções que restringem o acesso aos dados podem ajudar, mas muitas delas podem atrapalhar a produtividade. A resposta é detecção precoce, análise do comportamento do usuário e ação automatizada quando ocorrem padrões suspeitos. Em segundos.



O NetApp® Cloud Insights oferece exatamente esse tipo de detecção com um recurso chamado Cloud Secure. Com o Cloud Secure, você pode monitorar atividades, detectar anomalias e automatizar respostas.

• **Monitorar a atividade do usuário**

Para identificar as violações com precisão, todas as atividades do usuário em ambientes locais e de nuvem híbrida são capturadas e analisadas. Os dados são coletados usando um agente coletor de dados leve e stateless instalado em uma VM no ambiente do cliente. Esses dados também incluem dados de usuários de servidores Active Directory e LDAP e atividades de arquivos de usuários do NetApp ONTAP® e do Cloud Volumes ONTAP.

O Cloud Secure detecta anomalias no comportamento do usuário criando um modelo comportamental para cada usuário. A partir desse modelo comportamental, ele detecta alterações anormais na atividade do usuário e analisa esses padrões de comportamento para determinar se a ameaça é ransomware ou um usuário mal-intencionado. Esse modelo comportamental reduz o ruído causado pelo falso positivo.

• **Detectar anomalias e identificar possíveis ataques**

O ransomware e o malware de hoje são sofisticados, usando extensões e nomes de arquivo aleatórios, o que torna ineficaz a detecção por soluções baseadas em assinatura (lista de bloqueios). O Cloud Secure usa algoritmos avançados de aprendizado de máquina para descobrir atividades de dados incomuns e detectar um possível ataque. Essa abordagem fornece detecção dinâmica e precisa e reduz o ruído de detecção falsa.

• **Automatize políticas de resposta**

O Cloud Secure alerta você e tira automaticamente um snapshot (cópia instantânea) dos seus dados quando detecta um comportamento arriscado, garantindo que essas informações sejam armazenadas em backup para que você possa recuperá-las rapidamente.

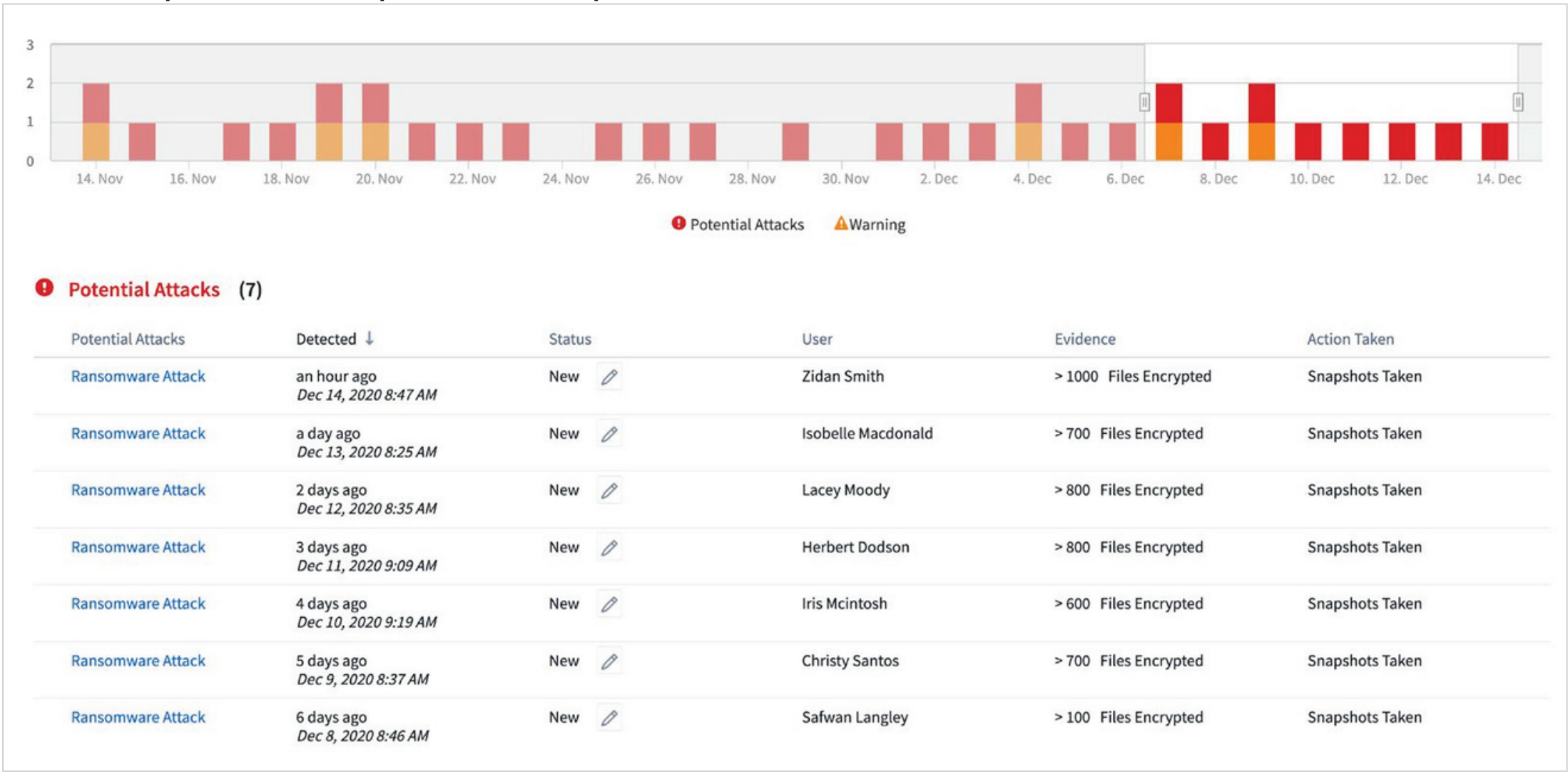


Figure 1) Cloud secure dashboard showing user activity.



Se você estiver interessado em saber mais sobre o Cloud Secure, inscreva-se em nosso teste gratuito de 30 dias.
Saiba mais e comece a sua avaliação gratuita.



Sobre a NetApp

Em um mundo cheio de generalistas, a NetApp é especialista. Estamos focados em uma coisa, ajudar a sua empresa a aproveitar ao máximo os seus dados. A NetApp traz para a nuvem os serviços de dados de nível empresarial que você confia e leva a flexibilidade simples da nuvem para o data center. Nossas soluções líderes do setor funcionam em diversos ambientes de clientes e nas maiores nuvens públicas do mundo.

Como uma empresa de software centrada em dados e liderada pela nuvem, somente a NetApp pode ajudar a construir a sua malha de dados exclusiva, simplificar e conectar a sua nuvem e fornecer com segurança os dados, serviços e aplicativos certos para as pessoas certas – a qualquer hora, em qualquer lugar.

