VERITAS

Detecção de anomalias para dados da nuvem

Uma ferramenta poderosa para monitorar seus dados da nuvem e a atividade do usuário.

A detecção de anomalias é um poderoso sistema de alertas preventivos que rastreia e alerta sobre atividades fora do comum ou comportamentos estranhos de seus dados da nuvem e atividades do usuário. Essencialmente, ele ajuda a ver os problemas antes que eles ocorram. Detectar essas anomalias agora é uma prática crítica para a segurança dos dados, pois as anomalias podem ser indicadores de uma quebra da segurança, um problema de hardware ou software, mudanças nas demandas dos clientes ou qualquer número de desafios que exijam atenção imediata. Ele funciona usando um processo de localização de pontos ou padrões incomuns em um conjunto de dados. Qualquer coisa que se desvie de uma linha de base estabelecida (dentro de uma tolerância predefinida) é considerada uma anomalia. Com um conjunto de parâmetros estabelecidos e indicadores inteligentes, os clientes são alertados sobre anomalias que requerem atenção imediata e podem facilmente visualizar um painel atualizado em tempo real com monitoramento de atividades. Exemplos de anomalias incluem atividade incomum de gravação de arquivo que pode indicar infiltração — mas também pode estar detectando extensões de arquivo ransomware conhecidas —, padrões de acesso a arquivos, caminhos de tráfego ou até mesmo um salto incomum na atividade em comparação com padrões típicos. Ser notificado imediatamente sobre qualquer coisa fora do comum oferece uma vantagem valiosa para agir ou mitigar rapidamente. É muito valioso ser capaz de ficar por dentro de qualquer problema que surja ou mitigar um risco e isolá-lo rapidamente para evitar qualquer coisa destrutiva, tempo de inatividade ou outros problemas relacionados a uma violação.

O poder de uma torre de vigia de dados

Com os dados da nuvem explodindo em tamanho e expansão, há uma necessidade crescente de detecção de anomalias, para servir como uma torre de vigia sobre todos os seus dados da nuvem, especialmente em face de ameaças cibernéticas e de ransomware. Historicamente, os criminosos cibernéticos têm obtido acesso a sistemas e dados em uma variedade de caminhos criativos. Eles entram em um sistema, começam a criptografar e baixam o máximo que podem, escapando antes de serem detectados. Nesse cenário, a detecção de anomalias alertaria sobre o problema e ajudaria você a agir.

A nuvem é o vetor de ataque de ransomware número um para criminosos cibernéticos em 2022[1], e agora os criminosos cibernéticos costumam usar estratégias a longo prazo, tirando algumas jogadas do manual do crime organizado. Eles aperfeiçoaram a arte do reconhecimento cibernético. Uma prática frequentemente chamada de ransomware inativo ou ransomware adormecido agora ocorre regularmente no mundo digital. Ou seja, uma vez obtido o acesso, os criminosos ficarão estrategicamente escondidos. Por que? A principal prioridade deles é observar, aprender e mover-se em seus ambientes de nuvem, tentando encontrar seus pontos fracos e explorar suas vulnerabilidades — tudo isso enquanto aguardam o momento ideal para atacar. Nessa situação, detectá-los antes que tenham a chance de agir oferece uma oportunidade poderosa de descobrir problemas antes que ocorram e de agir para evitar um impacto devastador.

Os malfeitores são altamente motivados a causar o máximo de destruição possível para ganhar mais dinheiro e maximizar seus esforços — assim como em qualquer negócio, tudo gira em torno do ROI. Alguns relatórios sugerem que o ransomware pode ficar inativo por até 18 meses. Os malfeitores sabem que a destruição ideal depende de vários fatores, como tempo e escopo. Eles querem que você não tenha escolha a não ser pagar o resgate. Passou-se a época em que violações e ataques aconteciam ao mesmo tempo. Essa complexidade adicional significa que eles geralmente podem conhecer seus sistemas melhor do que você, portanto, a chance de eles lançarem uma série de eventos projetados para interromper e desabilitar sistemas críticos para obter pagamentos maiores está aumentando drasticamente.

Visibilidade de dados entre nuvens

Antes que uma organização possa implementar a detecção bem-sucedida de anomalias, é importante dar um passo para trás para garantir que você saiba onde todos os seus dados residem e se certificar de que não haja dados obscuros ocultos em seu ambiente. De acordo com a Veritas Vulnerability Lag Research[2], 35% dos dados ainda estão obscuros. Isso é assustadoramente alto. Recomendamos que você comece a descobrir quais dados você tem e onde eles estão — imediatamente.

As soluções da Veritas fornecem uma visão abrangente de todos os seus dados em todos os seus provedores de nuvem, ambientes físicos e virtuais. Você também pode visualizar seu armazenamento, sua capacidade de computação, todas as principais soluções de proteção de dados e geração de relatórios cruzados, o que garante que nenhum sistema falhe. Isso é especialmente crucial no cenário de ameaças atual, pois os criminosos cibernéticos não esperam que você esteja mantendo um inventário preciso de todos os seus aplicativos e dados, ou que possa haver áreas em que você tenha segurança e/ou supervisão de dados limitada.

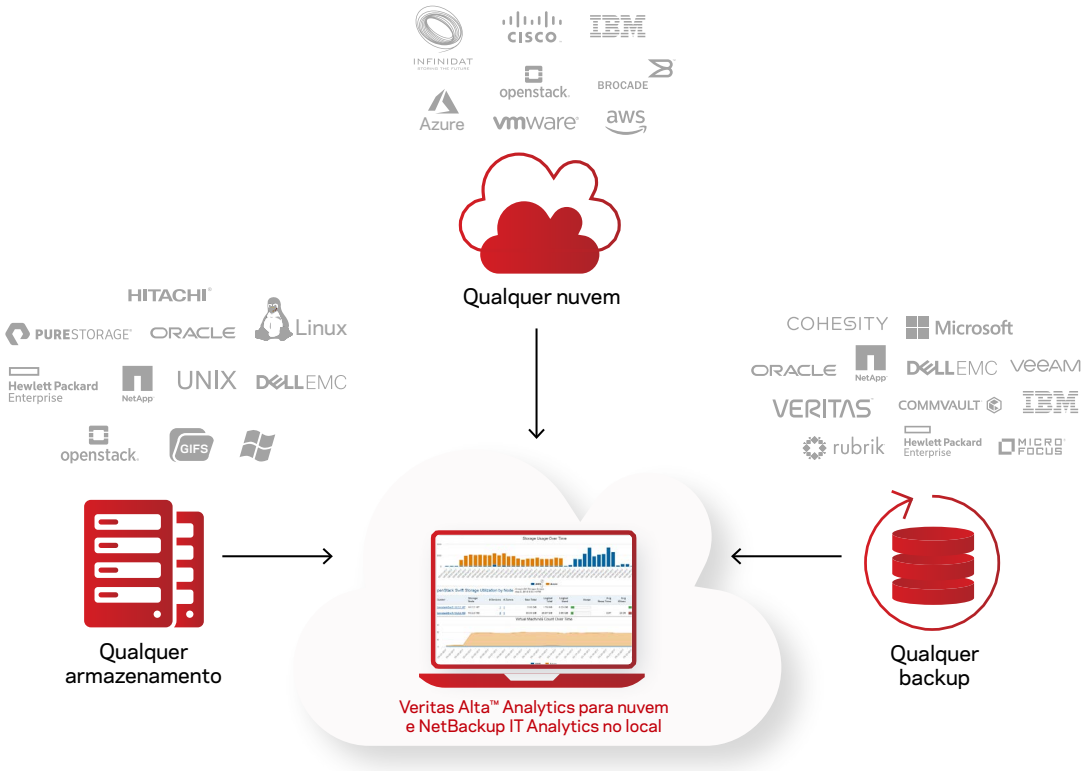

Figura 1: infraestrutura de TI unificada em todos os seus dados, independentemente de onde estejam

Além de iluminar as áreas escuras do seu ambiente, as soluções da Veritas fornecem insights abrangentes, alertas e relatórios no local, nuvem, proteção de dados e armazenamento. Você terá os insights necessários para tomar decisões informadas diante de um ataque cibernético com opções de geração de relatórios que ajudam a obter visibilidade em seu ambiente de backup, permitindo que sua organização:

- Descubra todos os hosts ou máquinas virtuais (VMs) em sua infraestrutura e compare-os com as VMs protegidas pelo Veritas Alta™ Data Protection para nuvem e NetBackup no local.
- Sinalize os hosts que estão faltando nos backups ou não têm backups recentes, como riscos potenciais.
- Detecte os possíveis arquivos afetados por ransomware, juntamente com seu tamanho e onde eles residem no ambiente.
- Acesse gráficos interativos que fornecem um histórico dos riscos gerados.

Detecção de anomalias alimentadas por IA entre nuvens

Depois que a visibilidade dos dados estiver em vigor, a próxima etapa é implementar a detecção de anomalias com tecnologia de IA. O Veritas Alta™ Data Protection para nuvem e o NetBackup no local detectam dados anômalos e atividades do usuário em todo o ambiente e alertam sobre anomalias suspeitas quase em tempo real. A tecnologia foi projetada para extrair uma enorme quantidade de dados, automatizar o monitoramento e a geração de relatórios e fornecer insights acionáveis sobre o que está acontecendo em seu ambiente.

Uma ótima maneira de visualizar a detecção de anomalias é imaginar um teste de polígrafo. Quando você faz um teste de polígrafo, o examinador começa com uma pré-triagem, onde faz uma série de perguntas para estabelecer parâmetros que serão considerados normais como linha de base. Quando você mente, os indicadores fisiológicos de **pressão arterial, pulso, respiração e condutividade da pele** flutuam, como esperado, fora dos parâmetros normais estabelecidos. Da mesma forma, o Veritas Alta™ Data Protection para nuvem e o NetBackup no local usarão um mecanismo de detecção com inteligência artificial para calcular os parâmetros do que é considerado normal com base nos padrões de metadados da tarefa de backup ao longo do tempo e fazer ajustes automáticos para políticas de backup personalizadas.

Os eventos que ocorrem fora do normal estabelecido são capturados e as notificações acontecem quase em tempo real. As anomalias observadas recebem uma pontuação com base na gravidade, que é calculada com base na distância observada do cluster. Quanto maior a distância, mais grave a pontuação. Isso foi projetado para ajudar os administradores a identificar quais insights são acionáveis e para reduzir falsos positivos.

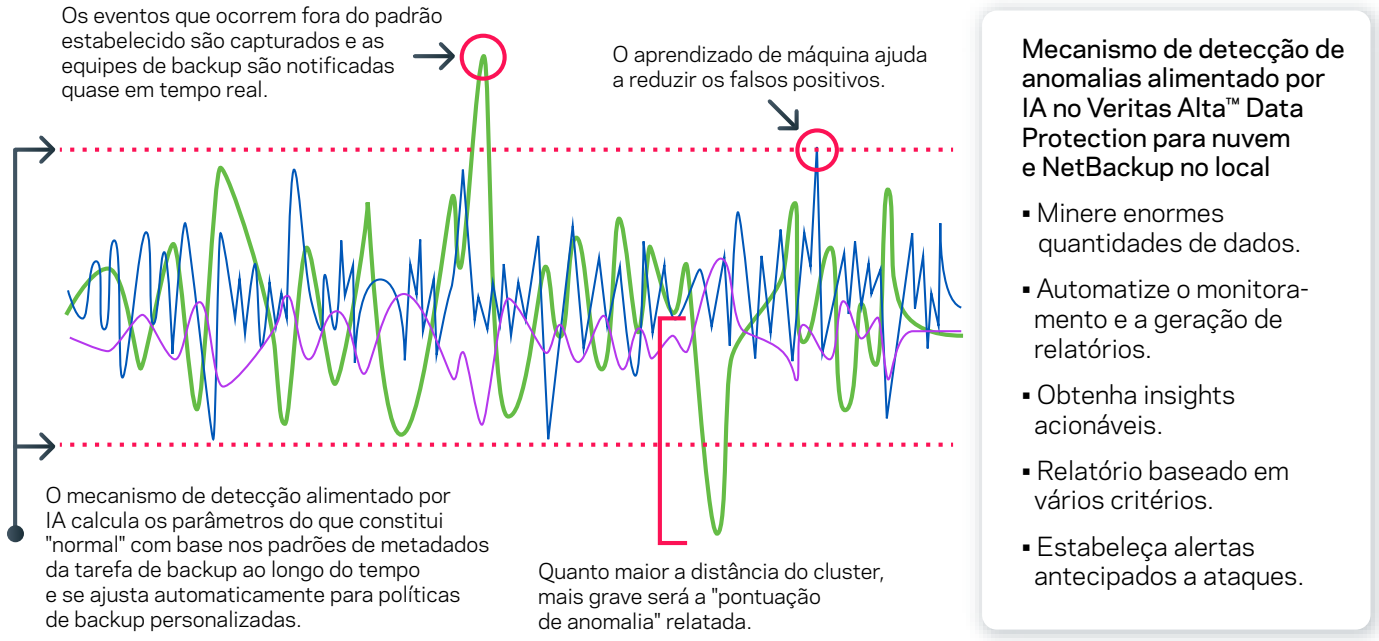

Figura 2: entendendo a detecção de anomalias

No geral, o mecanismo de detecção de anomalias alimentado por IA ajuda você a extrair enormes quantidades de dados, automatizar o monitoramento e a geração de relatórios, obter insights acionáveis, relatar com base em vários critérios e, mais importante, estabelecer um aviso antecipado de um ataque. Os administradores têm a capacidade de visualizar os dados e fornecer recomendações associadas a anomalias a qualquer momento, monitorando todos os dispositivos e estabelecendo um aviso antecipado sobre ataques para ficar por dentro dos problemas à medida que surgem. Por exemplo, a detecção de anomalias baseada em IA da Veritas integra-se perfeitamente ao servidor principal, permitindo que ele detecte formas anômalas de observações, considerando aquelas que não se enquadram no cluster como anomalias ou valores discrepantes. Esse recurso permite que um administrador veja anomalias e faça uma busca detalhada para identificar qualquer problema. Ele oferece a capacidade de extrair grandes quantidades de dados e de fornecer inteligência acionável para lidar com eventos de ransomware, bem como mudanças simples no ambiente das quais um administrador deve estar ciente. Essas soluções podem ajudar a reconhecer indicadores de que um ataque está em andamento ou prestes a começar, permitindo que você tome medidas imediatas e limite o impacto.

A ferramenta também é inteligente, com a capacidade de identificar possíveis falsos positivos comparando backups históricos com o novo backup e identificando anomalias como alterações significativas nas durações do trabalho, variações no tamanho da imagem e/ou alterações na configuração da política. O mecanismo de IA monitora arquivos ou grupos de arquivos e entende quando os seus caracteres estão mudando (até o nível de metadados), independentemente de estarem em disco de bloco ou se usarem armazenamento de objeto na nuvem — tudo isso sem pós-processamento. Somente a Veritas verifica e monitora todos os sistemas, é independente e pode cobrir todas as plataformas de nuvem, incluindo produtos de backup de terceiros. Nosso mecanismo de inteligência artificial/aprendizado de máquina (AI/ML) pode ser executado em qualquer servidor. Este nível de cobertura garante a eliminação de pontos cegos.

Verificação de malware

A Veritas pode ajudar você a detectar vários tipos de malware, como criptografia e exfiltração, fornecendo verificações automatizadas e sob demanda. O recurso automatizado de verificação de malware removerá as dependências humanas e permitirá que a tecnologia AI/ML entre em ação e escaneie em busca de malwares. O escaneamento de malware AI/ML é acionado automaticamente como consequência de uma pontuação alta de anomalia. O escaneamento inclui dados não estruturados, Windows, Linux e VMware. Essa inclusão é vital porque o malware geralmente entra em seu ambiente em um diretório inicial, pois costumam ser locais com grandes conjuntos de dados não estruturados.

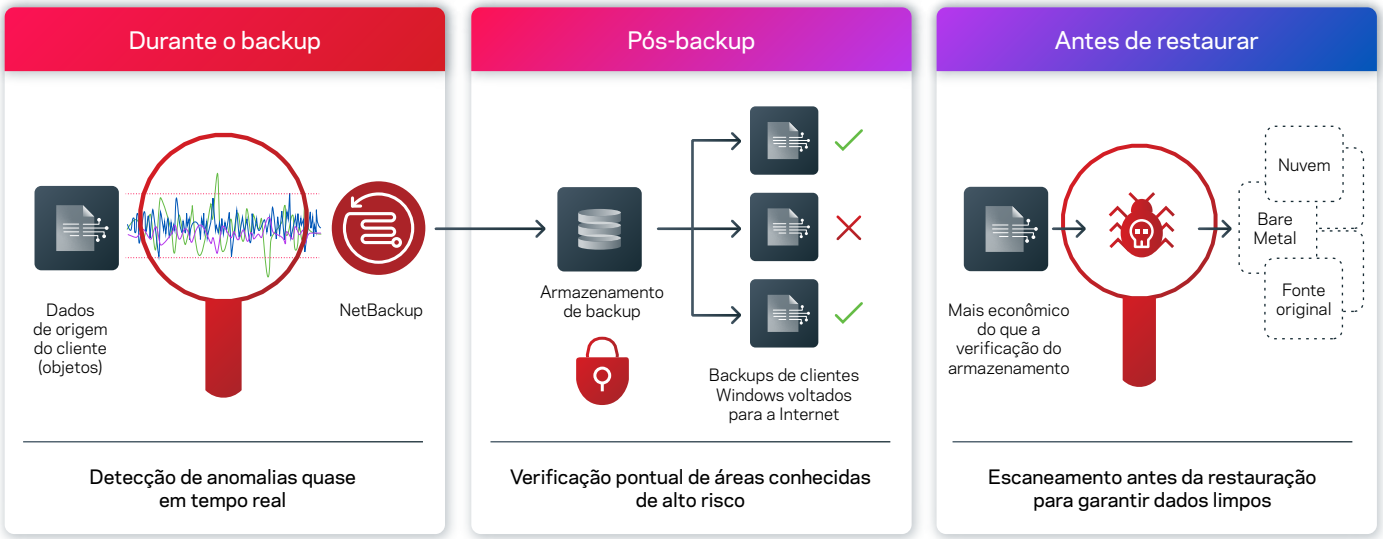

Figura 3: visão geral do escaneamento de malware

Além disso, quando a recuperação é necessária, os dados de backup podem ser verificados, garantindo que as assinaturas de malware mais recentes sejam aproveitadas. Visuais claros e prompts de aviso permitem que você identifique backups infectados, garantindo que todos os dados restaurados estejam limpos e sem impacto. Essa prática costuma ser chamada de restauração para a última cópia válida.

A Veritas é segura desde a concepção

A Veritas oferece toda essa visibilidade unificada de dados, detecção de anomalias e escaneamento de malware por meio do Veritas Alta™ Analytics para nuvem e NetBackup IT Analytics no local. A seguir, você pode ver um exemplo de painel.

Figura 4: um exemplo de painel do NetBackup IT Analytics mostrando o uso do armazenamento ao longo do tempo

Atributos do Veritas Analytics:

- **Abrangente** — uma solução única de um console integrado para identificar ativos de dados, o Veritas Alta™ Analytics para nuvem e o NetBackup IT Analytics no local fornecem suporte para todos os servidores, armazenamentos, hipervisores, bancos de dados e plataformas de aplicativos populares usados pelas empresas atualmente.
- **Escalável** — o gerenciamento centralizado fornece um coletor de dados sem agente reunindo aproximadamente 30 mil pontos de dados exclusivos de todos os aspectos de ambientes locais e na nuvem, incluindo aplicativos, nuvem, proteção de dados, hosts, rede, armazenamento, virtualização e dados não estruturados.
- **Inovador** — algoritmos proprietários — orientados por cinco patentes para design autônomo e atualizações da nuvem — analisam pontos de dados e fazem recomendações que melhoram o desempenho, a resiliência e a utilização. A análise é conduzida por máquina, mas governada por políticas humanas, com dados usados para apresentar soluções acionáveis para ajudar a melhorar as medidas de eficiência e minimizar riscos, prever falhas e simplificar auditorias e a conformidade.
- **Comprovado** — por mais de uma década, o NetBackup IT Analytics, agora incluindo o Veritas Alta™ Analytics para nuvem, liderou o setor com escalabilidade e confiabilidade comprovadas pelos clientes, reunindo e analisando dados de toda a organização.

Principais recursos do Veritas Analytics:

- Um console integrado que fornece informações sobre:
  - backup, computação e armazenamento local e em nuvem;
  - capacidade, custo e uso no local e na nuvem.
- Chargeback:
  - por qualquer grupo definido pelo usuário, como aplicativo, departamento e centro de custo;
  - uso em backup e nuvem, computação e armazenamento.
- Planejamento de capacidade:
  - orçamento baseado em custos de nuvem e taxas de uso;
  - planejamento de mídia/armazenamento com base no uso de consumo.

Maximize o valor comercial da nuvem com o Veritas Alta™ Analytics para nuvem e NetBackup IT Analytics no local

Na Veritas, descobrimos que as organizações estão migrando para a nuvem por vários motivos: organizações menores se beneficiam com a redução do esforço de manter um data center e/ou local de recuperação após desastres; organizações de médio porte apreciam o armazenamento externo de dados acessível, construído em hardware, e que é altamente escalonável, aproveitando a recuperação em nuvem just-in-time. Grandes organizações estão identificando cargas de trabalho capazes de aproveitar a disponibilidade e o custo da nuvem, ao mesmo tempo em que liberam espaço caro no data center para cargas de trabalho críticas ao seu funcionamento. Às vezes, uma organização requer espaço temporário para uma carga de trabalho. Em vez de inserir um novo rack de discos em um data center, ela pode aproveitar o espaço em um provedor de nuvem para evitar o custo adicional de adquirir hardware de data center. Os modelos de assinatura em nuvem funcionam bem para esses projetos, oferecendo modelos escalonáveis e simples de usar.

A grande tendência atual de mover dados para a nuvem gira em torno da redução de custos para as empresas. O modelo de nuvem é ágil quando se trata de requisitos, permitindo que as organizações adicionem um disco a um servidor com facilidade e rapidez, em vez de adquirir o hardware e pilhas de racks que o acompanham. A nuvem também permite que as organizações evitem o custo e o tempo associados à substituição ou atualização de hardware e de software no data center. Em vez disso, esses requisitos são atendidos pelo provedor de serviços em nuvem e são invisíveis para o negócio. Independentemente do motivo que leva uma organização a decidir fazer a transição para a nuvem, o Veritas Alta™ Analytics para nuvem e o NetBackup IT Analytics no local podem garantir que a experiência seja compatível e econômica em comparação com um ambiente local.

A Veritas fornece uma torre de vigilância com tecnologia de IA, para que você possa assumir o controle de seus dados da nuvem em expansão. Com a Veritas, você pode saber com segurança onde estão todos os seus dados, em um único painel de vidro para todos os dados da empresa, onde quer que estejam. Ela dimensiona facilmente, ao mesmo tempo em que oferece o melhor desempenho da categoria para capacidade em nível de petabytes e abre caminho para a TI como um serviço usando uma conveniente operação de autoatendimento. A Veritas elimina a incerteza com tecnologia completa de visibilidade de dados, detecção de anomalias inteligente e verificação de malware — tudo isso fornecido por nossas soluções de análise.

Pense além dos utilitários e produtos pontuais nativos da nuvem e crie uma estratégia unificada para gerenciamento de dados com segurança cibernética e proteção de dados fundamentais.

A Veritas oferece controle da nuvem.

1. https://www.esg-global.com/ransomware
2. https://www.veritas.com/content/dam/Veritas/docs/reports/GA_ENT_AR_Veritas-Vulnerability-Gap-Report-Global_V1414.pdf

Sobre a Veritas

A Veritas Technologies é líder global em proteção e disponibilidade de dados. Mais de 80 mil clientes, incluindo 95% da Fortune 100, confiam em nós para abstrair a complexidade de TI e simplificar o gerenciamento de dados. A Veritas Enterprise Data Services Platform automatiza a proteção e orquestra a recuperação de dados onde quer que estejam, garante disponibilidade 24 horas por dia, 7 dias por semana de aplicativos críticos para os negócios e fornece às empresas os insights de que precisam para cumprir os regulamentos de dados em evolução. Com uma reputação de confiabilidade em escala e um modelo de implantação para atender a qualquer necessidade, o Veritas Enterprise Data Services Platform suporta mais de 800 fontes de dados diferentes, mais de 100 sistemas operacionais diferentes, mais de 1.400 destinos de armazenamento e mais de 60 plataformas de nuvem diferentes. Saiba mais em www.veritas.com. Siga-nos no Twitter em @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

Para obter informações de contato globais, visite:
veritas.com/company/contact

V1627 22/12