Enterprise Strategy Group **Alcançando a verdade maior.™**

Validação técnica

Segurança cibernética da Veritas

Proteção contra ransomware da Veritas

Por Craig Ledo, analista de validação de TI

Setembro de 2022

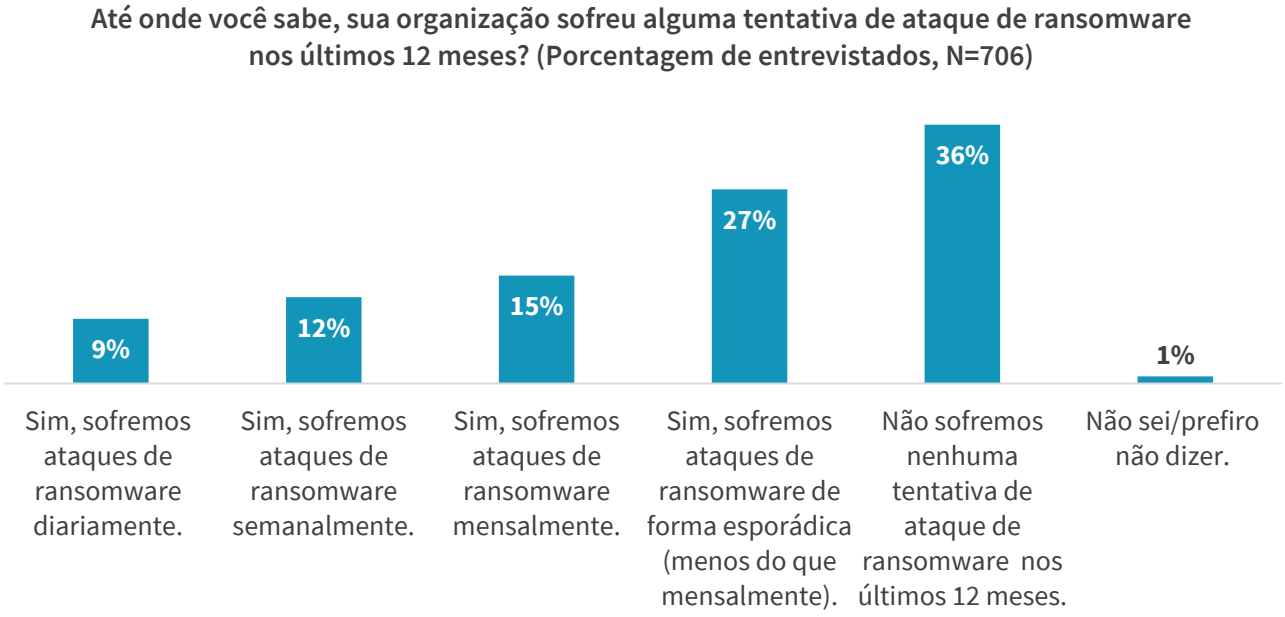
Introdução

Esta validação técnica de ESG documenta a avaliação detalhada da solução Veritas para segurança cibernética, incluindo proteção de dados, detecção de ameaças e recuperação em escala. Especificamente, esta avaliação envolveu a validação de 12 cenários de teste em todo o portfólio de soluções de segurança cibernética da Veritas.

Background

Os ataques de ransomware continuam sendo uma grande preocupação para líderes em empresas e na TI, e por boas razões. Eles comprometem o acesso à força vital de uma organização — os dados. Os contínuos ataques de ransomware resultaram em enormes custos às organizações, incluindo tempo de inatividade, improdutividade, custos de dispositivos, custo de rede, oportunidade perdida, resgates pagos, valor da marca, e assim por diante. Com milhões de dólares gastos por ano para proteger pontos de entrada de dados, muitas organizações ainda subestimam o valor estratégico de aumentar a proteção de dados. A pesquisa do ESG mostra que 36% dos entrevistados disseram que sua organização vivenciou esses ataques de sondagem pelo menos mensalmente nos últimos 12 meses, incluindo 9% que foram atacados diariamente e 12% que foram atacados semanalmente (consulte a figura 1).[1]

Figura 1. Ataques de ransomware recorrentes são comuns



Fonte: ESG, uma divisão da TechTarget, Inc.

Outros 27% dos entrevistados sofreram ataques de ransomware de forma mais esporádica. Portanto, é fundamental que as organizações implementem fortes medidas proativas e defensivas contra ataques de ransomware para impedir seu sucesso, especialmente porque as vítimas podem e serão revisitadas por esses criminosos.

Além disso, com demandas em excesso e com o maior risco de perda de dados, uma estratégia avançada de resiliência multicamadas é necessária, ajudando a garantir que os serviços de TI sejam seguros, resilientes e recuperáveis, ao mesmo tempo em que fornecem a experiência tranquila que os usuários finais esperam. Por exemplo: soluções que foram fortalecidas, de uma perspectiva de software e de hardware, e que suportam armazenamento imutável (que não pode ser alterado) e indelével (não pode ser excluído) ajudam a fornecer uma estratégia de segurança cibernética abrangente e de várias camadas.

[1] Fonte: Relatório de pesquisa do ESG, *Pesquisa de intenções de gastos com tecnologia de 2022*, novembro de 2021.

Visão geral da solução de segurança cibernética da Veritas

A Veritas oferece uma abordagem de plataforma unificada e multicamada que integra proteção proativa, detecção, backup e recuperação. Especificamente, a Veritas fornece às organizações um modelo de segurança de confiança zero, o qual permite que implementem um melhor controle de acesso, contenham violações, protejam ativos e reduzam a chance de sofrer danos.

Proteção:

- Garante que dados essenciais e a infraestrutura de TI sejam protegidos contra o desconhecido e o inesperado; assim, todas as partes do ambiente têm backup com proteção universal, aplicado de forma inteligente e gerenciada automaticamente para escalonamento.
- A infraestrutura de backup e os dados de backup permitem que organizações aumentem a infraestrutura de backup e de recuperação a um componente-chave no sucesso da resiliência.
- O Veritas NetBackup oferece suporte de ponta a ponta na nuvem, com mais de 800 fontes de dados, mais de 1.400 provedores de armazenamento e mais de 60 provedores de nuvem, para que os ambientes mais exigentes e abrangentes possam ser protegidos.
- As políticas inteligentes da Veritas trazem maiores níveis de automação, oferecendo mais eficiência aos administradores.
- A Veritas oferece uma solução de air gap para proteger a integridade dos dados e ajudar a garantir que arquivos de backup fiquem seguros e intocados por invasores mal-intencionados.
- As imagens de backup são imutáveis e indeléveis, com um relógio de conformidade seguro e gerenciado internamente.

Detecção:

- A Veritas oferece soluções que fornecem reconhecimento total da infraestrutura, iluminando todos os dados obscuros no ambiente de uma organização.
- Além disso, a Veritas garante que uma organização saiba que tudo no ambiente é seguro, protegido e capaz de superar ameaças de ransomware.
- A Veritas também oferece detecção de malware e de anomalias com IA em dados primários e de backup, além de escaneamento de malware acionado por evento, o qual oferece mais chances de agir antes que criminosos cibernéticos ou códigos maliciosos tenham a oportunidade de fazê-lo.

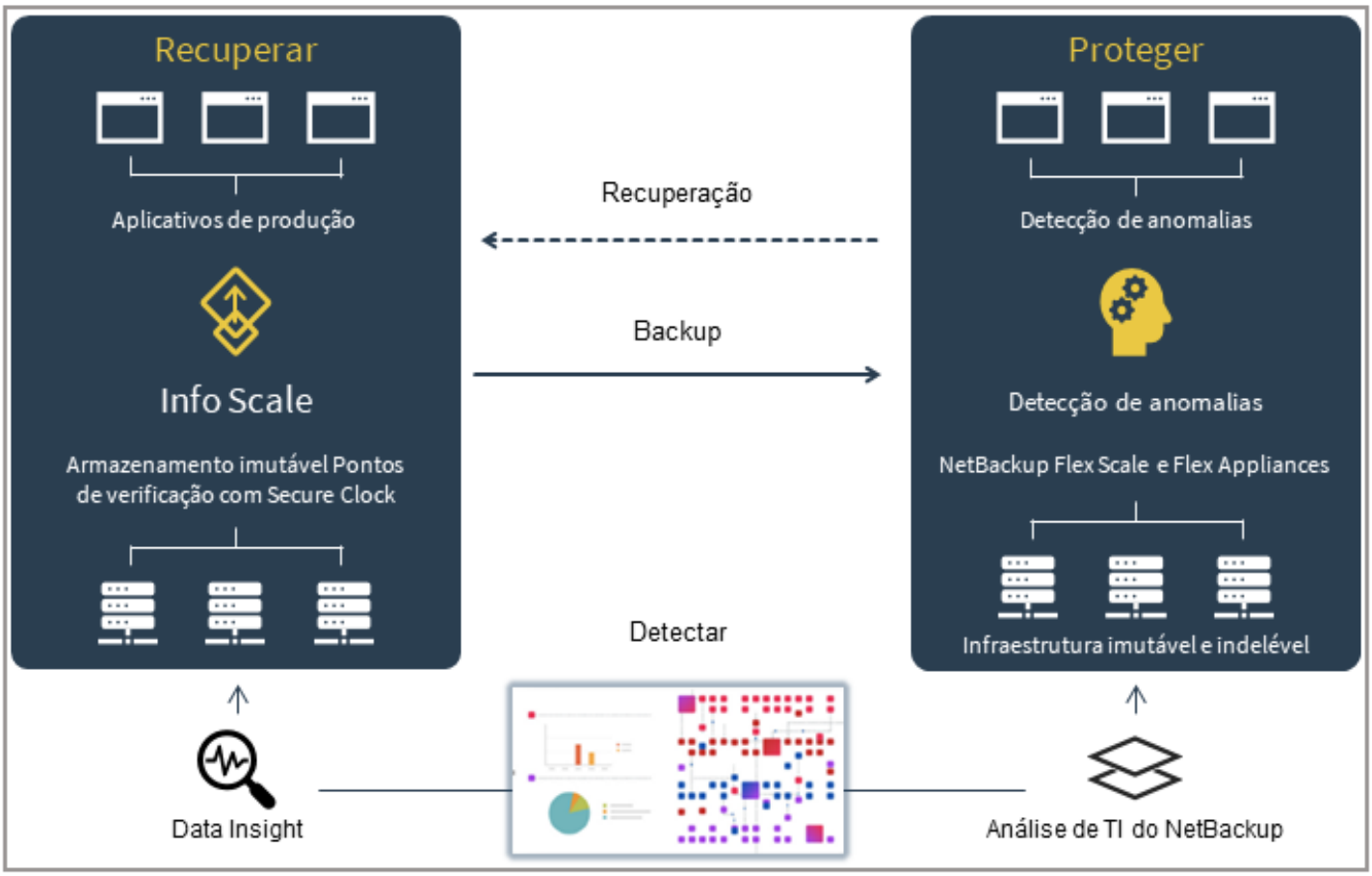
Recuperação:

- Com as soluções da Veritas como componente essencial ao sucesso da resiliência, os ambientes são otimizados para recuperação.
- A Veritas tem soluções de segurança integradas para garantir que dados e ambientes limpos e livres de ransomware voltem a ficar online.
- Às vezes, tudo é afetado, então as organizações podem precisar recuperar um data center inteiro na nuvem e sob demanda.
- Por outro lado, talvez apenas uma parte do ambiente seja afetada. Portanto, pode ser crucial ter soluções flexíveis para recuperar rapidamente bancos de dados e arquivos individuais para produção.

- No caso de servidores inteiros serem criptografados, as organizações podem precisar recuperar rapidamente esses servidores em outro lugar.
- As organizações podem só precisar recuperar um grande número de instâncias de aplicativos para voltar à produção.
- A Veritas fornece soluções para recuperação em escala, incluindo recuperação orquestrada e recuperação em massa.

As soluções da Veritas garantem que os dados estejam sempre disponíveis e protegidos, ajudam na alta disponibilidade de aplicativos e fornecem recuperação escalonável. A Veritas aborda a resiliência contra ransomware por meio de uma lente de valor de negócios, fornecendo uma estratégia de resiliência robusta que soluciona a proteção, detecção e recuperação de ransomware (consulte a figura 2).

Figura 2. Visão geral da solução de resiliência cibernética da Veritas



Fonte: ESG, uma divisão da TechTarget, Inc.

Validação técnica de ESG

O ESG realizou uma validação técnica da solução de segurança cibernética da Veritas, incluindo proteção de dados, detecção de ameaças e recuperação escalonável.

Proteção de dados

A Veritas oferece uma variedade de controles de segurança para ajudar na proteção de dados, incluindo:

- **Gerenciamento de identidade e acesso**: acesso baseado em função, login único e autenticação personalizável.
- **Criptografia de dados**: em trânsito e em repouso.
- **Gerenciamento e armazenamento de imagens imutáveis**: gerenciamento de imagens flexível e independente de armazenamento e imagens armazenadas em armazenamento WORM (grave uma vez, leia várias).
- **Fortalecimento da solução**: o NetBackup Flex e o NetBackup Flex Scale foram reforçados de uma perspectiva de software e hardware para oferecer uma solução segura completa que suporta armazenamento imutável.

Especificamente, o ESG validou os recursos-chave de proteção de dados a seguir.

Imutabilidade de dados da nuvem

A solução impede que os dados sejam alterados por um certo período de tempo para protegê-los contra invasões de criminosos cibernéticos e ameaças internas. Para melhorar ainda mais a segurança, o armazenamento de backup está em um armazenamento de dados seguro que só é visível e acessível ao serviço de armazenamento NetBackup, eliminando o acesso por parte de usuários e de serviços de sistemas de arquivos.

Impenetrabilidade aprimorada

A pilha completa do NetBackup Appliances teve sua segurança fortalecida, incluindo o sistema operacional Linux, acesso de gerenciamento, binários de aplicativos e definições de configuração. Inclui políticas de segurança proprietárias que estão em conformidade com as diretrizes do STIG e reforçam o controle de acesso obrigatório. Também inclui detecção de intrusão e serviços de proteção que restringem o acesso a processos e recursos e mantêm uma trilha de auditoria de ações importantes do usuário e do sistema.

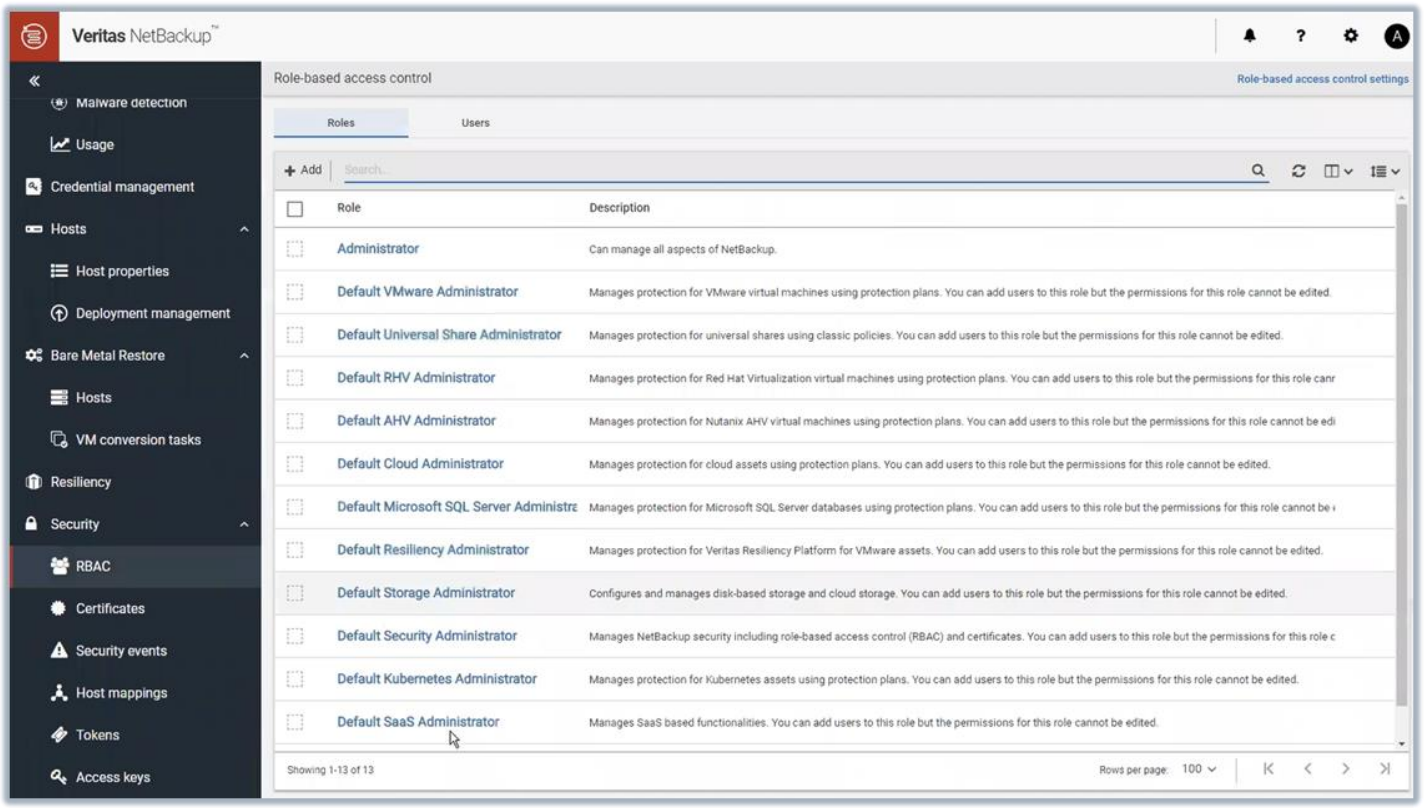
Hardware resistente a adulterações

Appliances que hospedam armazenamento imutável podem passar para um nível elevado de segurança para proteger os dados e a infraestrutura. Os administradores são impedidos de fazer alterações no sistema operacional e nos componentes internos; todos os endpoints são protegidos contra acesso não autorizado, e o acesso a todos os serviços é protegido e autenticado.

Controles de acesso seguros

A solução fornece modelos de controle de acesso baseado em função (RBAC), conforme mostrado na figura 3. Isso torna mais fácil para os administradores fornecer acesso ou permissões apropriados a usuários ou grupos de usuários. Os administradores também podem detalhar cada um dos modelos para ver as permissões detalhadas (por exemplo, NetBackup Management, Protection, Security, e Storage). Os administradores também podem criar permissões ou acessos personalizados para usuários ou grupos. Com base na função personalizada, os administradores também podem atribuir cargas de trabalho (selecionar os ativos de carga de trabalho que os usuários podem gerenciar), planos de proteção (selecionar os planos de proteção que os usuários podem gerenciar) e credenciais (selecionar as credenciais que os usuários podem gerenciar).

Figura 3. Controles de acesso seguros

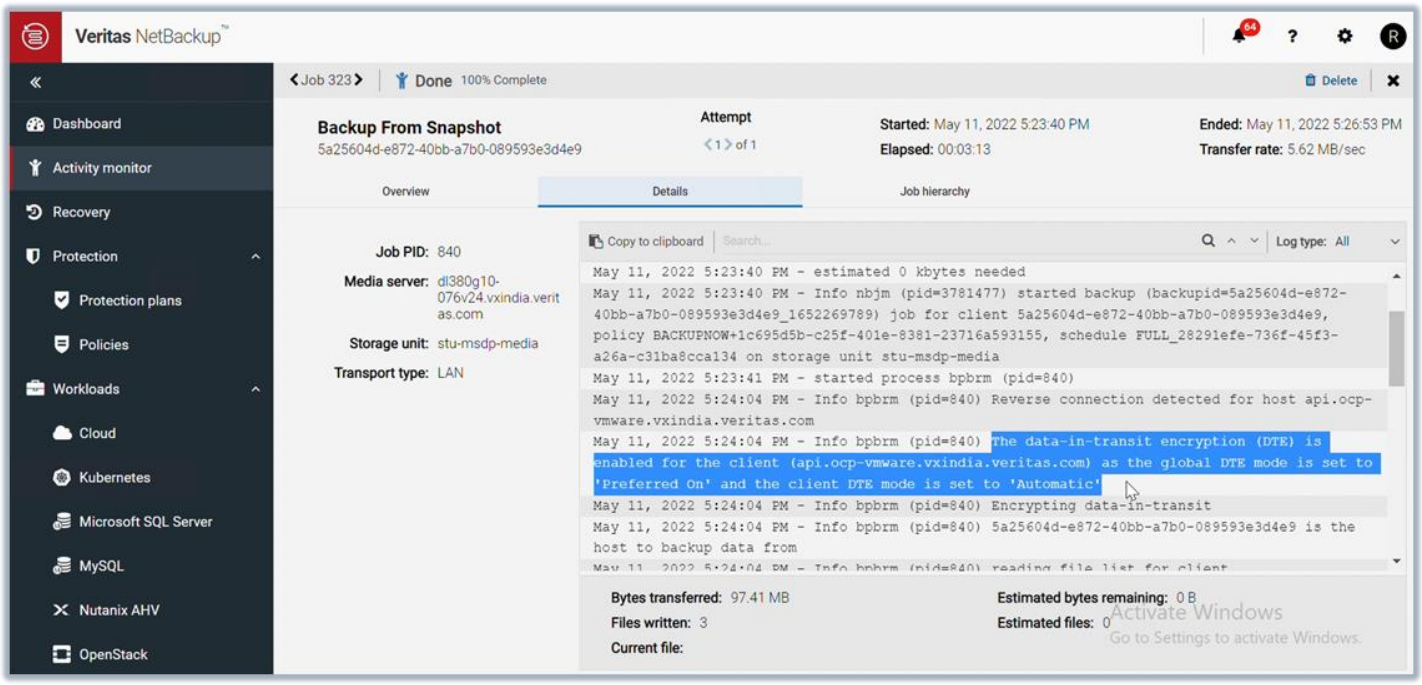


Fonte: ESG, uma divisão da TechTarget, Inc.

Proteção para infraestruturas modernas

A solução fornece tecnologias de proteção de dados de última geração para infraestruturas modernas, incluindo big data, bancos de dados MySQL/NoSQL de código aberto ou hiperconvergentes. O NetBackup permite que as organizações protejam cargas de trabalho multinuvem, virtuais, físicas e modernas, independentemente de onde residam — tudo a partir de um único console. A figura 4 mostra o backup de uma captura. O backup tinha criptografia de dados em trânsito (DTE) habilitada para o cliente, pois o modo DTE global está definido como "Preferivelmente ligado" e o modo DTE do cliente está definido como "Automático". Os usuários podem restaurar, se necessário, a partir deste backup, o qual tem o DTE ativado, pois o modo DTE da imagem de backup está definido como "Ligado ".

Figura 4. Proteção para infraestruturas modernas



Fonte: ESG, uma divisão da TechTarget, Inc.

Por que isso é importante

À medida que os ataques de ransomware evoluem e se tornam mais sofisticados, é importante que as empresas se adaptem aos vetores de ameaças que mudam rapidamente para evitar tempo de inatividade do serviço e perda de dados. A proteção avançada de dados e os dispositivos seguros da Veritas fornecem vários recursos para combater o ransomware, como detecção de anomalias integrada, escaneamento de malware, arquitetura de confiança zero e armazenamento imutável e indelével.

Detectando ameaças

A Veritas oferece uma ampla gama de controles de segurança para ajudar na detecção de ameaças, incluindo:

- Noção da infraestrutura de backup e armazenamento: o NetBackup IT Analytics fornece monitoramento de backup de ponta a ponta que inclui análise de mitigação, fontes com falhas consecutivas, fontes sem backup recente e falhas de backup por aplicativo.
- Detecção de anomalias: o NetBackup fornece detecção de anomalias com inteligência artificial que detecta dados incomuns em todo o ambiente e fornece alertas para anomalias suspeitas quase em tempo real.
- Detecção de armazenamento primário: a Veritas lida com os dados de backup secundário com o NetBackup e os dados de armazenamento primário com o Veritas Data Insight, o qual complementa as ferramentas de detecção de segurança existentes ao fornecer detecção de comportamento anômalo no contexto de dados e usuários quase em tempo real. Além disso, oferece modelos de consulta personalizados específicos de ransomware e identificação de extensão de arquivo, o que é útil para detectar ransomware.

- **Detecção de malware**: a Veritas oferece varreduras automatizadas e sob demanda para backups protegidos. O recurso automatizado de escaneamento de malware remove a dependência humana e permite que a tecnologia de inteligência artificial/aprendizado de máquina (AI/ML) interfira e verifique se há malware.

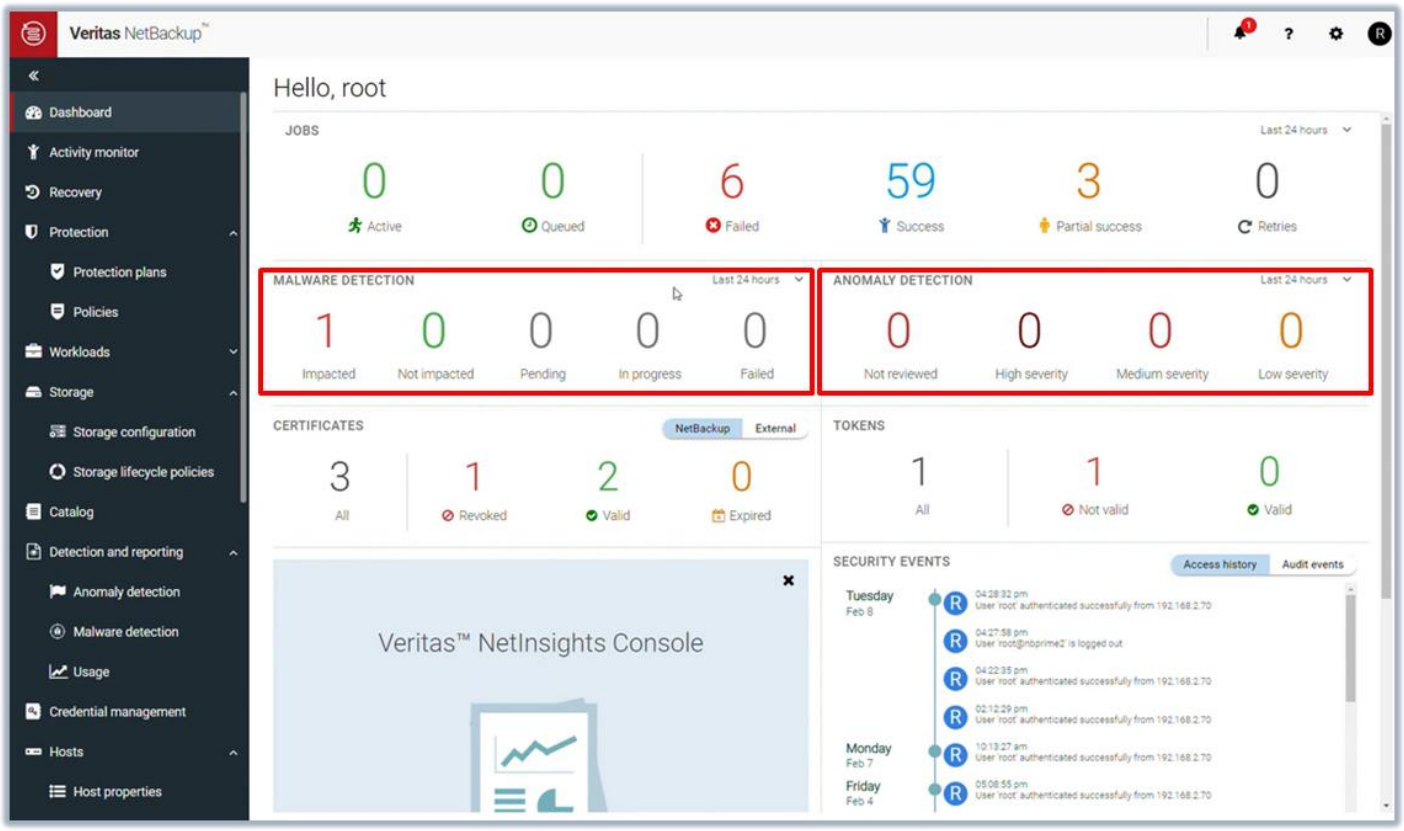
Especificamente, o ESG validou os seguintes recursos-chave de detecção de ameaças.

Escaneamento integrado de malware e detecção de anomalias

A detecção de anomalias rastreia os metadados da imagem separadamente da detecção de malware, mas a detecção de malware pode aproveitar as pontuações de detecção de anomalias. Os eventos de detecção de malware são classificados em Impactado, Não impactado, Pendente, Em andamento e Com falha, de acordo com as "últimas 24 horas", conforme mostrado na figura 5. O período também pode ser definido para "últimas 48 horas" ou "últimas 72 horas". Os usuários podem detalhar cada área (por exemplo, Impactado) para ver mais detalhes. Para cada imagem de backup afetada, os usuários podem tomar medidas, incluindo expirar todas as cópias ou visualizar arquivos infectados. O painel de detecção de malware fornece as seguintes informações: cliente, hora do backup, resultado do escaneamento, tipo de backup, data do escaneamento, escaneador de aplicativos de malware, número de arquivos afetados, nome do host do escaneamento e ID do backup. O tempo de escaneamento do malware varia dependendo de vários fatores, incluindo o tamanho da imagem e o número de arquivos.

Os eventos de detecção de anomalias são classificados em Não revisado, Alta gravidade, Média gravidade e Baixa gravidade, de acordo com as "últimas 24 horas", conforme mostrado na figura 5. O período também pode ser definido para "últimas 48 horas", "últimas 72 horas" ou "últimos 7 dias". Os usuários também podem filtrar o Status da revisão (Não revisado, Falso positivo, Anomalia, Ignorar) e a Gravidade da anomalia (alta, média, baixa). O painel de detecção de anomalias fornece as seguintes informações: ID do trabalho, Nome do cliente, Tipo de política, Contagem, Pontuação, Gravidade da anomalia, Resumo da anomalia, Recebido, Status da revisão, Nome da política, Nome do agendamento e Tipo de agendamento. Os usuários podem realizar as seguintes ações em relação às anomalias: Marcar como ignorar, Confirmar como anomalia e Reportar como falso positivo.

Figura 5. Escaneamento integrado de malware e detecção de anomalias



Fonte: ESG, uma divisão da TechTarget, Inc.

Geração de relatórios e alertas

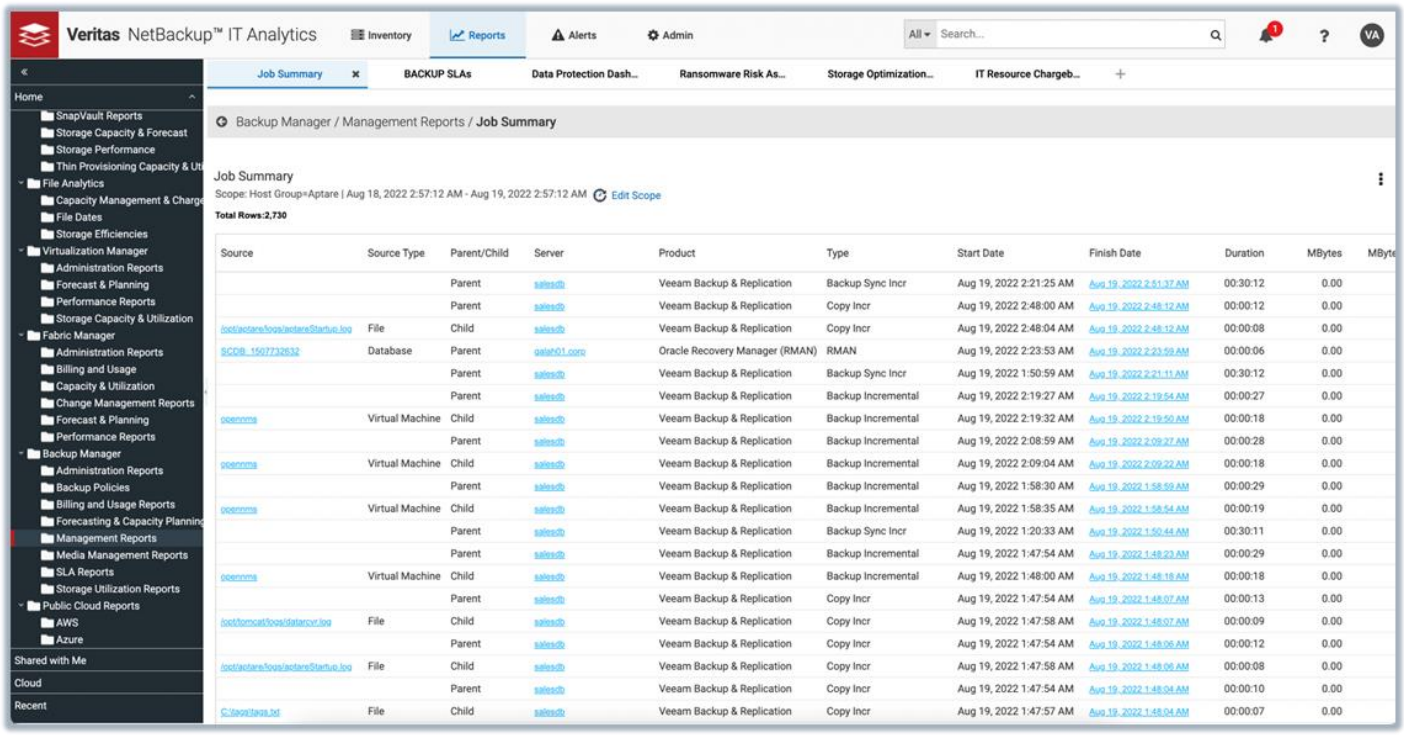
O Veritas NetBackup IT Analytics fornece um painel de avaliação de risco de ransomware pronto para uso. O painel oferece aos usuários uma visão rápida dos relatórios pré-identificados que usam análises preditivas para compreender os potenciais riscos em um ambiente de backup (consulte a figura 6). A análise ajuda os usuários a garantir que o ambiente de backup seja otimizado e seguro, fornecendo relatórios abrangentes sobre vários pontos de dados, incluindo:

- Descoberta – os usuários podem rastrear todas as alterações no ambiente de backup para ajudar a detectar ransomware e responder rapidamente, incluindo suporte para mais de 850 extensões de ransomware conhecidas.
- Visualização de riscos – gráficos intuitivos fornecem aos usuários uma visão em histórico de todos os riscos gerados no ambiente, sinalizam hosts que estão faltando no agendamento de backup e visualizam aplicativos com falha de backup.
- Monitoramento de backup – os usuários podem monitorar e identificar alterações no ambiente de backup com gráficos de resumo que fornecem insights acionáveis. Os usuários também podem reduzir o risco identificando anomalias usando uma linha de base de backups bem-sucedidos conhecidos.

Além de detectar arquivos com extensões de ransomware conhecidas, o NetBackup IT Analytics permite que os usuários organizem essas informações de maneira significativa para que possam executar um plano de ação rápido. Os usuários podem organizar os arquivos de ransomware detectados pelos hosts, locais com a maioria dos arquivos de ransomware, tipos de extensões de ransomware e os proprietários de arquivos.

O NetBackup IT Analytics também investiga backups bem-sucedidos para identificar possíveis falsos positivos, comparando backups no histórico 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. Isso dá aos usuários a garantia de que os serviços críticos de TI estão sendo protegidos.

Figura 6. Geração de relatórios e alertas



Fonte: ESG, uma divisão da TechTarget, Inc.

Por que isso é importante

Como dito anteriormente, os ataques de ransomware evoluíram e se tornaram mais sofisticados, portanto, a Veritas fornece visibilidade holística em tempo real do status de aplicativos e dados com detecção de anomalias e insights personalizados que ajudam a identificar a infiltração de malware nos dados primários e de backup.

Recuperação escalonável

A Veritas oferece diversos recursos para ajudar na recuperação escalonável, incluindo:

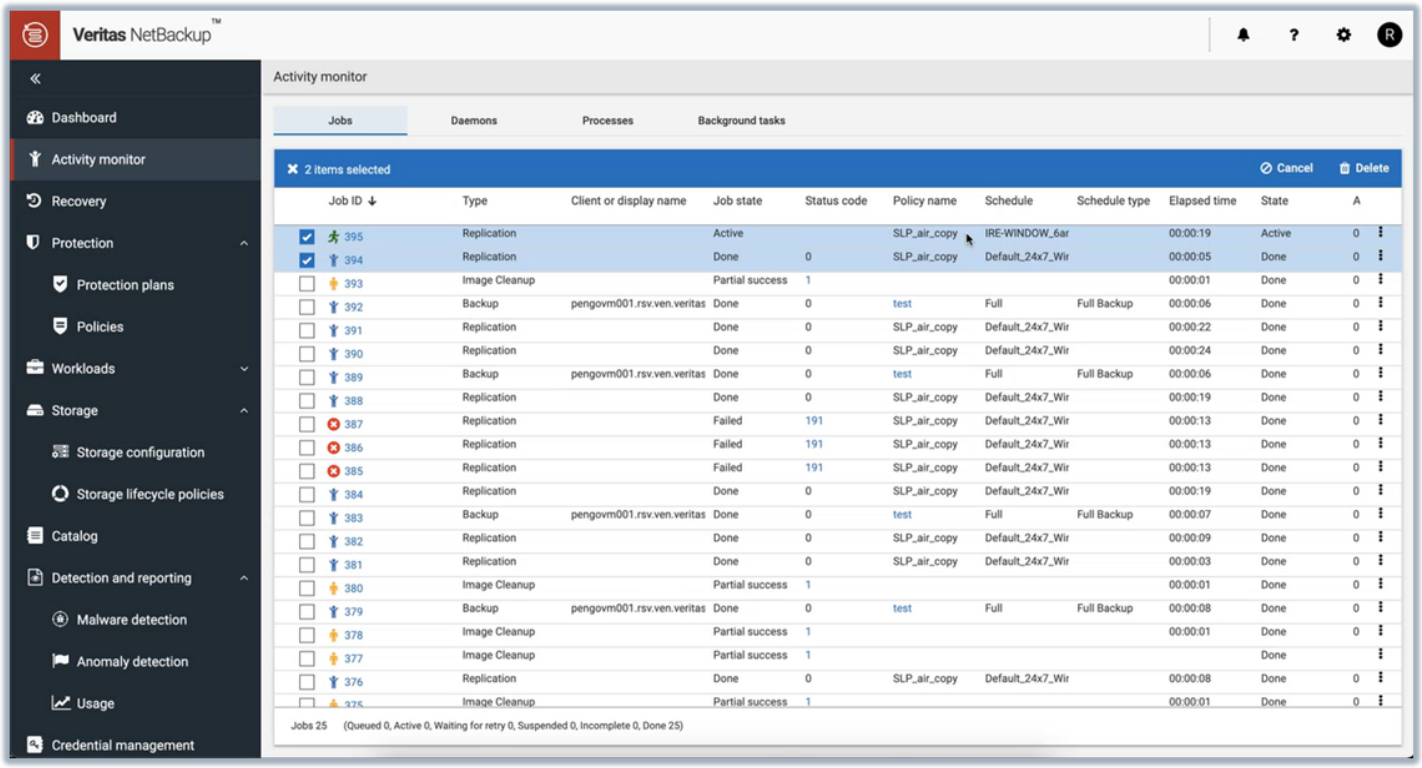
- Resiliência do NetBackup: fornece orquestração automatizada em todo o ambiente heterogêneo de uma organização com uma experiência de usuário consistente e com visibilidade das melhores opções de recuperação, com base nas opções disponíveis.
- NetBackup Instant Rollback for VMware: oferece recuperação de máquina virtual em alta velocidade usando o rastreamento reverso de bloco de alteração para identificar quais blocos exclusivos precisam ser recuperados, aplicando apenas essas alterações para trazer as VMs de volta a um estado íntegro em segundos.
- VM Recovery: oferece oito tipos de recuperação para um backup de VMs de VMware, incluindo VM completa, VMDK individual, arquivo e pasta, aplicativo completo, acesso instantâneo, download de arquivo, aplicativo GRT e conversão de AMI.
- Acesso instantâneo para MSSQL e Vmware: fornece recuperação de máquina quase instantânea (por exemplo, 1.600 VMs) sem esperar para transferir os dados da VM do backup. Também fornece a capacidade de testar ou recuperar VMs diretamente do armazenamento de backup.
- NetBackup CloudPoint: o NetBackup CloudPoint usa a tecnologia de snapshot nativa da nuvem de maneira independente do fornecedor da nuvem, o que permite a fácil proteção de infraestruturas híbridas e multinuvem.
- Compartilhamento universal e pontos de proteção: permite que as organizações provisionem armazenamento com eliminação de duplicações no servidor NetBackup como compartilhamentos seguros, protegendo bancos de dados ou outras cargas de trabalho onde não existe nenhum agente ou API de backup.
- NetBackup Universal Shares for Oracle: permite que administradores de banco de dados Oracle iniciem bancos de dados diretamente do armazenamento de um NetBackup Appliance.
- Arquivo morto de retenção a longo prazo: fornece uma solução econômica e durável com eliminação de duplicações e compactação de dados, incluindo o uso de armazenamento de objetos e nuvens públicas ou privadas com esse método. A recuperação tradicional inclui restauração granular de um arquivo específico, restauração completa de servidor/aplicativo e restauração de recuperação após desastres (DR) para um local diferente ou para a nuvem. Usando o Veritas Resiliency Platform, as organizações podem automatizar e orquestrar a recuperação tradicional com o apertar de um botão, simplificando o processo de recuperação após desastres.
- Bare Metal Restore: automatiza o processo de recuperação do servidor, tornando desnecessário reinstalar sistemas operacionais ou configurar hardware manualmente. Permite que as organizações reconstruam sistemas rapidamente do zero, restaurando o sistema operacional e os dados do aplicativo com uma única operação.

Especificamente, o ESG validou os seguintes recursos-chave de recuperação escalonável.

Ambiente de Recuperação Isolado

O ambiente de recuperação isolado do Veritas NetBackup permite planos de recuperação para milhares de VMs que podem fazer parte de ambientes complexos de vários níveis e a capacidade de executar ensaios do mesmo em um ambiente isolado (consulte a figura 7). Esse recurso pode fornecer suporte para imutabilidade e indelebilidade integradas, imutabilidade de hardware de terceiros, imutabilidade de armazenamento de objeto bloqueado baseado em nuvem e imutabilidade para backups de carga de trabalho SaaS. Além disso, o NetBackup pode enviar e armazenar dados com duplicação eliminada no AWS S3 Object Lock.

Figura 7. Ambiente de recuperação isolado

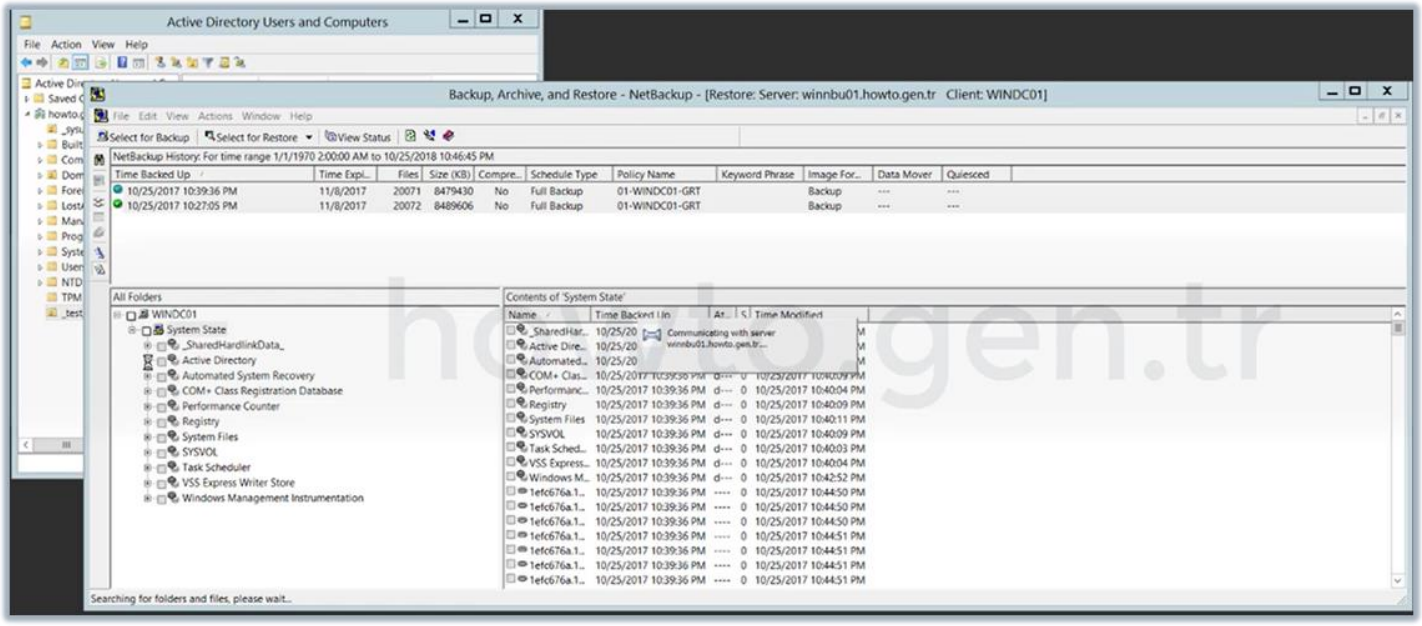


Fonte: ESG, uma divisão da TechTarget, Inc.

Recuperação perdida do Active Directory

A solução Veritas NetBackup oferece a capacidade de recuperar um Active Directory perdido navegando pelos backups do Active Directory (consulte a figura 8). Em seguida, o usuário simplesmente inicia o backup adequado do Active Directory. O usuário também pode visualizar o andamento da restauração até mostrar que a operação solicitada foi bem-sucedida.

Figura 8. Recuperação perdida do Active Directory

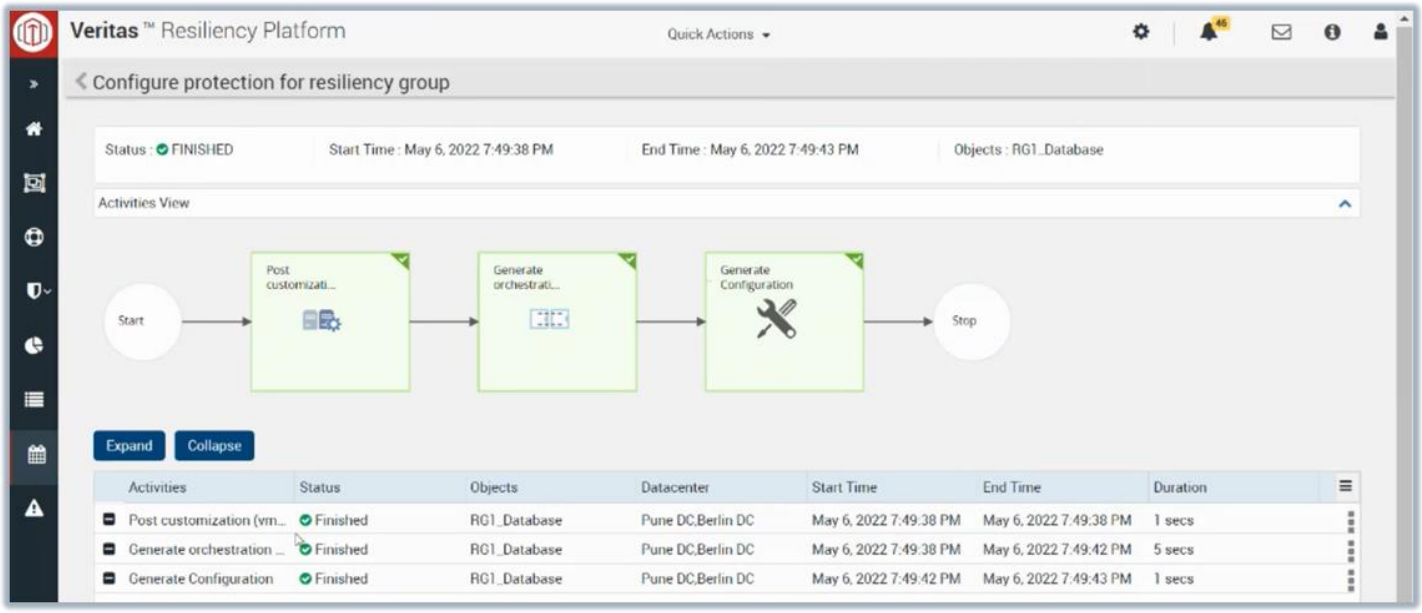


Fonte: ESG, uma divisão da TechTarget, Inc.

Orquestração de recuperação em camadas

Os serviços de negócios virtuais do Veritas NetBackup Resiliency permitem que os usuários gerenciem a recuperação de aplicativos multicamadas como uma única entidade consolidada. Com o Virtual Business Services, os usuários podem automatizar completamente a recuperação de um aplicativo complexo de várias camadas que abrange vários sistemas. No caso de um ataque de ransomware, isso proporciona uma recuperação mais fácil e rápida, e o aplicativo passa por um breve tempo de inatividade. Especificamente, a Veritas Resiliency Platform fornece orquestração de recuperação em camadas, por exemplo, configurando virtualização e nuvens (adicionando Vmware vCenter), servidores primários NetBackup, redes (pareamento de rede), servidores físicos, bancos de dados etc. Consulte a figura 9 para ver a configuração de proteção do grupo de resiliência concluída.

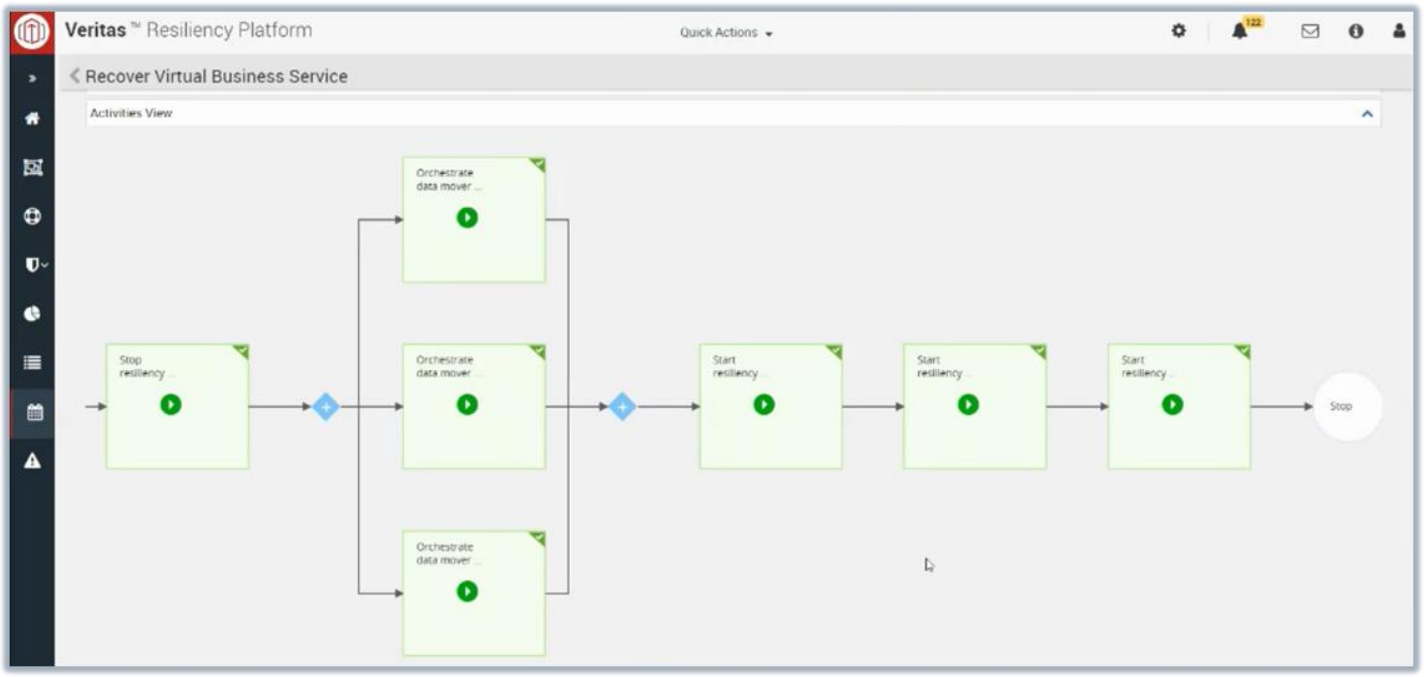
Figura 9. Configuração de recuperação em camadas



Fonte: ESG, uma divisão da TechTarget, Inc.

Após a conclusão da configuração da proteção do grupo de resiliência, o usuário precisa configurar o Virtual Business Service em camadas. Em seguida, o usuário pode orquestrar a recuperação em camadas do Virtual Business Service (consulte a figura 10).

Figura 10. Orquestração de recuperação em camadas



Fonte: ESG, uma divisão da TechTarget, Inc..

Por que isso é importante

À medida que os ataques de ransomware aumentam, é importante que as empresas tenham uma estratégia abrangente de resiliência e de recuperação após ransomwares. A Veritas oferece armazenamento avançado e recursos de recuperação rápida para dados primários com resiliência de armazenamento integrado, imutabilidade e recursos de isolamento de dados que garantem a disponibilidade de aplicativos, bem como a segurança e a integridade dos dados.

A grande verdade

Ransomwares e pessoas mal-intencionadas com acesso representam sérias ameaças. Novas vulnerabilidades de sistemas operacionais são descobertas a todo instante, e novas variantes de malware e de ransomware são desenvolvidas com regularidade. O ransomware é um grande negócio, o que significa que os malfeitores são motivados a continuar inovando em novas formas de penetrar na infraestrutura de uma organização e interromper seus negócios.

O ESG validou 12 cenários de teste que abrangem a solução Veritas para segurança cibernética, incluindo proteção de dados, detecção de ameaças e recuperação em grande escala. Uma estratégia de segurança cibernética holística, multicamada e abrangente é sempre a melhor defesa contra o tempo de inatividade e a perda de dados devido à infiltração de malware. A Veritas entende que isso pode ser um desafio complexo e forneceu uma base empresarial para ajudar as organizações a proteger os serviços de TI como parte de uma estratégia geral de segurança cibernética. A estratégia de segurança cibernética da Veritas fornece às organizações ferramentas, funcionalidade e garantia de que os serviços de TI serão altamente disponíveis, resistentes e protegidos de ransomware.

www.esg-global.com contact@esg-global.com 508.482.0188