

NOTA DE SOLUÇÃO

CONSTRUINDO UMA INFRAESTRUTURA ÁGIL E RESILIENTE

No cenário de negócios acelerado e competitivo de hoje, a agilidade e a inovação impulsionam o sucesso de uma empresa. À medida que a tecnologia continua evoluindo, a rede moderna deve ser adaptável, acompanhando o ritmo da inovação ao aproveitar os últimos avanços, permitindo a implementação eficiente de novos aplicativos e serviços, além de proporcionar a flexibilidade necessária para responder às mudanças nas demandas do mercado.



O RITMO DA MODERNIZAÇÃO É IMPLACÁVEL

Até 2026, pelo menos 50% dos aplicativos locais serão modernizados para se integrarem às ferramentas de uma plataforma de gerenciamento de SaaS (SMP), contra 20% em 2021, de acordo com um relatório da Gartner. Com a digitalização, as redes estão ficando mais dinâmicas e mudando o tempo todo. Diversos fatores contribuem para a aceleração da modernização, incluindo trabalho remoto, expansão multinuvem, novas exigências de cibersegurança e a necessidade de novos conjuntos de competências.

DEFICIÊNCIAS DOS SERVIÇOS DE REDE CRÍTICOS ANTIGOS

A infraestrutura de rede compreende muitos componentes: firewalls, roteadores, switches, dispositivos Wi-Fi, servidores de nome de domínio, servidores DHCP etc. A maioria dos elementos de infraestrutura mais importantes já foram atualizados para versões modernas de hardware ou software. E os servidores de nome de domínio e os servidores DHCP? Seus principais serviços de rede ainda estão desatualizados? Recorrer a serviços de rede antigos (como softwares gratuitos, soluções improvisadas ou sistemas díspares) representa um grande obstáculo para sua jornada digital.

- **Sistemas antigos são desarticulados:** o gerenciamento manual é caro e apresenta alto risco de tempo de inatividade e interrupções.
- **Sistemas antigos são lentos:** as redes devem ser ágeis para adotar novas ideias e tecnologias como parte de iniciativas estratégicas de digitalização ou F&A.
- **Sistemas legados estão expostos:** as lacunas de segurança e a falta de percepção contextual resultam em uma remediação ineficiente e atrasada das ameaças.

O DNS e o DHCP são essenciais para todas as redes. Se você ainda estiver utilizando serviços nativos, sua rede estará sujeita a grandes interrupções.

PRINCIPAIS FATORES DA MODERNIZAÇÃO: CAMINHO A SEGUIR

As organizações estão modernizando suas redes para enfrentar os desafios do cenário regulatório em constante crescimento, das restrições de recursos, das ameaças em constante evolução e das lacunas de habilidades na esfera da segurança. Elas precisam reduzir constantemente o tempo de inatividade, gerenciar as despesas indiretas e minimizar as violações de segurança para garantir 100% de tempo de atividade, adotar novas ideias e aprimorar a pilha de segurança existente. Para isso, é necessário repensar as abordagens em relação às operações essenciais da rede, incluindo DNS, DHCP e gerenciamento de endereços IP (em conjunto, “DDI”). Aqui estão os principais fatores para modernizar a sua rede.



SIMPLIFIQUE AS OPERAÇÕES: SUBSTITUA SOFTWARES GRATUITOS POR FERRAMENTAS ESPECÍFICAS

Parece gratuito, mas não é. Embora as despesas de capital iniciais possam parecer menores, as despesas operacionais que você tem ao usar ferramentas DDI gratuitas ou de baixo custo superam as vantagens. Soluções de software gratuito, como as da Microsoft ou ferramentas de código aberto, não conseguem ser expandidas para acompanhar o crescimento devido a limitações do sistema e à falta de recursos avançados para permitir alta disponibilidade, descoberta de máquinas virtuais não utilizadas, validações baseadas em políticas etc. As infraestruturas da Microsoft são propensas a interrupções e a tempo de inatividade, seja devido a atualizações constantes de patches ou à necessidade de migração para o Azure AD. O gerenciamento manual de sites distribuídos contribui para a ineficiência e aumenta os custos indiretos.

A melhor abordagem é utilizar **ferramentas específicas** para simplificar e agilizar operações de missão crítica. Essas ferramentas são criadas para a globalização e permitem reduzir as tarefas operacionais ao expandir-se sem dificuldades para infraestruturas diversas e locais remotos. Elas simplificam o gerenciamento, otimizam a manutenção e reduzem o tempo, fornecendo automação, descoberta e visibilidade centralizada da rede. Oferecem atualizações sem qualquer tempo de inatividade e reduzem o tempo de inatividade ao fornecerem alta disponibilidade em escala.



ACELERE AS INOVAÇÕES: UTILIZE UMA ÚNICA FERRAMENTA CENTRALIZADA EM VEZ DE SISTEMAS DIFERENTES

A maioria das empresas utiliza de duas a quatro soluções de DNS, o que dificulta o gerenciamento de serviços essenciais e a agilidade na resposta aos problemas. Os silos organizacionais e informacionais costumam causar atrasos e erros. Diferentes convenções de nomenclatura e modelos operacionais entre vários provedores de nuvem levam a configurações incorretas e períodos de inatividade. A visibilidade fragmentada nas redes aumenta o tempo necessário para a solução de problemas e auditoria.

As organizações devem encontrar uma solução eficiente e eficaz para acelerar inovações e viabilizar iniciativas de negócios, como expansão multinuvel, fusões e aquisições etc. Ao investir em uma **ferramenta centralizada**, você poderá atingir esses objetivos por meio da automação, de uma única convenção de nomenclatura de DNS e da visibilidade em redes locais e na nuvem. Em vez de usar uma combinação de sistemas díspares, você pode se adaptar mais rápido às necessidades empresariais e reduzir ineficiências com uma ferramenta centralizada. Ela oferece controle e consistência de políticas, solução de problemas mais rápida e melhor colaboração, além de eliminar os erros e as configurações incorretas e reduzir os riscos de auditoria e conformidade e os custos operacionais.



PROTEJA A INTEGRIDADE DA MARCA: UTILIZE O DNS PARA DETECTAR AMEAÇAS DE FORMA PRECOCE

Os domínios em constante evolução do cenário de ameaças, como malware, ransomware, domínios lookalike, exfiltração de dados e phishing, representam grandes riscos para a identidade da marca e a proteção de dados. Há uma lacuna de segurança significativa, pois as soluções existentes no mercado ignoram o DNS e não conseguem evitar os ataques. Só no ano passado, hackers usaram quase 42 mil domínios falsos em um ataque de phishing em larga escala. Além disso, sistemas isolados e díspares, escassez de habilidades, gerenciamento manual e falta de percepção contextual resultam em ineficiências no SecOps e tempos de resposta atrasados.

A detecção precoce de ameaças reduz os riscos e elimina a lacuna de segurança. O uso da **caça a ameaças baseada em DNS** detecta e bloqueia ameaças antecipadamente, já que a maioria dos ataques cibernéticos depende do DNS. O uso do DNS como primeira linha de defesa protege contra exfiltração de dados, algoritmos de geração de domínios e impostores, além de proteger todos os dispositivos de IoT/OT. Isso melhora a eficiência do SecOps ao reduzir o tempo de investigação, automatizar a remediação e avaliar proativamente os riscos de vulnerabilidade.

SOLUÇÕES DA INFOBLOX PARA UMA INFRAESTRUTURA ÁGIL E RESILIENTE

Visibilidade, automação e controle

A Infoblox oferece às organizações visibilidade, automação e controle inigualáveis sobre quem e o que se conecta à sua rede. A Infoblox reduz significativamente o tempo de inatividade dispendioso ao eliminar a manutenção obrigatória e trabalhosa, automatiza tarefas operacionais que demandam muita mão de obra e reduz a carga associada ao gerenciamento de inventário de ativos de rede. As soluções da Infoblox são criadas com foco na segurança, reduzindo alertas falsos por meio de maior consciência contextual e aprimorando a eficiência. A Infoblox oferece:

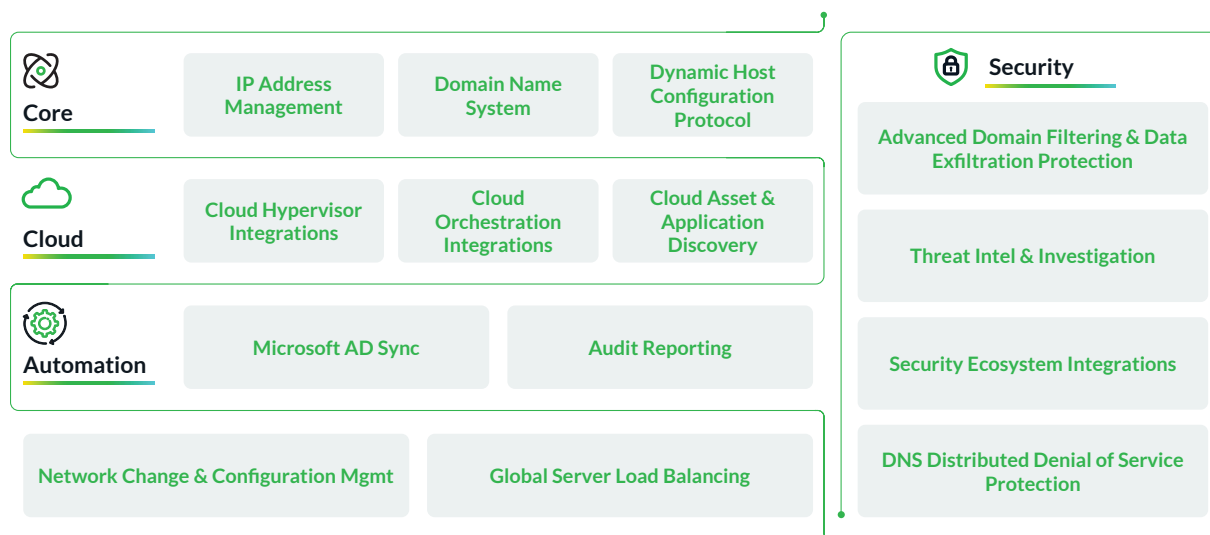


Figura 1: soluções da Infoblox

CONCLUSÃO

A modernização promove a transformação digital. A escolha da solução certa para a sua rede promove a modernização contínua. As abordagens antigas de gerenciamento de serviços de rede essenciais prejudicarão sua capacidade de inovar com rapidez, adaptar-se às demandas dinâmicas de negócios e manter-se competitivo. Aproveite a visibilidade, a automação e o controle que a Infoblox proporciona para modernizar sua rede na velocidade necessária e adequada à expansão dos seus negócios.



A Infoblox une rede e segurança para oferecer desempenho e proteção incomparáveis. Confiada por empresas da Fortune 100 e inovadores emergentes, oferecemos visibilidade e controle em tempo real sobre quem e o que se conecta à sua rede, para que sua organização funcione mais rapidamente e detecte ameaças mais cedo.

Sede Corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1,408,986,4000
www.infoblox.com