LEMBAR DATA

Infoblox Threat Defense™ Advanced

DNS Protektif yang didukung oleh intelijen ancaman prediktif melindungi segala sesuatu, di mana pun—sebelum dampak terjadi

DNS ADALAH TITIK PENCEGAHAN PALING AWAL UNTUK SEMUA SERANGAN SIBER

DNS adalah titik pertama untuk deteksi dan pencegahan semua serangan siber. Apakah dimulai dengan email phishing, teks smishing, atau kerentanan yang dieksploitasi, hampir setiap serangan menghasilkan kueri DNS ke domain berbahaya. Sebagai hasilnya, DNS menyediakan titik visibilitas dan kontrol yang kuat dan terpusat untuk mengamankan seluruh perusahaan, termasuk pengguna, perangkat, IoT/OT, dan beban kerja baik di lokasi, di cloud, maupun di tepi jaringan.

Sebagai langkah pertama dalam komunikasi apa pun, mendeteksi dan memblokir aktivitas ancaman di lapisan DNS membantu menghentikan lalu lintas berbahaya sebelum mencapai alat hilir dan memicu peringatan. Dengan mengorelasikan data DNS dengan konteks perangkat dan aset, tim NetOps dan SecOps mendapatkan visibilitas yang lebih mendalam tentang apa yang terjadi di seluruh lingkungan mereka, sehingga meningkatkan efisiensi operasional dan postur keamanan.

SOLUSI "DETEKSI DAN RESPON" TRADISIONAL TIDAK LAGI EFEKTIF

Pelaku ancaman semakin sering menggunakan AI untuk meluncurkan kampanye yang lebih produktif, canggih, dan tersembunyi. Mereka menghasilkan malware yang dirancang secara unik dan sekali pakai yang membuat alat 'deteksi dan respons' tradisional—yang menunggu infeksi 'pasien nol'—menjadi tidak efektif. Setiap serangan berubah menjadi skenario "pasien nol" di mana tidak ada tanda tangan atau perilaku yang dikenal. Alat-alat "deteksi dan tanggap" sering kali bertindak terlambat dalam rantai pembunuhan untuk mencegah kerusakan. Oleh karena itu, diperlukan pendekatan preemptif yang berbeda. Satu yang menghentikan ancaman sebelum mereka memasuki lingkungan atau bergerak secara lateral. Ini tidak hanya memblokir serangan lebih awal tetapi juga mengurangi beban pada alat 'deteksi dan respons' tradisional.

DNS berfungsi sebagai titik kontrol hulu yang memberikan tim keamanan kesempatan proaktif untuk mendeteksi dan memblokir ancaman lebih awal, sebelum mencapai pengguna, beban kerja, atau titik akhir.

KEAMANAN PREEMPTIF DENGAN DNS

Infoblox Threat Defense™ Advanced menyediakan **pendekatan preemptif** yang unik untuk deteksi ancaman. Pendekatan yang tidak bergantung pada "pasien nol." Ini menggunakan kombinasi **intelijen ancaman prediktif** yang memblokir infrastruktur pelaku ancaman sebelum mereka dipersenjatai, dan analisis berbasis algoritmik/ML dari kueri DNS di jaringan pelanggan untuk memberikan perlindungan sebelum dampak. Melalui identifikasi cepat aset yang terlibat dalam insiden keamanan, integrasi ekosistem, dan ruang kerja intuitif, ini memungkinkan deteksi yang lebih cepat, respons yang lebih cepat, dan pengembalian investasi (ROI) yang lebih besar dari investasi keamanan Anda yang ada.

FAKTA & ANGKA

- Memantau **204K** kluster aktor ancaman real-time dan terus berkembang
- Mengurangi tingkat positif palsu menjadi **0,0002%**
- Memblokir **82%** ancaman sebelum kueri pertama
- Memberikan perlindungan **68.4** hari sebelum serangan rata-rata
- Memblokir **5X lebih banyak** domain berisiko tinggi/berisiko menengah dibandingkan dengan alat yang hanya mencari perilaku berbahaya yang diketahui
- Menghemat rata-rata **500 jam analis SOC** per bulan*
- Membantu mewujudkan **$400 ribu** dalam penghematan produktivitas per tahun*
- Mengurangi puluhan ribu peringatan menjadi hanya beberapa saja*

Survei SOC SANS 2025 mengungkapkan bahwa tujuh dari 10 hambatan utama yang menghalangi pemanfaatan SOC sepenuhnya melibatkan peringatan, integrasi alat, dan kekurangan keterampilan.

*Berdasarkan data pelanggan dunia nyata.

BLOKIR ANCAMAN SEBELUM BERDAMPAK

Infoblox Threat Defense menerapkan intelijen ancaman DNS prediktif dengan analisis algoritmik/pembelajaran mesin pada lalu lintas DNS waktu nyata untuk memblokir aktivitas ancaman sebelum memengaruhi jaringan Anda, sering kali mendeteksi ancaman yang tidak terdeteksi oleh alat lain. Dengan menghentikan ancaman pada lapisan DNS, Infoblox juga membantu mengurangi volume dan beban kerja peringatan pada alat keamanan hilir, dengan pelanggan melaporkan pengurangan hingga 50 persen dalam peringatan pada firewall generasi berikutnya (NGFW) dan sistem deteksi dan respons titik akhir (EDR).

> *"DNS yang aman dapat mengurangi kemampuan 92% serangan malware untuk berhasil menyebarkan malware pada jaringan tertentu."*
>
> **Anne Neuberger,**
> **Direktur Keamanan Siber Direktorat,**
> **National Security Agency (NSA)**

Kemampuan Utama	Deskripsi	Infoblox Threat Defense	NGFW	SASE	EDR
Resolver Aman di Seluruh Perusahaan dan Pencatatan Log Kueri DNS	Menggunakan data kueri DNS untuk menemukan dan menghukum domain-domain	●	◑	◑	◑
Pemantauan Perilaku DNS Secara Menyeluruh	Memantau semua jenis catatan DNS untuk aktivitas berbahaya	●	●	◔	○
Deteksi dan Penghapusan Domain Mirip/Doppleganger	Mengurangi permukaan serangan lookalike/doppleganger	●	○	◑	○
Perlindungan DNS Zero Day	Mengidentifikasi domain baru atau yang sedang muncul untuk organisasi Anda yang dapat menimbulkan ancaman	●	◑	◑	○
Deteksi Tunneling DNS Berbasis Perilaku	Mendeteksi terowongan DNS yang digunakan untuk eksfiltrasi/infiltrasi data, komunikasi C2, dan lain-lain.	●	◑	◑	○
Proaktif Perlindungan Domain Mencurigakan/ Berisiko Tinggi	Mengidentifikasi dan memblokir domain mencurigakan secara preemptif yang kemungkinan akan digunakan dalam kampanye jahat di masa depan	●	◑	◑	◑
Pengayaan Konteks Otomatis dan Asli	Menghubungkan konteks jaringan tanpa memerlukan klien atau sinkholing (pengguna, perangkat, IP Sumber, lokasi, alamat MAC, VLAN)	●	◑	◑	◑
Deteksi dan Penghentian Sistem Distribusi Ancaman (TDS) Proaktif	Mengidentifikasi infrastruktur TDS aktor ancaman, bukan hanya domain individu, untuk melawan aktor ancaman yang berpindah-pindah di berbagai domain untuk menghindari deteksi	●	◔	○	○

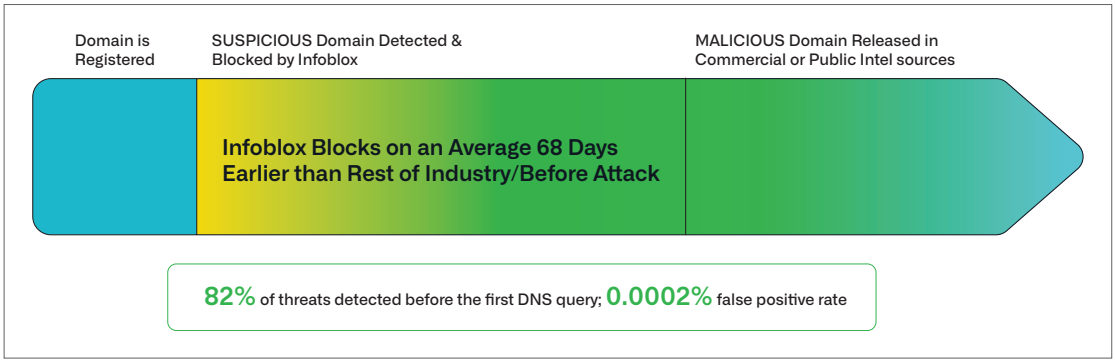
Gambar 1. Kemampuan unik untuk Threat Defense yang tidak dapat sepenuhnya diatasi oleh alat lain

FITUR UTAMA DARI THREAT DEFENSE

- **Monitor "Protection Before Impact".** Memungkinkan CISO dan tim keamanan untuk menjalankan strategi keamanan preemptif mereka dan dengan percaya diri melaporkan kepada dewan dengan metrik yang jelas dan terukur tentang ancaman yang dinetralkan sebelum dampak—mendapatkan keuntungan waktu kritis dan mengurangi beban pada pusat operasi keamanan (SOC).
- **Penemuan dan Integrasi Inventaris Aset.** Identifikasi cepat aset yang terlibat dalam insiden keamanan untuk penilaian dan respons insiden yang lebih cepat.
- **Ruang Kerja Keamanan.** Antarmuka pengguna yang disederhanakan dan intuitif yang memungkinkan tim keamanan memahami apa yang terjadi di lingkungan mereka dan menyarankan cara untuk mengurangi risiko keamanan.
- **Mode Deteksi.** Untuk penerapan yang mudah dan pembuktian konsep tanpa mengubah infrastruktur TI atau jaringan yang ada.

TINGKATKAN KEAMANAN PREEMPTIF DENGAN INTELIJEN PREDIKTIF

Infoblox adalah pencipta terkemuka intelijen ancaman DNS orisinal. Perusahaan mengambil pendekatan preemptif, bukan hanya defensif, dengan menggunakan wawasannya untuk melacak infrastruktur pelaku ancaman saat sedang dibangun dan mengganggu kejahatan dunia maya di sumbernya, sering kali sebelum serangan diluncurkan.



Gambar 2. Infoblox threat intelligence dapat melindungi dari ancaman sebelum industri keamanan lainnya

Bagaimana Infoblox Menciptakan Original DNS Threat Intelligence

Pakar DNS: Infoblox menemukan aktor ancaman yang bersembunyi di DNS dengan mengetahui di mana harus mencari. Dimulai dengan domain berisiko tinggi atau mencurigakan, tim menghubungkan titik-titik untuk mengidentifikasi infrastruktur penyerang dan melacaknya saat berkembang dan memunculkan ancaman baru, sebelum mereka dikenali di tempat lain.

Keahlian Ancaman: Infoblox memahami cara kerja aktor jahat dan bagaimana ancaman seperti malware, ransomware, phishing, dan eksploitasi berbasis DNS muncul. Keahlian tersebut menggerakkan sistem prediktif yang mendeteksi domain mirip, aktivitas DNS command-and-control (C2), registered domain generation algorithms (RDGAs), dan perilaku mencurigakan lainnya.

Ilmu Data: Infoblox menerapkan pembelajaran mesin dan ilmu data canggih pada volume besar data kueri DNS. Ini memungkinkan perlindungan hampir waktu nyata terhadap eksfiltrasi data, algoritma pembuatan domain (DGAs), dan berbagai ancaman evasif.

BEKERJA LEBIH CERDAS DENGAN SOC INSIGHTS

Dari kelelahan peringatan dan kelelahan analis hingga upaya investigasi dan respons yang panjang, Infoblox Threat Defense menawarkan bantuan signifikan kepada SOC, dengan paket SOC Insights tambahan.

- Bantu analis mengetahui apa yang paling penting dengan analitik berbasis AI yang menyaring ratusan ribu peringatan menjadi beberapa wawasan.
- Otomatiskan pengumpulan dan korelasi log, intelijen ancaman, dan pengumpulan data lainnya sehingga analis dapat segera memulai investigasi dan respons.
- Mempercepat respons insiden dengan penemuan aset dan integrasi inventaris, membantu para analis mengidentifikasi perangkat yang terkena dampak lebih cepat.

Gambar 3. Infoblox Threat Intel membagikan data penelitian yang mengejutkan tentang meningkatnya risiko domain Lookalike

EKSPOR LOG DNS BERNILAI TINGGI DALAM SKALA BESAR

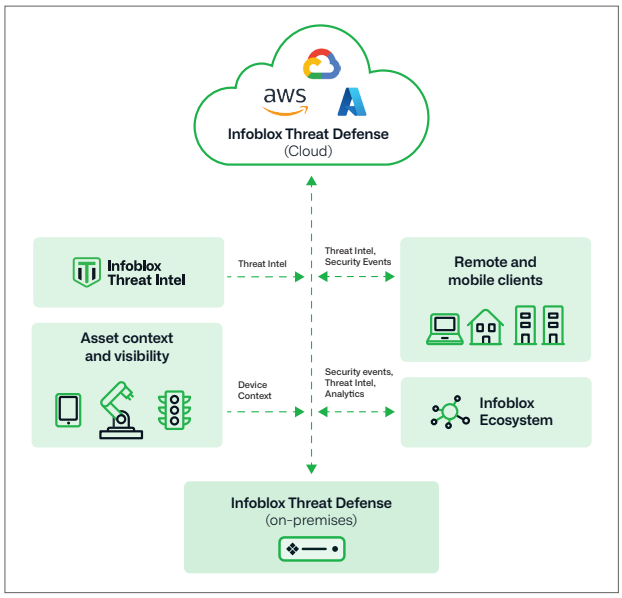
Infoblox memudahkan pengiriman kueri DNS berkualitas tinggi dan data peristiwa ke SIEM, SOAR, atau data lake Anda untuk visibilitas terpusat dan korelasi ancaman yang lebih cepat.

- Saring dan teruskan hanya peristiwa DNS bernilai tinggi untuk mengurangi biaya penyerapan SIEM dan kebisingan peringatan.
- Alirkan log DNS yang diperkaya secara real-time menggunakan Infoblox Cloud Data Connector.
- Tingkatkan deteksi dan respons di seluruh ekosistem Anda dengan memberikan setiap alat konteks yang diperlukan.
- Bagikan data dengan mulus dengan alat lain melalui integrasi dua arah yang tersertifikasi—meningkatkan deteksi, triase, dan respons ujung ke ujung.

MENYELIDIKI LEBIH CEPAT DENGAN BERKAS

Dossier melengkapi para analis dengan alat penelitian terpadu yang kuat untuk memvalidasi ancaman, berfokus pada indikator kompromi (IOC), dan mempercepat penyelidikan—tanpa perlu beralih di antara platform yang berbeda.

- Konsolidasikan intelijen ancaman internal, Infoblox, dan pihak ketiga ke dalam satu antarmuka yang intuitif.
- Segera selidiki IOC dan ungkap ancaman terkait dengan pengayaan bawaan dan analisis tautan.
- Kurangi waktu investigasi hingga 67 persen dengan menghilangkan pengumpulan data manual dan peralihan konteks.



Gambar 4. Arsitektur hibrida Infoblox memungkinkan perlindungan di mana saja dan penerapan di mana saja untuk melawan lanskap ancaman berkemampuan AI saat ini.

LINDUNGI MEREK ANDA DARI PENIPUAN YANG DITARGETKAN

Infoblox menawarkan dua kemampuan terintegrasi — Pemantauan Domain Mirip dan Layanan Mitigasi Domain — yang membantu melindungi merek, pelanggan, dan karyawan Anda dari serangan siber berbasis penipuan. Bersama-sama, mereka memberikan Anda visibilitas terhadap ancaman yang muncul dan kemampuan untuk mengambil tindakan cepat dan efektif terhadap domain berbahaya sebelum berdampak pada bisnis Anda.

Pemantauan Domain Mirip

Tetap waspada terhadap serangan peniruan identitas yang mengeksploitasi merek Anda atau pihak ketiga yang tepercaya.

- Deteksi domain yang terdaftar untuk menyamar sebagai perusahaan Anda, rantai pasokan, atau properti yang berhubungan dengan pelanggan.
- Identifikasi domain yang digunakan dalam kampanye phishing dan penipuan yang menargetkan karyawan atau pelanggan Anda.
- Pantau domain prioritas tinggi untuk perubahan dalam postur risiko dan terima peringatan secara real-time.

Layanan Mitigasi Domain

Segera memvalidasi dan menonaktifkan domain berbahaya yang aktif di jaringan.

- Konfirmasikan dan dokumentasikan aktivitas berbahaya melalui validasi insiden yang dipimpin oleh manusia dan pelaporan ringkasan.
- Bekerja sama dengan ISP global, penyedia hosting, dan badan pengatur untuk penghapusan cepat—seringkali dalam waktu 24 jam.
- Pantau ancaman yang telah diatasi selama 30 hari setelah penghapusan untuk mendeteksi dan menghapus upaya pengaktifan kembali tanpa biaya tambahan.
- Menangani berbagai jenis ancaman termasuk phishing, hosting malware, infrastruktur C2, dan data yang dicuri.

Untuk mempelajari lebih lanjut cara Infoblox Threat Defense mengamankan data dan infrastruktur Anda, silakan kunjungi https://www.infoblox.com/products/threat-defense/.

Infoblox menyatukan jaringan dan keamanan untuk memberikan kinerja dan perlindungan yang tak tertandingi. Dipercaya oleh perusahaan-perusahaan Fortune 100 dan para inovator baru, kami memberikan visibilitas dan kontrol real-time atas siapa dan apa saja yang terhubung ke jaringan Anda, sehingga organisasi Anda dapat berjalan lebih cepat dan menghentikan ancaman lebih awal.

Kantor Pusat Perusahaan
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Versi: 20250121v1