LEMBAR DATA

BloxOne® Threat Defense Advanced

Memperkuat dan mengoptimalkan postur keamanan Anda dari dasar

KEBUTUHAN KEAMANAN DASAR SESUAI SKALA

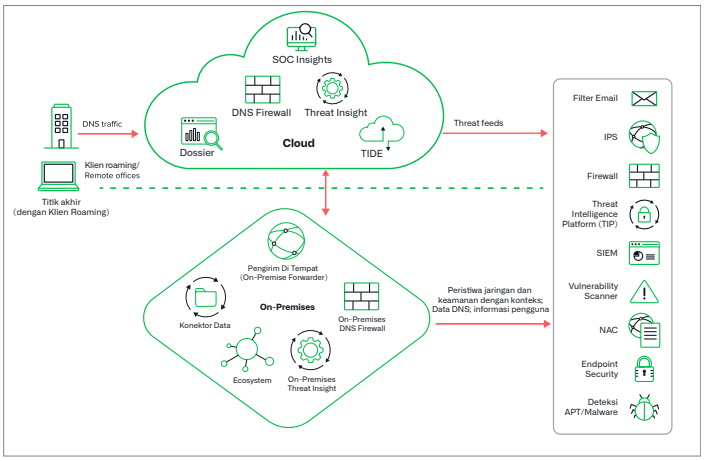
Model keamanan tradisional tidak memadai dalam dunia transformasi digital saat ini.

- Perimeter telah bergeser, dan pengguna Anda secara langsung mengakses aplikasi berbasis cloud dari mana saja.
- IoT menyebabkan ledakan perangkat yang tidak menerima teknologi titik akhir tradisional untuk perlindungan.
- Sebagian besar sistem keamanan bersifat kompleks dan tidak mudah ditingkatkan ke tingkat yang diperlukan untuk melindungi lingkungan yang dinamis ini.

Yang dibutuhkan oleh organisasi adalah solusi keamanan yang dapat diskalakan, sederhana, dan otomatis yang melindungi seluruh jaringan tanpa perlu menggunakan atau mengelola infrastruktur tambahan.

INFOBLOX MENYEDIAKAN PLATFORM YANG DAPAT DISKALAKAN YANG MEMAKSIMALKAN INVESTASI PERTAHANAN ANCAMAN YANG ADA

Infoblox BloxOne Threat Defense Advanced, solusi DNS Detection and Response (DNSDR) yang komprehensif, mendeteksi aktivitas ancaman yang terlewatkan oleh solusi lain dan menghentikan serangan sebelum terjadi dengan intelijen ancaman DNS pra-kampanye yang diburu untuk mengganggu rantai pasokan penyerang. Integrasi dan otomatisasi ekosistem yang cerdas mengurangi upaya manual, sementara keunikan Infoblox Analisis berbasis AI memfokuskan analis pada hal-hal yang paling penting dan memberikan wawasan yang mengurangi MTTR, meningkatkan ROI alat keamanan yang ada, dan meningkatkan efisiensi SecOps secara keseluruhan.



Gambar 1: Arsitektur hibrida Infoblox memungkinkan perlindungan di mana saja dan penerapan di mana saja

KEMAMPUAN UTAMA

- Mendeteksi dan memblokir eksploitasi, phishing, ransomware, dan malware modern lainnya yang terlewatkan oleh solusi lain
- Melindungi pengguna dan perangkat, apa pun platform atau OS-nya, pada lapisan DNS, termasuk BYOD, IoT, dan ICS
- Menemukan aplikasi berisiko tinggi dan mengelola Shadow IT, Insider, Compliance, dan risiko lainnya
- Mencegah teknik penyaringan data dengan pembelajaran mesin/ analisis AI, termasuk DNS-eksfiltrasi data berbasis, DGA, dan DNSMessenger
- Membatasi akses pengguna ke konten web yang tidak sesuai atau tidak diinginkan dan melacak aktivitas
- Melindungi merek Anda dengan Pemantauan Domain Lookalike untuk properti internet Anda yang paling berharga
- Mempercepat investigasi 3X lipat dan merampingkan respons ancaman dan aktivitas threat-hunting
- Meningkatkan visibilitas: Dapatkan visibilitas yang tepat "dan konteks jaringan yang kaya" dengan mengintegrasikan dengan metadata aset IPAM untuk pemahaman dan korelasi peristiwa yang optimal
- SOC Insights memungkinkan Anda memulai penyelidikan dan respons terhadap ancaman yang paling penting dan mengurangi MTTR dengan AI-Driven Insights

MAKSIMALKAN EFISIENSI PUSAT OPERASI KEAMANAN

Mengurangi Waktu Respons Insiden

- Secara otomatis memblokir aktivitas malicious dan memberikan data ancaman ke seluruh ekosistem keamanan Anda untuk penyelidikan, karantina, dan remediasi
- Optimalkan solusi SOAR Anda menggunakan jaringan kontekstual dan data intelijen ancaman, dan integrasi ekosistem Infoblox (enabler penting bagi SOAR) - kurangi waktu respons ancaman dan OPEX
- Gunakan kemampuan Infoblox SOC Insights untuk mengetahui peristiwa mana yang paling penting dengan analitik berbasis AI yang melampaui dasbor peringkat risiko malware sederhana

Menyatukan Kebijakan Keamanan dengan Portabilitas Intel Ancaman

- Mengumpulkan dan mengelola data intelijen ancaman dari sumber internal dan eksternal dan mendistribusikannya ke sistem keamanan yang ada
- Mengurangi biaya umpan ancaman sekaligus meningkatkan efektivitas intel ancaman di seluruh tumpukan keamanan

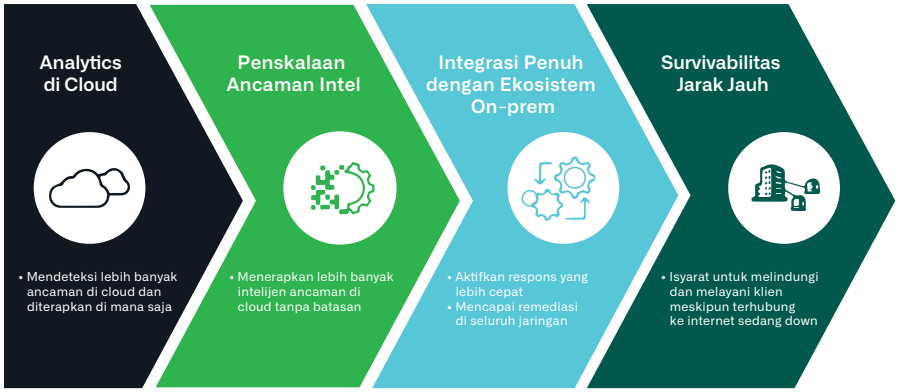
Investigasi dan Perburuan Ancaman Lebih Cepat

- Memulai investigasi dan respons terhadap ancaman yang paling penting dan mengurangi MTTR dengan wawasan berbasis AI yang melampaui dasbor peringkat risiko malware sederhana
- Membuat tim analis ancaman Anda **3x lebih produktif** dengan memberdayakan analis keamanan dengan investigasi ancaman otomatis, wawasan tentang ancaman terkait, dan perspektif penelitian tambahan dari sumber-sumber siber ahli untuk mengambil keputusan yang cepat dan akurat tentang ancaman

Gambar 2: BloxOne Threat Defense terintegrasi dengan seluruh ekosistem keamanan siber

> *"Di zaman sekarang ini, ada terlalu banyak hal ransomware, spyware, dan adware yang masuk melalui tautan yang dibuka oleh pengguna Internet. Solusi keamanan cloud Infoblox membantu memblokir pengguna dari pengalihan yang membawa mereka ke situs-situs yang tidak baik, menjaga agar mesin tidak terinfeksi, dan membuat pengguna lebih aman."*
>
> **Senior System Administrator and Network Engineer**
> **City University of Seattle**

PENDEKATAN HYBRID MELINDUNGI DI MANA SAJA ANDA DIKERJAKAN



Analisis di Cloud

- Memanfaatkan kemampuan pemrosesan yang lebih besar dari cloud untuk mendeteksi ancaman yang lebih luas, termasuk eksfiltrasi data, algoritme pembuatan domain (DGA), fluks cepat, malware tanpa berkas, DGA Kamus, dan lainnya menggunakan analitik berbasis pembelajaran mesin
- Mendeteksi ancaman di cloud dan menerapkannya di mana saja untuk melindungi kantor pusat, pusat data, kantor jarak jauh, atau perangkat roaming

Penskalaan Inteligensi Ancaman

- Menerapkan intelijen komprehensif dari penelitian Infoblox dan penyedia pihak ketiga untuk menegakkan kebijakan di tempat atau di cloud dan secara otomatis mendistribusikannya ke seluruh infrastruktur keamanan
- Menerapkan lebih banyak intelijen ancaman di cloud tanpa investasi besar ke lebih banyak peralatan keamanan untuk setiap situs

Integrasi yang kuat dengan ekosistem keamanan Anda

- Memungkinkan integrasi penuh dengan on-premises Infoblox dan teknologi keamanan pihak ketiga, memungkinkan remediasi di seluruh jaringan dan meningkatkan ROI dari teknologi tersebut

Kemampuan bertahan/ketahanan jarak jauh

- Jika terjadi gangguan pada konektivitas Internet Anda, on-premises Infoblox dapat terus mengamankan jaringan

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

ROI DARI KEAMANAN INFOBLOX

Membongkar perangkat keamanan yang tegang

- Mengurangi beban pada tegang perangkat keamanan perimeter seperti firewall, IPS, dan proxy web dengan menggunakan server DNS Anda yang sudah tersedia sebagai garis pertahanan pertama
- **Pengurangan lalu lintas hingga 60 kali lipat** dikirim ke NGFWs*.

Tingkatkan ROI pada investasi yang ada

- Dapatkan nilai lebih dari berdekatan/produk pelengkap oleh berbagi informasi ancaman dan penyerang secara dua arah
- Jika mengirim data DNS ke SIEM, kurangi biaya solusi SIEM dengan hanya mengirim data DNS yang mencurigakan ke platform ini

Otomatisasi

- Kurangi biaya sentuhan/kesalahan manusia menggunakan otomatisasi
- Mengatasi kekurangan sumber daya terampil - 60% lebih sedikit permintaan pada tim Anda untuk mengimplementasikan (mengonfigurasi dalam hitungan jam, bukan bulan) dan mengoperasikan untuk keterampilan dan biaya
- Jadikan analis ancaman Anda 3x lebih produktif dengan konsol tunggal yang mudah digunakan untuk intelijen ancaman yang mendalam

Berdasarkan data pelanggan nyata

infoblox.

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: 20240122v1