Resume
Securing your Remote Workforce with Forescout

Kontrol Akses Jaringan

Pertumbuhan eksplosif dalam perangkat dan tipe perangkat terus berlanjut. Banyak yang tidak dapat dilihat atau dikelola oleh metode berbasis agen atau alat NAC tradisional, yang memungkinkan perangkat yang tidak sah mengakses jaringan Anda dan menyelidiki kerentanan. Kendalikan dengan platform visibilitas yang dapat melihat setiap jenis perangkat di jaringan dan menegakkan kebijakan Anda.

Solusi ForeScout Platform ForeScout menawarkan kemampuan NAC yang komprehensif dan lebih banyak lagi, berdasarkan visibilitas waktu nyata dari perangkat saat mereka mengakses jaringan — terlepas dari di mana jaringan itu berada dalam perusahaan besar Anda. Ini terus-menerus memindai jaringan dan memonitor aktivitas perangkat yang diketahui, milik perusahaan serta perangkat yang tidak dikenal seperti milik pribadi dan titik akhir yang jahat. Dan itu memungkinkan Anda mengotomatisasi dan menegakkan kontrol akses jaringan berbasis kebijakan, kepatuhan titik akhir dan keamanan perangkat seluler. Sebagian besar perangkat IoT dan PL di jaringan Anda tidak termasuk — atau tidak bisa menangani — agen perangkat lunak. Itulah sebabnya platform ForeScout menawarkan teknologi penemuan tanpa agen dan teknik pemantauan pasif untuk menghindari gangguan bisnis. Ini juga menyediakan serangkaian luas kontrol otomatis yang menjaga pengalaman pengguna dan menjaga operasi bisnis berjalan semaksimal mungkin. Landasan intelijen platform dan fungsionalitas ForeScout dapat diringkas dalam tiga kata.

1. Lihat penemuan dan pembuatan profil tanpa agen menawarkan kemampuan unik untuk mengidentifikasi perangkat begitu mereka terhubung ke jaringan Anda, tanpamembutuhkan agen perangkat lunak atau pengetahuan perangkat sebelumnya. Platform ForeScout profil dan mengklasifikasikan perangkat, pengguna, aplikasi dan sistem operasi sambil terus memonitor perangkat yang dikelola, titik akhir virtual, beban kerja cloud, perangkat milik pribadi dan sistem lainnya. Ia bahkan dapat mengetahui apakah IoT dan perangkat lain menggunakan standar pabrik dan kredensial yang biasa digunakan yang dapat dengan mudah diretas.
2. Kontrol Setelah Anda memahami postur kepatuhan setiap perangkat, Anda memerlukan cara otomatis untuk mengizinkan, menolak atau membatasi akses jaringan berdasarkan kebijakan keamanan Anda. Karena platform ForeScout terintegrasi dengan switch kabel / nirkabel, konsentrator VPN, sistem manajemen berbasis cloud, dan firewall generasi baru, platform ForeScout dapat secara dinamis menetapkan perangkat ke segmen jaringan — menggunakan konteks perangkat waktu nyata — untuk mengatasi perubahan perilaku perangkat, keamanan postur atau modifikasi jaringan. Dengan menilai dan memulihkan titik akhir berbahaya atau berisiko tinggi, platform ForeScout mengurangi ancaman pelanggaran data dan serangan malware yang jika tidak akan membahayakan organisasi Anda. Selain itu, dengan terus memantau perangkat di jaringan Anda dan mengendalikannya sesuai dengan kebijakan keamanan Anda, platform ForeScout merampingkan kemampuan Anda untuk menunjukkan kepatuhan terhadap mandat dan peraturan industri.

3. Orkestrasi Platform ForeScout terintegrasi dengan lebih dari 70 produk jaringan, keamanan, mobilitas, dan manajemen TI * melalui ForeScout Base dan Extended Module. Kemampuan ini untuk berbagi intelijen keamanan real-time di seluruh sistem dan menegakkan kebijakan keamanan jaringan terpadu mengurangi jendela kerentanan dengan mengotomatiskan respons ancaman seluruh sistem. Terlebih lagi, ini memungkinkan Anda mendapatkan ROI lebih tinggi dari alat keamanan yang ada sambil menghemat waktu melalui otomatisasi alur kerja.

Platform ForeScout mengumpulkan wawasan kontekstual yang kaya mengenai titik akhir, lokasinya, siapa yang memilikinya dan apa yang ada di dalamnya. Itu dapat memastikan:

- Perangkat yang tidak diotorisasi dan aplikasi yang tidak disetujui tidak ada di jaringan Anda
- Perangkat resmi dikonfigurasikan dengan sistem operasi terbaru, perangkat lunak antivirus terbaru diinstal dan dijalankan, dan kerentanan ditambal dengan benar
- Enkripsi dan agen pencegahan kehilangan data bekerja
- Pengguna dicegah menjalankan aplikasi yang tidak sah atau perangkat periferal di jaringan

Ketika titik akhir tidak memenuhi standar organisasi, platform ForeScout secara otomatis memulai satu atau lebih tindakan penegakan dan perbaikan berbasis kebijakan mulai dari pemberitahuan email tentang ketidakpatuhan hingga perbaikan wajib (seperti pembaruan perangkat lunak) hingga karantina langsung atau pencegahan akses. Tidak perlu adanya intervensi manusia atau kerja manual yang terkait dengan mengelola akses tamu, menemukan sistem, dan membuka atau menutup port jaringan. Akses jaringan dikendalikan sesuai dengan kebijakan. Untuk lebih dari 2.900 perusahaan di lebih dari 80 negara, * ForeScout menyediakan kontrol akses jaringan yang cerdas dan hemat biaya yang memenuhi standar tertinggi untuk keamanan dan kepatuhan terhadap peraturan serta kemudahan penggunaan dan penyebaran. Platform ForeScout dijual sebagai alat virtual atau fisik yang digunakan dalam infrastruktur Anda yang ada dan biasanya tidak memerlukan perubahan pada konfigurasi jaringan Anda. Ini menginstal out-of-band, menghindari latensi atau masalah yang terkait dengan potensi kegagalan jaringan, dan dapat dikelola secara terpusat untuk secara dinamis mengelola hingga dua juta titik akhir dari satu konsol Enterprise Manager.

BrightTALK

Certificate of Attendance

This is to certify that:

Ilham Eka Putra

Mahasiswa, Universitas Sriwijaya

Viewed:

Securing Your Remote Workforce with Forescout

On: April 26, 2020
For: 1 of 34 minutes

Presented by:

Eduard Serkowitsch, Principal Systems Engineer & Jan Hof, EMEA Marketing Director, Forescout Technologies

April 26, 2020
Date

www.brighttalk.com/webcast/13811/399281
Content link