



Pertimbangan TI untuk merancang sistem video IP

Sembilan masalah krusial TI saat merancang sistem video IP

Daftar Isi

Pendahuluan	3
1. Peran keahlian TI dalam sistem video	4
2. Menyesuaikan peralatan untuk memenuhi kebutuhan kamera pengawas.....	5
3. Peran krusial jaringan.....	6
4. Mengutamakan nilai di atas harga	7
5. Ancaman dan perbaikan keamanan siber	7
6. Keterbatasan pendekatan “air-gap”	8
7. Memastikan tidak ada data video yang hilang	9
8. Mengelola siklus hidup sistem pengawasan IP	10
9. Ekosistem TI dalam sistem video	10

Alcatel-Lucent Enterprise menugaskan SourceSecurity.com untuk membuat dokumen ini.



Pendahuluan

Sistem kamera pengawas memiliki kebutuhan khusus dalam hal teknologi informasi (TI). Meskipun sistem video digital mungkin menggunakan teknologi yang sama dengan sistem TI lainnya, konfigurasinya berbeda dengan mempertimbangkan kebutuhan khusus kamera pengawas.

Video adalah bidang yang lebih menuntut dan memberikan beban kerja yang lebih berat pada setiap bagian sistem TI. Mengingat tekanan tersebut, dan terutama dalam kasus sistem perusahaan yang lebih besar, banyak hal bisa saja mulai rusak. Memilih peralatan yang tepat untuk tugas ini akan menjamin keandalan yang lebih besar seiring waktu.

Alcatel-Lucent Enterprise bekerja sama dengan pakar industri SourceSecurity.com dan Stone Security untuk mengidentifikasi sembilan masalah krusial TI ketika merancang sistem video IP. Dalam White Paper ini, kami mengeksplorasi bagaimana kebutuhan khusus sistem kamera pengawas berdampak pada teknologi TI yang diterapkan dan cara penggunaannya.

White Paper

Sembilan masalah krusial TI saat merancang sistem video IP



1. Peran keahlian TI dalam sistem video

Merancang dan membuat sistem kamera pengawas berbasis Internet Protocol (IP) memerlukan keahlian TI tingkat tinggi dalam komunitas integrator.

Sejumlah integrator memiliki keterampilan yang mumpuni untuk meluncurkan sistem video IP secara ahli, sedangkan yang lain mungkin kesulitan.

Pelatihan dan sertifikasi tambahan yang familiar bagi sebagian besar masyarakat dunia TI dapat memungkinkan integrator memberikan layanan berlevel tinggi yang dibutuhkan. Sejak dimulai, installer harus memiliki bakat yang tepat dan pemahaman dasar tentang jaringan dan keterampilan *troubleshooting*.

Integrator dapat memastikan tenaga kerja berpengetahuan luas dengan membatasi pilihan teknologi mereka dan memastikan setiap karyawan terlatih dengan baik dalam teknologi tersebut. Memilih solusi terbaik di bidangnya dan memastikan karyawan ahli dalam produk tersebut memungkinkan integrator memberikan sistem dengan kualitas lebih tinggi kepada pelanggan.

Membatasi jenis produk juga memungkinkan integrator untuk lebih memahami luasnya fitur yang ditawarkan oleh produk tertentu. Seringkali, pelanggan membeli sistem yang menawarkan berbagai fitur dan kemudian hanya menggunakan beberapa fitur saja dalam pengoperasian sehari-hari, sehingga menurunkan nilai dari sistem yang mereka bayar.

Integrator dapat membantu pelanggan dengan mengedukasikan cara mendapatkan manfaat penuh dari setiap sistem yang mereka beli.

Integrator mungkin juga mengandalkan layanan pra-konsultasi dari produsen peralatan untuk memandu mereka. Dalam sejumlah kasus, produsen peralatan memiliki pengetahuan khusus tentang berbagai pasar vertikal, berdasarkan dari pengalaman dan sejarah produsen melayani pasar tersebut.

Produsen yang serius dengan pasar industri tertentu akan mempekerjakan pakar industri untuk memastikan dukungan tertentu untuk setiap kebutuhan pelanggan. Panduan mereka dapat membantu integrator agar berhasil di pasar baru dan/atau menyederhanakan praktik terbaik di pasar tempat mereka beroperasi.

Produsen juga memberikan pelatihan dan sertifikasi untuk memastikan integrator memiliki bakat yang mumpuni untuk menginstal sistem mereka. Pelatihan yang efisien dan substantif harus diberikan dalam sesi yang singkat dengan memperhatikan ketersediaan waktu setiap peserta.

2. Menyesuaikan peralatan untuk memenuhi kebutuhan kamera pengawas

Masalah seperti bandwidth dan persyaratan *Power over Ethernet* (PoE) merupakan variabel penting dalam sistem video. Dan server video memiliki beban yang lebih berat, terutama jika menyangkut video dari live feed. Setiap bit data bahkan yang direkam pun akan masuk ke server.

Buffer video dipastikan setidaknya ada beberapa detik video yang dapat disimpan sebelum rekaman video memicu alarm yang sebenarnya. Periode buffering yang lebih lama mungkin diperlukan ketika mengidentifikasi gambar yang ditangkap dari jarak jauh. Semua input dan output melewati server, meskipun hanya sejumlah data terbatas yang akan dicatat ke penyimpanan jangka panjang.

Ada perbedaan mendasar antara cara integrator sistem keamanan dan profesional TI dalam melihat ukuran sistem. Integrator sistem lebih cenderung berfokus dalam hal jumlah kamera, sementara profesional TI lebih cenderung berfokus dalam hal pengelolaan data dari sistem. Tentunya, keduanya terkait secara intrinsik, tetapi hubungannya tidak linier. Secara umum, jumlah kamera yang lebih banyak berarti lebih banyak data yang harus dikelola oleh departemen TI. Namun, ada faktor lain yang memengaruhi kebutuhan data, seperti jumlah frame, persyaratan kualitas gambar, kebutuhan penyimpanan, aplikasi siang/malam dan penggunaan analitika video.

Keterampilan utama ketika menentukan spesifikasi sistem keamanan IP adalah menerjemahkan persyaratan peralatan dan fungsionalitas sistem menjadi data yang diperlukan untuk memenuhi kebutuhan tersebut. Untuk sistem on-premise atau lokal, hal ini setara dengan kebutuhan untuk menentukan server komputer yang memaksimalkan kinerja sistem sekaligus menurunkan biaya. Permasalahan seperti virtualisasi dan sistem *cloud* bisa saja mempersulit proses ini sekaligus memberikan fleksibilitas baru.

Variabel lain yang terkait dengan desain sistem adalah penggunaan kamera di tepi jaringan untuk merekam video menggunakan kartu SD. Bahkan kini ada sistem “tanpa server”; misalnya, semua perekaman dilakukan di tepi jaringan. Pendekatan seperti itu pada dasarnya memindahkan beban komputasi dari server ke tepi, sehingga mengurangi kebutuhan akan kapasitas server. Kamera masa kini menyediakan data di luar saluran video, seperti metadata dan audio, yang juga memengaruhi desain sistem.

Profesional TI harus memiliki gambaran menyeluruh tentang kesesuaian sistem, seperti apa yang akan dihubungkan, kecepatan frame, resolusi dan codec video kamera. Dengan informasi ini, mereka dapat menghitung kebutuhan jaringan, daya, server, kapasitas disk, memori, penyimpanan dan menentukan penggunaan sistem *cloud* atau lokal. Hal ini memastikan pendekatan desain dan penerapan yang menyeluruh dan matang.

Produsen menyediakan “kalkulator” perangkat lunak untuk membantu integrator merancang sistem dengan menerjemahkan persyaratan sistem ke dalam spesifikasi peralatan tertentu. Perlu diingat bahwa perhitungan harus memenuhi atau melampaui ekspektasi dan memungkinkan untuk perkembangan di masa depan.

Penerapan sistem *cloud* menjadi variabel lain dalam perancangan sistem kamera pengawas. Tren umumnya yaitu penggunaan lebih banyak sistem *cloud* untuk kamera pengawas. Namun, pemilihan solusi *cloud* versus solusi lokal harus dilakukan berdasarkan kasusnya. Perancang sistem dan *end users* harus menolak *cloud* yang terlihat mutlak, dan lebih memilih mengambil keputusan berdasarkan kebutuhan pelanggan.

Banyak produsen berada di bawah tekanan untuk melakukan transisi sistem mereka ke *cloud*, namun sebaiknya juga memberikan pelanggan mereka sejumlah pilihan sistem dan bukan merupakan solusi yang terlalu general.

Produsen memiliki posisi yang baik untuk memberi saran kepada pelanggan mengenai keinginan konfigurasi *cloud* versus sistem desain lokal. Integrator juga harus memahami keuntungan dari kedua pendekatan serta memfasilitasi keputusan pelanggan. Pasar tidak boleh memaksakan aplikasi ke *cloud* kecuali *cloud* menjadi pendekatan yang paling optimal untuk setiap pelanggan.

3. Peran krusial jaringan

Sistem video akan kuat mengikuti tautan terlemahnya. *Switch* jaringan mungkin tidak terlihat jelas seperti kamera dan VMS, namun keduanya sama krusialnya.

Namun, pelanggan seringkali menganggap remeh pengoperasian suatu jaringan, tidak begitu memperhatikan cara kerjanya atau bagaimana memaksimalkan kegunaannya. Bahkan, beberapa pelanggan berniat memasang sistem video menggunakan infrastruktur jaringan yang sudah ada. Hal ini memungkinkan, tetapi kemampuan untuk mengoptimalkan bagian jaringan dari sistem video mungkin jadi terbatas.

Idealnya, pelanggan akan memilih *Switch* terbaik untuk kamera pengawas, yang akan menjamin sistem beroperasi dengan andal dan efektif.

Setiap sistem video itu berbeda, sehingga jika diperhatikan dengan saksama kebutuhan individual sistem akan memastikan tujuan tertentu tercapai. Saat merancang suatu sistem, jaringan tidak boleh dianggap sebagai hal remeh. Justru, jaringan harus dirakit secara hati-hati menggunakan komponen-komponen terbaik untuk memungkinkan dan meningkatkan operasi di keseluruhan sistem.

Switch dengan kinerja “kecepatan kabel”, yang berarti memiliki daya pemrosesan yang cukup untuk menangani kecepatan *Ethernet* penuh pada ukuran paket minimum, kini menjadi standar umum di industri. Titik pembeda baru di antara *Switch* adalah kemampuan untuk memahami dan mengelola lalu lintasnya.

Switch yang tidak dikelola tersedia di pasar tetapi biasanya tidak digunakan untuk implementasi komersial dan/atau perusahaan. *Switch* ini dirancang untuk jaringan kecil dengan kebutuhan dasar; tanpa pengaturan untuk dikonfigurasi.

Sebaliknya, *Switch* yang dikelola memungkinkan deteksi dan diagnosis masalah kinerja serta memastikan kinerja sistem kamera pengawas yang dapat diandalkan. *Switch* ini memungkinkan pengguna untuk melihat secara terperinci apa yang mungkin menyebabkan masalah dalam sistem dan memberikan pemahaman tentang penjelasan informasi tersebut.

Kelebihan dari *Switch* terkelola, yang sepenuhnya dapat dikonfigurasi, disesuaikan dan menyediakan berbagai data tentang kinerja sistem, dengan jelas akan memberikan nilai lebih selama masa pakai sistem, dengan memberikan wawasan penting ke dalam pengoperasian sistem dan memungkinkan *troubleshooting* yang lebih mudah untuk mengidentifikasi masalah.

Switch harus dirancang untuk memenuhi kebutuhan sistem video IP. Sebagai contoh, dalam kasus *Switch* 16-port, kebutuhannya adalah anggaran daya yang cukup untuk mengoperasikan semua kamera video yang terhubung ke *Switch*. PoE kamera masa kini mengkonsumsi lebih banyak daya dibandingkan generasi sebelumnya. Integrator perlu memahami dengan jelas bahwa *Switch* menyediakan daya yang cukup untuk menangani jumlah kamera dan penambahan di kemudian hari.

“Saat kami menentukan pilihan hardware, kami ingin setiap *Switch* memiliki kemampuan bandwidth, anggaran daya dan merupakan *Switch* terkelola yang menghemat banyak waktu saat *troubleshooting*. *Switch* ini akan menghemat uang kami dan menghemat uang pelanggan. Memang jadi lebih banyak investasi di awal, namun akan terbayar dalam jangka panjang dengan menciptakan sistem yang lebih mudah digunakan.”

**Aaron H. Simpson,
President & CTO, Stone
Security**

4. Mengutamakan nilai di atas harga

Reliabilitas menjadi faktor yang sangat penting dalam kamera pengawas, dan ini dimulai dengan pilihan peralatan.

Memilih komponen dengan kualitas lebih rendah mungkin tampak seperti kebutuhan ekonomi pada awalnya. Namun, dalam jangka panjang, pengoperasian sistem akan terganggu. Kerugian yang harus dihadapi karena memilih operasi yang kurang optimal mungkin tidak terlihat jelas saat merancang suatu sistem, namun seiring waktu akan sangat jelas terasa.

Sebaliknya, memilih peralatan yang lebih baik – meskipun lebih mahal – akan membuahkan hasil yang baik.

Sangat krusial untuk membandingkan biaya (seperti harga peralatan yang lebih baik) dengan risiko ketidakmampuan atau kegagalan sistem. Melakukan pendekatan *total cost of ownership* (TCO) ketika mengevaluasi biaya dan risiko merupakan strategi terbaik. Elemen biaya jangka panjang lainnya yang perlu dipertimbangkan adalah nilai dari sistem terbuka, yang dapat menjamin fleksibilitas ketika memperluas atau mengubah sistem di kemudian hari.

Jalan terbaik tentunya bekerja sama dengan pemasok yang menawarkan produk yang mereka banggakan dan dapat mereka dukung dalam jangka waktu yang lama.

5. Ancaman dan perbaikan keamanan siber

Secara historis, terdapat ironi dalam industri keamanan fisik yaitu kurangnya perhatian terhadap keamanan siber pada sistem IP.

Untungnya, para pemangku kepentingan di bidang keamanan fisik kini lebih memperhatikan masalah keamanan siber di setiap tingkat dan di seluruh rantai pasokan keamanan fisik. Bahkan faktanya, keamanan siber telah menjadi salah satu pilar utama dalam proses pengambilan keputusan untuk sistem keamanan video dalam skala lebih besar.

Langkah minimum untuk melindungi diri dari ancaman dunia maya dan membatasi akses ke sistem adalah dengan menghindari penggunaan kata sandi *default*. Hal ini kurang aman dan mudah ditebak oleh peretas atau bot. Faktanya, kata sandi *default* telah dilarang di California.

Risiko keamanan siber dimulai dari rantai pasokan, di mana serangan dapat membahayakan suatu produk bahkan sebelum produk tersebut dikirimkan. Analisis produk untuk kemungkinan serangan "*backdoor*" atau "*buffer overflow*" sebelum pengiriman dapat mengurangi ancaman tersebut. Pelanggan juga dapat memilih untuk menginstal "*good code*" secara virtual setelah produk perangkat keras dikirimkan, sehingga memastikan keamanan siber serta melakukan overwrite terhadap setiap kode berbahaya yang mungkin diinstal selama pengiriman.

Terdapat juga serangkaian langkah keamanan siber yang harus ditangani selama instalasi dan berbagai tahap implementasi sistem. Misalnya, "*learned port security*" memastikan bahwa *port* hanya diakses oleh perangkat yang diotorisasi. Jika perangkat yang tidak diotorisasi mencoba menyambung ke sistem — misalnya, untuk menyambungkan kamera baru — akan memicu peringatan dan akses ke port ditolak hingga akses diizinkan oleh manusia.

Teknologi *Shortest Path Bridging* (SPB) dapat mencegah aktivitas jahat berpindah dari satu sistem ke sistem lainnya. Aturan ditetapkan sehingga kamera hanya dapat melakukan *streaming* ke perekam, dan teknologi segmentasi canggih lainnya diterapkan pada jaringan multi-IoT.

Sistem harus menonaktifkan protokol yang tidak aman seperti FTP dan Telnet, yang memfasilitasi komunikasi antarm jaringan, namun juga dapat memberikan peluang bagi peretas. Aktivitas ini harus "aman secara *default*" sehingga tidak mengizinkan koneksi ke jaringan kecuali disengaja.

Keamanan siber yang efektif juga memerlukan pembatasan akses fisik ke sistem. Jika *Switch* dipasang di ruang petugas di mana akses fisik dapat dilakukan oleh semua orang, maka *Switch* tersebut tidak terlindungi dengan baik. Membolehkan akses fisik ke suatu sistem akan memudahkan siapa saja — termasuk karyawan yang mungkin menjadi ancaman orang dalam — untuk menyambungkan laptop dan mengakses seluruh sistem.

Kamera harus merekam akses ke peralatan jaringan sebagai pendekatan "pertahanan yang mendalam".



6. Keterbatasan pendekatan “air-gap”

Ketika membahas perlindungan sistem video dari serangan keamanan siber melalui internet, pendekatan yang umum dilakukan selama ini adalah menciptakan sistem *air gap*.

Sistem *air gap* melibatkan isolasi komputer atau jaringan dan mencegahnya menjalin koneksi eksternal. Karena komputer *air gap* secara fisik terpisah dan tidak mampu terhubung secara nirkabel atau fisik dengan komputer atau perangkat jaringan lain, pendekatan ini dipandang sebagai solusi mutlak untuk memastikan keamanan siber dari sistem video.

Namun, akan menjadi proposisi yang berisiko jika hanya bergantung pada sistem *air gap* sebagai satu-satunya perlindungan keamanan siber. Ada berbagai situasi di mana sistem *air gap* mungkin terekspos ke internet, bahkan walau hanya sejenak. Ketika hal ini terjadi, sistem akan bergantung pada langkah-langkah keamanan siber lainnya – jika ada – untuk melindungi diri dari bencana.

Berasumsi bahwa suatu sistem dalam kondisi *air gap* selamanya bukanlah solusi untuk keamanan siber. Sebaliknya, justru menjadi bencana di kemudian hari.

Sistem *air gap* juga tidak dapat memanfaatkan kecerdasan buatan (AI) dan fitur lainnya yang bergantung pada akses banyak pengguna dan analisis pengalaman bersama. Data dari satu pelanggan tidak begitu berguna jika dibandingkan data dari ratusan pelanggan yang tersedia di *cloud*. Sistem *air gap* tidak memungkinkan pelanggan untuk memanfaatkan nilai lebih dari analitika yang lebih cerdas. Menyerahkan sebagian data (dengan pertimbangan privasi) adalah harga yang harus dibayar pelanggan untuk memanfaatkan nilai yang lebih besar.

Dengan mempertimbangkan kebutuhan pelanggan saat ini untuk selalu terhubung dan memiliki akses ke sistem mereka, skenario penggunaan sistem *air gap* menjadi semakin terbatas.

Terdapat kecenderungan dimana organisasi akan menolak prospek pembuatan infrastruktur jaringan yang benar-benar terpisah untuk kamera pengawas. Tidak ada jaringan “terpisah dan aman”.

7. Memastikan tidak ada data video yang hilang

Data yang hilang merupakan masalah serius bagi setiap sistem TI, namun menjadi jauh lebih kritis bagi sistem TI yang menyediakan kamera pengawas. Sistem kamera pengawas sangatlah krusial dan harus beroperasi sepanjang waktu. Tidak ada waktu jeda yang memperbolehkan administrator untuk mendiagnosis dan memecahkan masalah kehilangan data; sebaliknya, masalah tersebut harus ditangani terus-menerus dan secara real-time.

Di sinilah *Switch* terkelola dapat membantu. *Switch* yang dikelola dapat memungkinkan administrator sistem mendiagnosis dan mengatasi masalah kehilangan data dengan cepat. *Switch* ini juga mempermudah identifikasi sumber kehilangan data, sehingga tidak “menuduh” suatu komponen sistem atas kesalahan yang terjadi.

Sejumlah paket data bisa hilang karena data dikonversi dari transmisi serat optik menjadi tembaga dan *Ethernet*. Pemancar listrik digunakan untuk mengubah data dari transmisi serat ke transmisi listrik, dan perangkat tersebut dapat menjadi sumber paket-paket data yang hilang.

Dalam kamera pengawas, hilangnya sebuah paket data berarti kehilangan sebuah gambar video, sehingga data hilang selamanya. Tidak ada cara untuk memulihkan gambar video yang hilang selama gangguan. Misalnya di aplikasi kasino, di mana konsekuensi dari kegagalan sistem video adalah kehilangan liputan di meja permainan yang juga dapat berarti kehilangan pendapatan.

Dalam berbagai implementasi kamera pengawas, redundansi diperlukan untuk memastikan operasi yang terus-menerus setiap saat.

Kebutuhan akan reliabilitas harus dipertimbangkan antara risiko dan manfaatnya. Suatu sistem mungkin lebih murah, lebih sederhana dan/atau kurang toleran terhadap kesalahan, tetapi sistem tersebut mungkin tidak berfungsi seperti yang diinginkan, yang akan menjadi kerugian tersendiri.

Variabel lain yang dapat menyebabkan masalah kinerja dalam sistem video berkaitan dengan perbedaan antara *unicast* dan *multicast*, yang merupakan dua metode untuk mengirimkan data melalui jaringan. *Unicast* menyediakan model komunikasi one-on-one di mana satu pengirim hanya dapat mengirimkan data kepada satu penerima. Sebaliknya, *multicast* adalah model one-to-many di mana satu pengirim dapat mengirimkan data kepada beberapa penerima.

Banyak aplikasi kamera pengawas beroperasi dalam mode *unicast*. Ini berarti kamera dipantau secara real-time oleh seseorang, hanya melibatkan satu saluran video.

Namun, sejumlah aplikasi memerlukan *multicast*, di mana satu saluran video dilihat oleh banyak pengguna. Masalah muncul ketika suatu sistem bertransisi dari *unicast* ke *multicast*. Melakukan transisi tersebut tidak hanya dengan “menekan tombol”, juga nuansa serta detail transisi dapat menyebabkan masalah pada kinerja sistem. Masalah akan muncul jika bagian dari suatu sistem disetel untuk *unicast* padahal seharusnya digunakan secara *multicast* atau sebaliknya. Untuk hal ini, konfigurasi yang tepat di keseluruhan sistem sangatlah penting.

Kemampuan penasihat jaringan yang ahli akan memungkinkan *end user* memahami hal-hal normal dalam kinerja jaringan serta kemudian mendeteksi ketika ada sesuatu yang tidak normal, atau di luar batas ekspektasi pada umumnya. Setiap penyimpangan dilaporkan secara otomatis, dan manusia dapat melakukan intervensi sesuai kebutuhan untuk mengatasi masalah tersebut.



8. Mengelola siklus hidup sistem pengawasan IP

Dalam dunia TI, siklus hidup produk dapat mencapai 3 hingga 10 tahun tergantung pada industri dan produknya. Terdapat protokol untuk mengatasi masalah seperti *meantime between failure* (MTBF), *firmware* dan patch keamanan.

Di bidang kamera pengawas, secara historis siklus hidup produk lebih panjang, ada banyak kamera video berusia puluhan tahun yang masih dapat digunakan di lapangan. Mengadaptasi strategi manajemen TI ke sistem video IP dapat mengungkap ketimpangan yang ada.

Dukungan TI yang disediakan oleh produsen memberikan nilai yang sangat besar bagi integrator dan *end user*. Secara historis, siklus hidup keamanan fisik yang lebih lama menghasilkan sistem untuk terus beroperasi melebihi periode yang diharapkan dan dalam lingkungan yang tidak didukung.

Terdapat risiko permanen jika terus menggunakan peralatan yang tidak didukung oleh produsennya. Misalnya, kegagalan memperbarui *firmware* dapat membuka gerbang terhadap ancaman keamanan siber.

Mayoritas peralatan saat ini memiliki garansi selama lima tahun dan nyatanya dapat terus beroperasi hingga lima tahun berikutnya. Namun, dengan ranah teknologi yang berubah dengan cepat, sebagian besar pelanggan ingin memanfaatkan kemampuan terkini. Dampaknya, percepatan teknologi berarti siklus hidup keamanan yang lebih pendek, sebagaimana yang terjadi di lingkungan TI dan jaringan yang lebih luas.

9. Ekosistem TI dalam sistem video

Ekosistem TI terpadu menjadi pendekatan terbaik untuk memastikan keberhasilan sistem video IP. Keberhasilan setiap teknologi baru bergantung pada ekosistem TI yang mendukungnya. Masalah seperti interoperabilitas perangkat keras dan perangkat lunak akan memastikan kelancaran operasi sistem.

Standar terbuka memastikan fleksibilitas tertinggi bagi pelanggan di masa kini dan masa depan. Penawaran yang disederhanakan juga bermanfaat. Misalnya, [Alcatel-Lucent Enterprise](#) memiliki sistem operasi tunggal yang berfungsi dengan setiap *Switch Ethernet* yang dijual perusahaan ini.

Pertahankan strategi dalam merangkul produk yang “berfungsi baik” di lingkungannya dan dengan produk lain di ekosistemnya untuk memastikan kesuksesan operasional.

Ekosistem TI yang sukses tidak terjadi begitu saja. Nyatanya, hal ini dipupuk oleh kolaborasi dengan mitra industri untuk memastikan kesuksesan. Prinsip-prinsip seperti keterbukaan dan interoperabilitas berkontribusi pada ekosistem TI. Kesuksesan operasional akan meningkatkan kinerja setiap komponen sistem dan sistem secara keseluruhan.

Pelajari lebih lanjut tentang Alcatel-Lucent Enterprise [solusi kamera pengawas](#).