بسمه‌تعالی

محافظت تعریف‌شده نرم‌افزاری (SDP: Software Defined Protection)

(معماری امنیتی نوین مبتنی بر هوش‌مصنوعی)

امروزه چرخ کسب و کار با کمک جریان آزاد اطلاعات می‌چرخد. داده‌ها از میان شبکه‌های ابری و دستگاه‌های تلفن‌همراه می‌گذرند، در میان ایده‌ها شکوفا می‌شوند و در شبکه‌های اجتماعی منتشر می‌گردند. معرفی BYOD (Bring Your Own Device)، پویایی و رایانش ابری و همچنین نیازمندی‌های شبکه‌های پویا و زیرساخت‌ها، انقلابی را در محیط ایستا فناوری اطلاعات به وجود آورده است.

هرچند محیط فناوری‌اطلاعات رشد سریعی داشته‌است، ولی رشد افق تهدیدات (threat landscape) از آن هم سریع‌تر بوده است. پیچیدگی و شتاب این سیر تکاملی با ابداع مستمر انواع حملات جدید، ترکیب تهدیدات شناخته و ناشناخته، بکارگیری آسیب‌پذیری «روز صفر (zero-day)»، و به کارگرفتن بدافزارهای پنهان در داخل اسناد، وب‌سایت‌ها، میزبان‌ها (Host) و شبکه‌ها، رشدی نمایی به خود گرفته‌است.

در دنیایی با شبکه‌ها و زیرساخت‌های فناوری اطلاعات پرکاربرد، در دنیایی که پارامترها دیگر به خوبی تعریف نمی‌شوند و تهدیدات روز به روز هوشمندتر می‌شوند، لازم است که با تعریف راهکاری صحیح، از شرکت‌ها در برابر افق همیشه در حال تغییر تهدیدات، محافظت کرد.

ما {در عصر حاضر} شاهد افزایش گسترده‌ی محصولات امنیتی هستیم؛ هرچند این محصولات بیشتر در ماهیت، جهت انفعالی و تاکتیکی دارند و روش مبتنی بر معماری، چندان در آن‌ها به چشم نمی‌خورد. امروزه شرکت‌ها به معماری واحدی نیازمند هستند تا ابزارهای امنیتی را با حفاظت‌های پیش‌گیرانه‌ی بی‌درنگ (real-time)، ترکیب کنند.

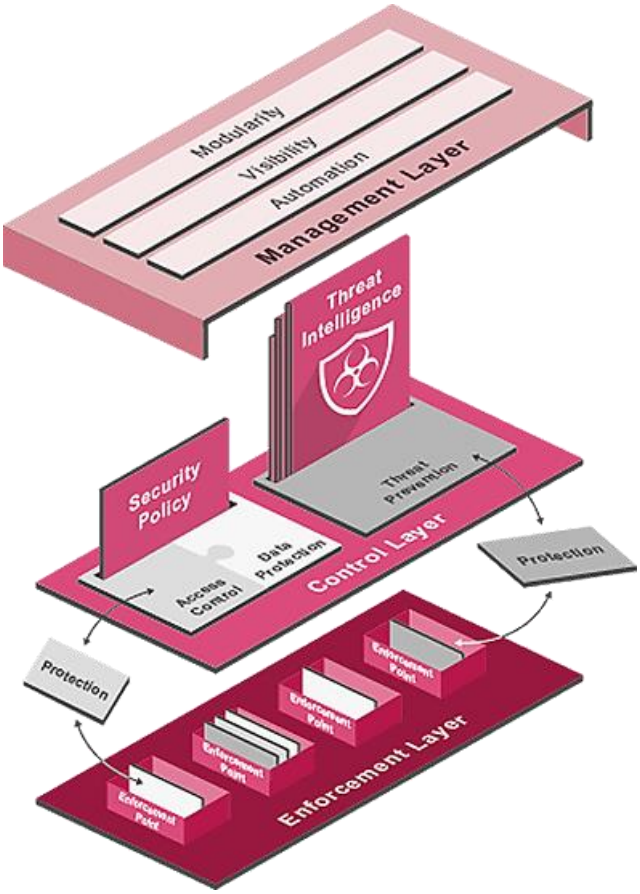
برای محافظت فعالانه از سازمان‌ها به الگوی جدیدی نیاز است. "محافظت تعریف‌شده نرم‌افزاری" یک متدولوژی و معماری امنیتی عملی و جدید است که زیرساخت‌هایی ماژولار، چابک و از همه مهم‌تر، امن را در اختیارمان قرار می‌دهد.

یک معماری این چنینی بایستی توانایی محافظت از سازمان‌ها با هر اندازه و در هر مکانی را دارا باشد: شبکه‌های مرکزی، دفاتر شعب، رومینگ تلفن‌های هوشمند و یا دستگاه‌های تلفن همراه، حتی به هنگام استفاده از محیط‌های ابری.

این محافظت باید به طور خودکار با افق تهدید نیز سازگار باشد به‌طوری که بدون‌نیاز به دستورات دستی مدیران امنیتی و یا توصیه مشاوران، به‌درستی عمل کند. این محافظت‌ها باید بطور یکپارچه با یکدیگر ادغام‌شده، محیط‌های فناوری اطلاعات بزرگ‌تری را شکل دهند، و به همین جهت، حالت مقابله معماری موردنظر باید به گونه‌ای باشد که بطور هم‌زمان منابع داخلی و خارجی را به‌هم متصل کند.

معماری "محافظت تعریف‌شده نرم‌افزاری" (SDP) زیرساخت امنیتی را به سه لایه به‌هم مرتبط تقسیم می‌کند:

- لایه اجرایی که براساس مقاصد امنیتی فیزیکی، مجازی و مبتنی بر میزبان، طراحی‌شده و هم‌گام با اتصال شبکه، منطق حفاظت را در محیط‌های با تقاضای بالا، اجرا می‌کند.
- لایه کنترل که منابع مختلف را تجزیه و تحلیل می‌کند و حفاظت‌ها و سیاست‌های اجرایی لایه‌ی اجرایی را ایجاد می‌کند.
- لایه مدیریتی که سازمان‌دهی زیرساخت را بر عهده دارد و بالاترین درجه چابکی را برای کل معماری فراهم می‌کند.



معماری محافظت تعریف‌شده نرم‌افزاری با ترکیب "لایه اجرایی" با عملیات بالا و "لایه کنترلِ" درحال توسعه و پویای مبتنی بر نرم‌افزار، نه تنها قابلیت انعطاف‌پذیر عملیاتی را ارائه می‌دهد بلکه در راستای کنترل حوادث مربوط به افق همواره در حال تغییر تهدیدات، نیز اقداماتی پیشگیرانه انجام می‌دهد.

معماری "محافظت تعریف‌شده نرم‌افزاری"، با طراحی موجود از امنیت سنتی شبکه، الزامات سیاست کنترلی را پشتیبانی می‌کند و همچنین پیشگیری‌های لازم شرکت‌های مدرن از فن‌آوری‌های نوین مانند رایانه‌های همراه و "شبکه‌های نرم‌افزاری تعریف‌شده" (SDN) را فراهم می‌سازد.

❖ لایه اجرایی:

لایه‌ی اجرایی معماری "محافظت تعریف‌شده نرم‌افزاری"، مطمئن، سریع و ساده طراحی شده است و دروازه‌های امنیتی شبکه و نرم‌افزارهای تحت میزبان که به عنوان "نقاط اجرایی" شبکه‌های سازمانی،

عمل می‌کنند را شامل می‌شود. این "نقاط اجرایی" می‌توانند به عنوان اجزای فیزیکی، مجازی و یا به عنوان اجزای پایه در میزبان شبکه‌های سازمانی یا شبکه‌های ابری، پیاده‌سازی شوند.

اصل اساسی پشت این لایه اجرایی، تقسیم‌بندی است. تقسیم‌بندی برای بقای یک سازمان تحت حمله، بسیار ضروری است چرا که حملاتی که تنها جزئی از سازمان را مورد هدف قرار می‌دهند نباید تمامی زیرساخت‌های امنیتی سازمان را تضعیف کنند. نقش تقسیم‌بندی در معماری "محافظت تعریف‌شده نرم‌افزاری" بدین صورت است که براساس فرآیندهای کسب و کار سازمانی، از توسعه پیداکردن حمله در شبکه جلوگیری می‌کند و تنها به ترافیک مجاز، اجازه عبور می‌دهد.

پیاده‌سازی این تقسیم‌بندی با تعریف بخش‌های «اتمی» در شبکه آغاز می‌شود. یک بخش اتمی حاوی عناصری است که دارای سیاست و ویژگی محافظتی مشابه می‌باشند. نقاط اجرایی در مرزهای هر بخش اتمی و برای اجرای منطق "محافظت تعریف‌شده"، اعمال می‌شوند. می‌توان بخش‌های اتمی را برای محافظت ماژولار، گروه‌بندی کرد. علاوه براین، کانال‌های امن به‌منظور محافظت از تعاملات و جریان داده بین بخش‌های شبکه، ایجاد می‌شود.

در زیر به چهار مرحله کلیدی این تقسیم‌بندی، اشاره شده است:

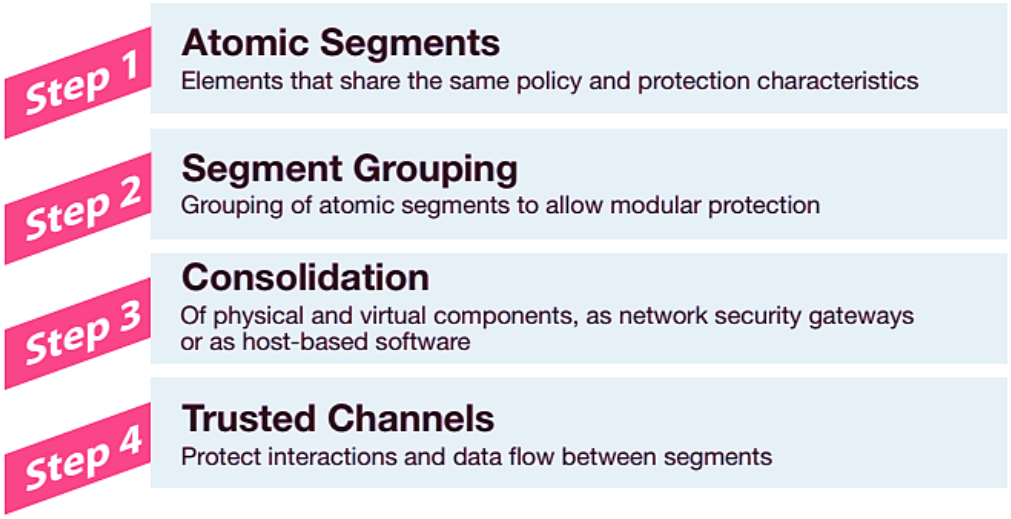
- ✓ گام اول: بخش‌های اتمی

  عناصری که سیاست و ویژگی‌های حفاظتی مشابه دارند.
- ✓ گام دوم: گروه‌بندی بخش‌ها

  گروه‌بندی بخش‌های اتمی برای حفاظت ماژولار.
- ✓ گام سوم: تثبیت اجرا

  تثبیت اجزای فیزیکی یا مجازی به عنوان دروازه‌های امنیت شبکه و یا نرم‌افزار مبتنی بر میزبان.
- ✓ گام چهارم: کانال‌های امن

  حفاظت از تعاملات و جریان اطلاعات بین بخش‌ها.



✓ گام اول: بخش‌های اتمی:

یک بخش اتمی شامل مجموعه‌ای از محاسبات و عناصر شبکه‌ای است که:

۱) دارای مشخصات امنیتی مشترکی هستند؛

۲) نمی‌توان آن‌ها را به بخش‌های کوچکتری تقسیم کرد؛

۳) می‌توانند توسط کنترل‌های امنیتی مبادله‌ای بین بخش‌ها و نهادهای خارجی، محافظت شوند.

نمونه‌ای از یک بخش اتمی ممکن است دستگاهی واحد باشد که نرم‌افزار امنیتی بر روی آن نصب‌شده است و یا این‌که بر روی آن تعدادی میزبان دارای شبکه‌ای مشترک، توسط یک دروازه امنیتی، محافظت می‌شوند. یک بخش اتمی مجموعه‌ای از میزبان‌های محاسباتی و اجزای شبکه است که مشخصات امنیتی مشترکی دارند.

تعریف بخش‌های اتمی و شناسایی نهادهای خارجی دارای مشخصه امنیتی مشترک، اولین قدم در پیاده‌سازی معماری "محافظت تعریف‌شده نرم‌افزاری" است. براساس ارزش دارایی‌های شرکت در یک بخش و سطح اعتماد اعطاشده به کاربران و کنترل‌های امنیتی آن بخش، برای هر یک از بخش‌ها یک مشخصه امنیتی تعریف می‌شود.

تهدیدات ممکن است در هنگام تعامل دو بخش با مشخصه امنیتی متفاوت، رخ دهد. به علاوه، پتانسیل تهدیدات به موازات افزایش اختلاف بین دو مشخصه امنیتی، افزایش می‌یابد. جهت جلوگیری از چنین ریسکی، بسیاری از سازمان‌ها برای داده‌ها، میزبان‌ها، برنامه‌ها و شبکه‌هایی که از این روش تجزیه و تحلیل پشتیبانی می‌کنند، از یک شیوه طبقه‌بندی سازمانی، استفاده می‌کنند.

✓ گام دوم: گروه‌بندی بخش‌ها

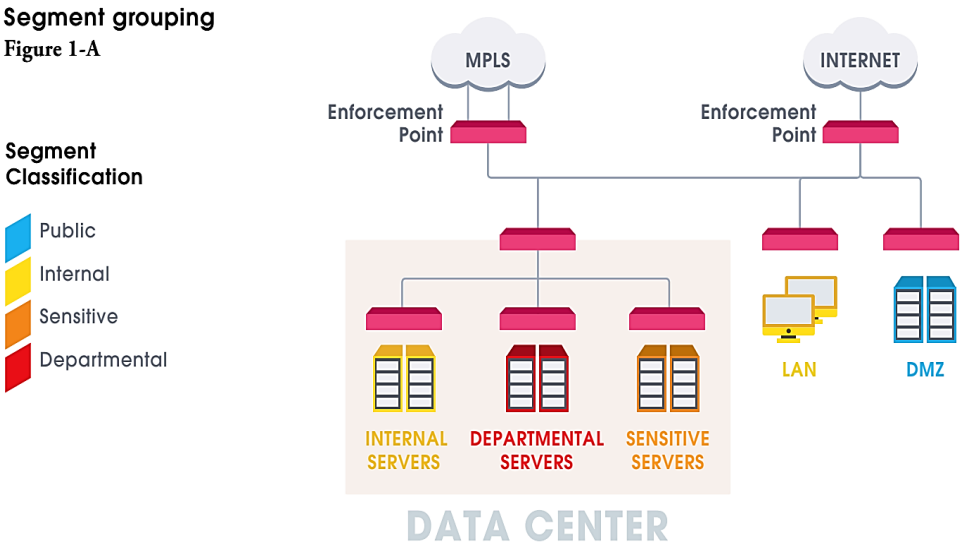
پس از شناسایی بخش‌های اتمی، می‌توان آن‌ها را در سلسله‌مراتبی از گروه‌ها، گروه‌بندی کرد (به عنوان مثال، برنامه‌های کاربردی را می‌توان بصورت یک سلسله مراتب در گروه‌های میزبان، میزبان‌های چندگانه در یک شبکه و شبکه‌های چندگانه گروه‌بندی کرد).

درحالی‌که هر زیربخش تنها محافظت از خود را بر عهده دارد، گروه‌بندی از موارد زیر پشتیبانی می‌کند:

- تفکیک بالا از طریق انتزاع و پنهان‌سازی اطلاعات.
- افزایش اعتماد و حفاظت وسیع‌تر در قسمت مرزی بالاتر از زیربخش‌ها.
- کنترل متمرکز و ارائه خدمات زیرساخت امنیتی.
- مهار عفونت و بهبودی.

در یگ گروه‌بندی سلسله‌مراتبی، تعاملات ممکن است از چندین نقطه اجرایی عبور کنند. به عنوان مثال، یک سرور در بخش «سرورهای داخلی» که به یک منبع در اینترنت متصل می‌شود (مثلا سرویس به‌روز رسانی محتوا)، ممکن است از نقاط اجرایی پیوسته و میانی زیر نیز عبور کند:

۱- نرم‌افزار امنیتی نصب‌شده بر روی «سرور داخلی» بخش میزبان
۲- بخش مرزی «سرور داخلی» نقطه اجرایی
۳- نقطه اجرایی واقع در مرکزداده



۴- نقطه اجرایی internet-facing

تعاملات از طریق پراکسی‌های واقع‌شده در بخش DMZ از مسیرهای کنترل اضافی شامل نقطه اجرایی DMZ، به داخل و خارج از بخش DMZ، عبور می‌کنند.

با تکرار فرآیند گروه‌بندی بخش‌ها در قسمت‌های متوالی بخش‌های بزرگ‌تر شبکه، شرکت‌ها می‌توانند این اطمینان را بدهند که تمامی دارایی‌ها در یک بخش محافظت‌شده قرار گرفته‌اند. با توجه به بخش‌های گروه‌بندی‌شده، خطوط سلسله‌مراتبی مقابله، شبکه‌های داخلی را بهم متصل‌کرده و حفاظتی مناسبی را به وجود می‌آورد.

✓ گام سوم: تثبیت اجرا

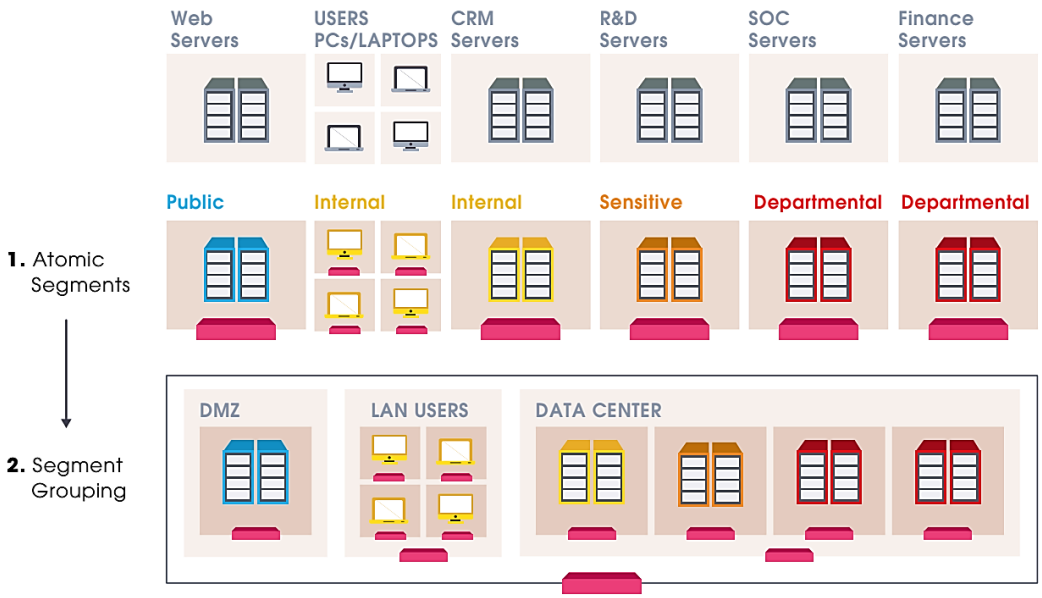
مدل‌سازی و پیاده‌سازی:

پس از ساخت مدل تقسیم‌بندی، نقاط اجرایی تعریف‌شده باید به عنوان دروازه‌های امنیت شبکه یا نرم‌افزارهای مبتنی بر میزبان، پیاده‌سازی شوند. فناوری‌های تلفیقی و مجازی‌سازی شامل دروازه‌های

چندگانه، مجازی‌سازی دروازه، شبکه‌های مجازی (VLANs)، SDN و مجازی‌سازی شبکه، می‌توانند برای دستیابی به عمل‌کردی مطلوب و قابل مدیریت، مورد استفاده قرار گیرند.

روند تقسیم‌بندی (شکل B-۱)، بخش‌هایی از یک نمونه ایستگاه‌کاری کاربر، سرورها (CRM، R&D وFinance)، مرکز عملیات امنیت (SOC) و سرورهای خارجی در بخش DMZ ، را نشان می‌دهد. مشخصه امنیتی به بخش‌های اتمی (شکل A-۱) وابسته‌اند. نقاط اجرایی در مرزهای هر بخش قرار می‌گیرد و بخش‌ها براساس مشخصات امنیتی‌شان، گروه‌بندی می‌شوند.

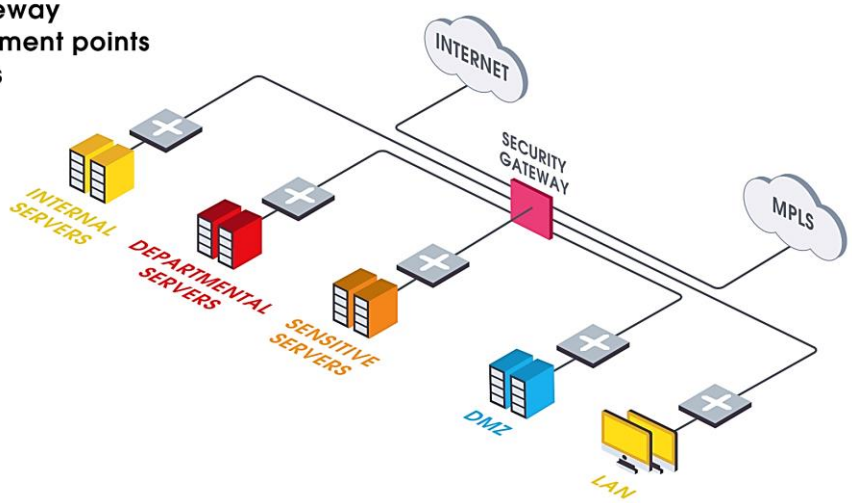
Enterprise segmentation process
Figure 1-B



ا دغام دروازه: ب ا آنکه شکل A-۱ هشت قسمت مجزای مرزی

شبکه (به غیر از نقاط اجرایی امنیتی نرم‌افزار در بخش LAN) را نشان می‌دهد، عموما پیاده‌سازی شامل هشت عدد دستگاه دروازه امنیتی، نمی‌شود. وابسته به محدودیت‌های امنیتی، مالی و عمل‌کردی، چند نقطه اجرایی می‌تواند در یک دستگاه امنیتی، یکپارچه شود. شکل C-۱ پیکربندی ساده‌ای از یک دروازه امنیتی یکپارچه را نشان می‌دهد که برای کنترل تمامی تعاملات داخلی بین بخش‌ها از آن استفاده می‌شود.

A single security gateway consolidates enforcement points for multiple segments
Figure 1-C

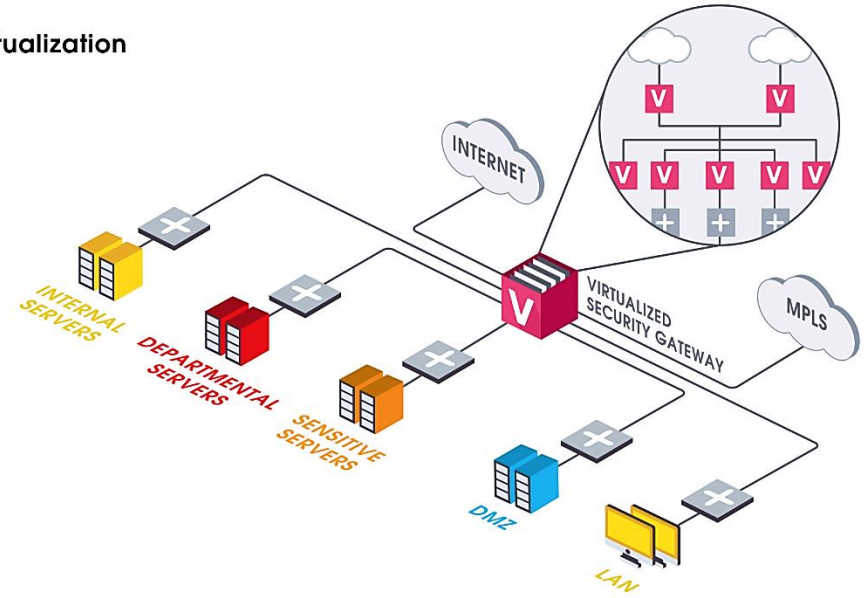


مجازی‌سازی امنیت:

درحالی‌که ادغام دروازه‌ها می‌تواند منافع قابل توجهی را همراه داشته باشد ولی ممکن است باعث شود تا برخی از نقاط اجرایی ادغام‌شده، دچار نقض‌هایی شوند. به طور خاص، یک سیاست امنیتی پیچیده‌تر را می‌توان به معنای افزایش ریسک خطای پیکربندی، دانست. به عنوان مثال، ضابطه‌ای با خطای پیکربندی که اجازه دسترسی بین دو بخش داخلی را صادر می‌کند، ممکن است به طور تصادفی اجازه دسترسی به اینترنت ورودی را نیز صادر کند.

می‌توان یک دروازه امنیتی مجازی را جایگزین پیکربندی یکپارچه‌ی نشان داده شده در شکل ۱-C کرد (شکل ۱-D).

Security control virtualization
Figure 1-D



سرور مجازی‌سازی (ابر):

در محیط یک سرورمجازی‌سازی‌شده، مطابق با شکل D-۱، می‌توان با استفاده از ماشین‌های مجازی‌سازی‌شده (VMs)، دروازه‌های امنیتی مجازی را پیاده‌سازی کرد. زیرساخت ابری، تکنولوژی مجازی‌سازی پایه را فراهم کرده و تضمین می‌کند که ترافیک بین بخشی با ایجاد VLANها و اتصال آن‌ها از طریق نقاط اجرایی، در نقاط اجرایی سطح VM جریان می‌یابد. مبادله ترافیک بین VMهای مختلف در یک میزبان فیزیکی یکسان، می‌تواند به شکل موثری توسط یک نقطه‌ی اجرایی در حال اجرا در VM یک میزبان، کنترل و به کار گرفته شود.

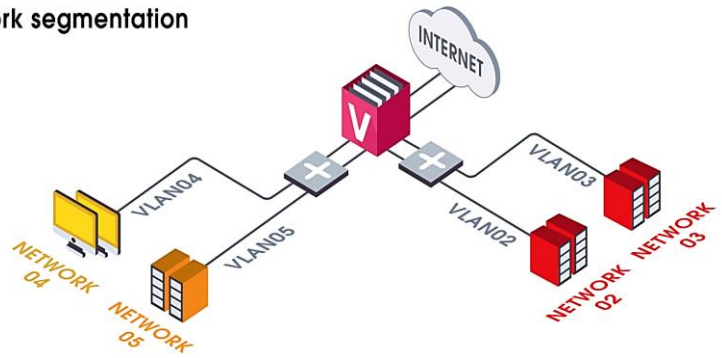
پیاده‌سازی نیز می‌تواند در خود هایپرویزور، یکپارچه شود که در اینصورت این تضمین داده نمی‌شود که تمامی اطلاعات بدون نیاز به مهندسی مجدد شبکه مجازی، برای قراردادن ماشین در پشت نقطه اجرایی، مبادله شده‌اند. نقاطه اجرایی سطح هایپرویزور از قلاب‌های ارائه‌شده توسط پلت‌فرم مجازی‌سازی، استفاده می‌کند تا تمامی ترافیک شبکه را از VMهای میزبان دریافت و به آن‌ها ارسال کند.

علاوه‌براین، محیط مجازی‌سازی‌شده سرور، می‌تواند دروازه‌های امنیتی مجازی و فیزیکی را نیز دربرگیرد (مشابه شکل D-۱) تا فرآیند امنیت را از سرورمجازی‌سازی‌شده آفلود و بر روی سخت‌افزاری سفارشی با کارایی بالا، اجرا کند.

شبکه‌های مجازی (VLAN):

VLAN یک مکانیزم کلیدی شبکه است که برای تقسیم‌بندی شبکه سازمانی از آن استفاده می‌شود. یک دروازه‌ی امنیتی متصل به یک سوئیچ که از رابط تنه (trunk) استفاده می‌کند، می‌تواند ترافیک شبکه را از طریق چند VLAN تجزیه و تحلیل کرده و انتقال دهد. این پیکربندی به یک دروازه امنیتی این اجازه را می‌دهد تا ترافیک بین صدها VLAN را کنترل کند. در شکل E-۱ دستگاه سوئیچ به گونه‌ای پیکربندی خواهد شد تا تمامی فریم‌های شبکه جاری از VLAN۰۲ به VLAN۰۳ درون دروازه امنیتی را به جلو ارسال کند، و از طریق نقطه اجرایی مجازی بخش که بر روی دروازه، پیاده‌سازی شده است، مبادله ترافیک بین بخش‌ها را تضمین کند.

Using VLANs for network segmentation
Figure 1-E

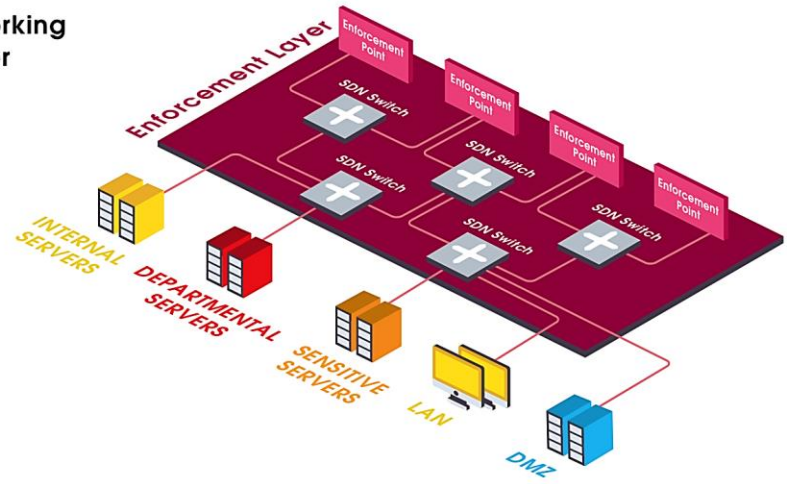


شبکه تعریف‌شده نرم‌افزاری (SDN):

در زیرساخت‌های سنتی شبکه، شبکه‌ها و ابزارهای امنیتی شبکه مانند روترها، سوئیچ‌ها، فایروال‌ها و IPSها به عنوان دستگاه‌هایی فیزیکی، پیاده‌سازی می‌شوند. جریان‌های شبکه توسط توپولوژی

شبکه تعیین می‌شود؛ بدین صورت که هر دستگاه شبکه، جداگانه عمل تصمیم‌گیری در مورد بهترین مسیر انتقال یک بسته به سمت مقصدش را انجام می‌دهد. اما با ظهور سرورهای مجازی‌شده و محیط شبکه مجازی مبتنی بر ابر، توانایی گسترش سریع برنامه‌های جدید آن هم بدون تغییرات پیچیده شبکه به یک نیاز عمومی تبدیل شده است. "محافظت تعریف‌شده نرم‌افزاری"، یک معماری شبکه در حال ظهور است که در آن، کنترل شبکه از زیرساخت آن، تفکیک شده است.

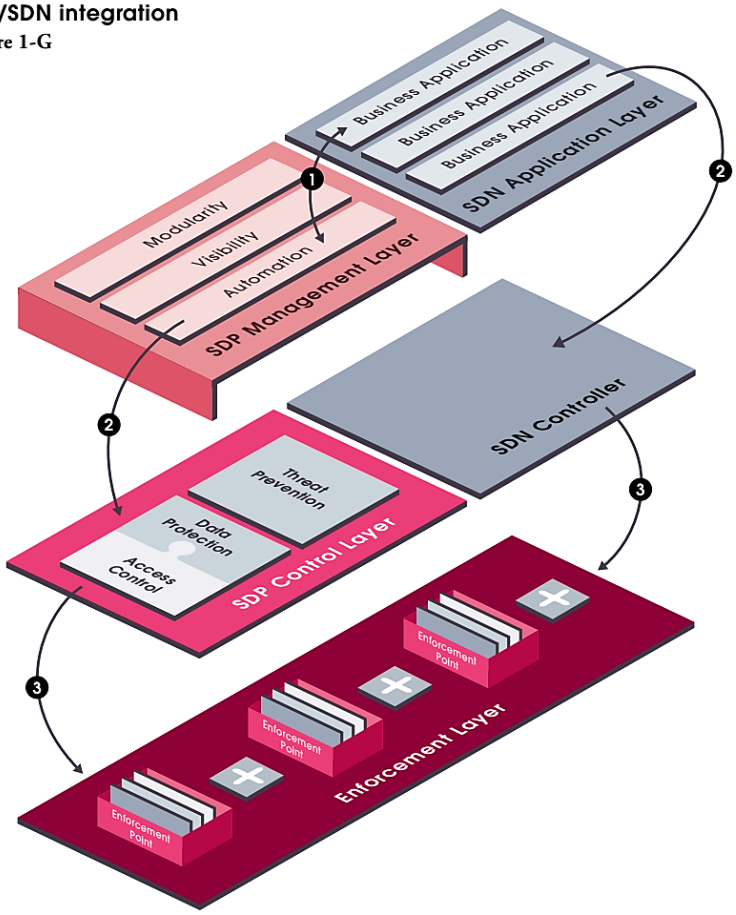
Software-defined Networking (SDN) Enforcement Layer
Figure 1-F



با ادغام لایه اجرایی "محافظت تعریف‌شده نرم‌افزاری" و لایه زیرساخت SDN، مانند شکل F-۱، سوئیچ‌های SDN به عنوان نقاط اجرایی ساده، ثبت می‌شوند. نقاطی که نقش‌شان آفلود جریان‌ها و زیرجریان‌های مناسب به نقاط اجرایی مناسب بخش "محافظت تعریف‌شده نرم‌افزاری" است.

شکل G-۱ یکپارچگی معماری "محافظت تعریف‌شده نرم‌افزاری" و SDN را نشان می‌دهد. لایه اجرایی "محافظت تعریف‌شده نرم‌افزاری" با استفاده از برنامه‌ی APIهای SDN (۱) و با هماهنگ کردن سیاست‌های شبکه و امنیتی بین لایه‌های کنترل "محافظت تعریف‌شده نرم‌افزاری" و SDN (۲)، این ادغام را هماهنگ می‌کند. جریان‌های شبکه توسط لایه کنترل SDP/SDN برنامه‌ریزی می‌شود تا از طریق نقاط اجرایی فیزیکی یا مجازی "محافظت تعریف‌شده نرم‌افزاری"، عبور کند (۳). این روند تضمین می‌کند که تمامی تعاملات بین‌بخشی با ثبت سوئیچ‌های SDN به عنوان نقاط اجرایی ساده، مبادله شده‌اند. نقش امنیتی آن سوئیچ‌ها، آفلود جریان‌ها و زیرجریان‌های مناسب به نقاط اجرایی مناسب بخش است.

SDP/SDN integration
Figure 1-G



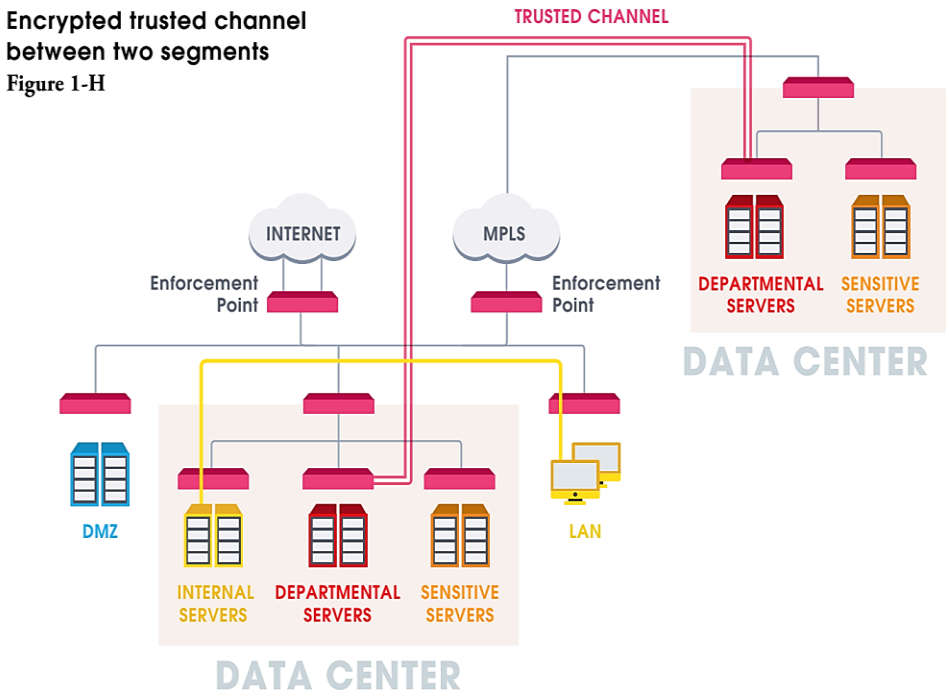
✓ گام چهارم: کانال‌های امن:

نقاط اجرایی بخش از تعاملات غیرمجاز درون‌بخشی، جلوگیری می‌کند. با این‌حال، تعامل مجاز نیز باید محافظت شود. هنگامی‌که دو بخش شبکه دارای عنصر مشترک باشند، یک دروازه امنیتی می‌تواند بصورت فیزیکی به هر دو بخش متصل شود تا مبادله‌گر تعاملات درون بخشی باشد. زمانی‌که از نظر فیزیکی از یکدیگر جدا شوند، چنین تعاملاتی باید در حین عبور از زیرساخت شبکه، امنیت داشته باشد.

اگر تعاملات بین بخش‌ها توسط یک بخش سلسله مراتبیِ درون یک شبکه امن ایجاد شوند، بخش سلسله‌مراتبی، مسئول امنیت داده‌های درحال عبور (انتقال) است. با این‌حال، اگر شبکه نسبت به ویژگی‌های امنیتی دو بخش، «ناامن (untrusted)» باشد، مهاجمان می‌توانند به داده‌های جاری بین دو بخش دسترسی پیدا کنند و یا آن‌ها را تغییر دهند. بنابراین، لازم است تا یک کانال امن بین بخش‌ها

برقرار شود و برای تعاملات بین بخش‌ها از رمزنگاری (encryption) استفاده شود. چنین کانالی از دسترسی غیرمجاز به هر داده جاری در آن جلوگیری کرده و هم‌زمان هرگونه اقدام مربوط به تغییر اطلاعات را شناسایی و مسدود می‌کند.

مثال بعدی دو بخش اداری که در سایت‌های مختلفی واقع شده‌اند و با یک کانال امن تعامل دارند را نشان می‌دهد. در این مثال، کاربران داخلی می‌توانند مستقیما به سرورهای داخلی دسترسی پیدا کنند.



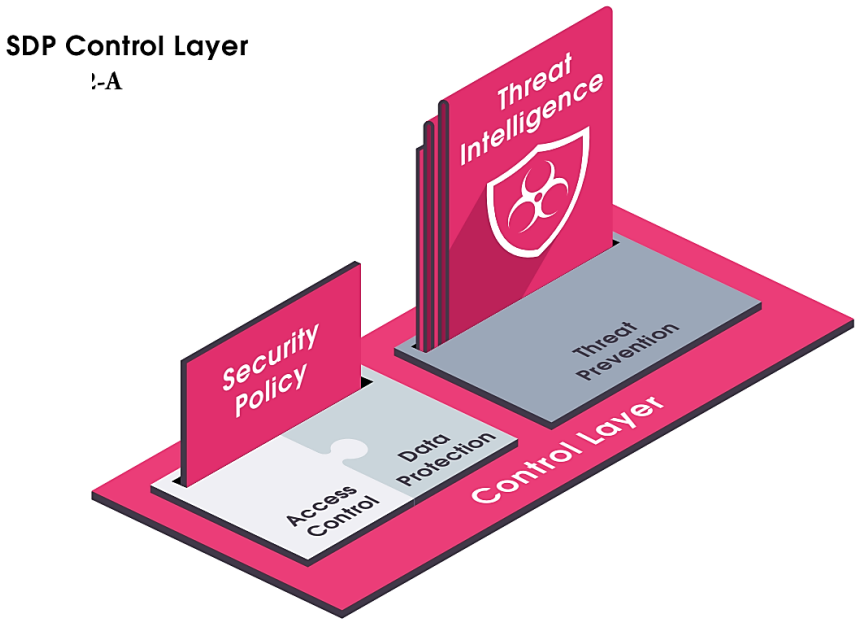
Encrypted trusted channel between two segments
Figure 1-H

❖ لایه کنترل:

نقش "لایه‌ی کنترل" ایجاد محافظت و نوبت‌دهی، برای اجرا در نقاط اجرایی است. این لایه شامل "پیش‌گیری تهدید"، "کنترل دسترسی" و "حفاظت داده" می‌باشد.

سیاست "پیش‌گیری تهدید"، ساده است: «مسدودکردن آدم‌های بد!!». این سیاست تااندازه‌ای هم ویژه هریک از شرکت‌ها است، ولی به طور کلی سیاستی عمومی است و لازم است تا در همه سازمان‌ها، مورد استفاده قرار گیرد.

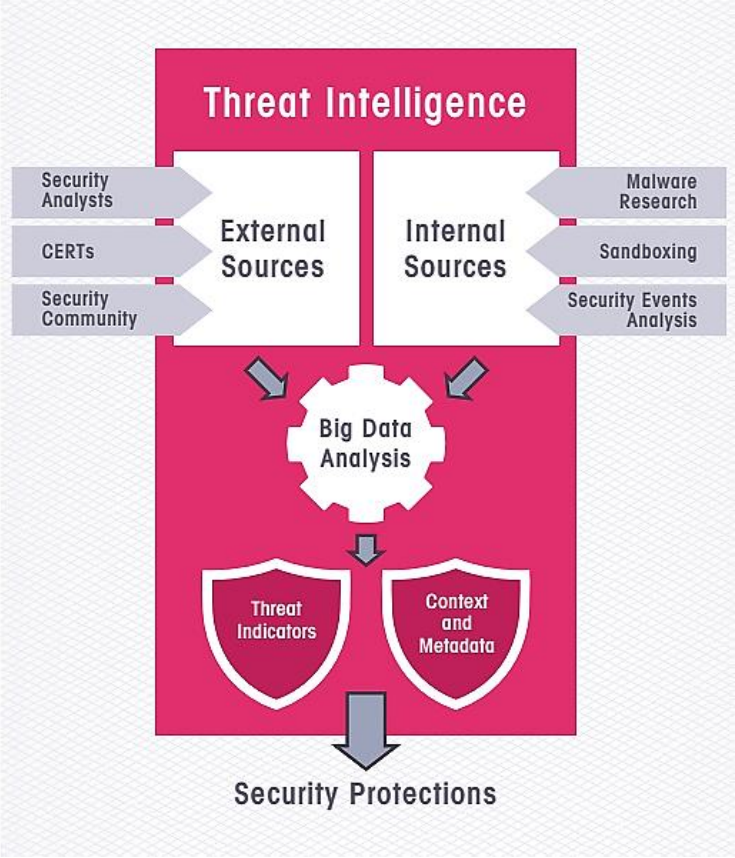
حفاظت "پیش‌گیری تهدید" مهاجمان را مسدودکرده، استخراج آسیب‌پذیری‌ها و تحویل بارهای مخرب را رد می‌کند. آن‌ها همچنین از اتصال بدافزارها و ربات‌ها به مراکز Command و Control (C&C) جلوگیری می‌کنند.



اجزای "پیش‌گیری تهدید" لایه کنترل به منظور تضمین صحت انتخاب اجرایی، یافته‌های موتورهای چندگانه، اعم از امضاها، اعتبار، رفتار، شبیه‌سازی بدافزار و اعتبار انسانی، را برای تولید حفاظت امنیتی مناسب، به‌هم مرتبط می‌کنند.

جهت مناسب‌شدن کنترل "پیش‌گیری تهدید"، لازم است تا آن‌ها با اطلاعاتی گسترده و مطمئن، تغذیه شوند. سازمان‌ها باید انتظار ورود غیردستی جریان ثابتی از "هوش تهدیداتی" به محیط امنیتی‌شان را داشته باشند.

"هوش تهدیداتی" بااستفاده از منابع داخلی و خارجی داده تهدید، بدست می‌آید. بطور ایده‌آل این منابع باید شامل هوش امنیتی عمومی، مانند تیم‌های آمادگی پاسخ‌گویی اورژانس کامپیوتر (CERTs) و تیم‌های پاسخ‌گویی به حوادث امنیتی کامپیوتر (CSIRTs)، چندین تحلیل‌گر امنیتی، فروشندگان محصولات امنیتی و دیگر سازمان‌های درون جامعه امنیتی باشد. علاوه بر این منابع خارجی "هوش تهدیداتی" از طریق بررسی بدافزار، تکنیک‌های sandboxing و تجزیه و تحلیل داده‌های جمع‌آوری شده از نقاط اجرایی در داخل سازمان نیز تولید می‌شود.



هوش تهدیداتی، عوامل تهدید، کمپین‌ها، تاکتیک‌ها، تکنیک‌ها و روش‌ها (TTPs) را توصیف و ویژگی‌های تهدید real-time را تهیه می‌کند.

کنترل‌های "پیش‌گیری تهدید" با استفاده از هوش تهدیداتی، ابرداده‌های امنیتی را به قالب شاخص‌ها و توصیفات حمله، تبدیل می‌کنند.

برخلاف "پیش‌گیری تهدید"، "کنترل دسترسی" داده برای شرکت‌های خصوصی بسیار خاص‌تر هستند.

"کنترل دسترسی" و "محافظت داده" با تعریف تعاملات بین کاربران و داده‌های درون شرکت‌های جمعی، فرآیندهای کسب و کار را ممکن می‌کند. آن‌ها جهت حداقل سطح مورد نیاز برای پشتیبانی از کسب و کار، اجرای اصول امنیتی «حداقل امتیاز» را اعمال می‌کنند.

این کنترل‌های حفاظتی به مخازنی که قوانین کسب و کار خاص شرکت، دارایی‌ها، کاربران، نقش‌ها و برنامه‌های کاربردی را تعریف می‌کنند، بستگی دارند و سیاست‌های امنیتی را برای مجموعه تعاملات مجاز بین دارایی‌ها، کاربران و برنامه‌های کاربردی مشابه، تعریف می‌کنند.

تجزیه و تحلیل و کنترل ترافیک با استفاده از روشی سازگار انجام می‌گیرد. به عنوان مثال، درمورد ترافیک اینترنت، لایه کنترل ممکن است برای اطلاع از آخرین کاربردها و پروتکل‌ها با یک پایگاه‌داده ابری، ارتباط برقرار کند، درحالی‌که در مورد ترافیک داخلی، ممکن است از تعریف برنامه‌های کاربردی متناسب یا پروتکل مورد استفاده در سازمانی دیگر، استفاده کند.

علاوه بر این، لایه کنترل از تغییرات شبکه و تعاریف پیاده‌سازی در دیگر سیستم‌های فناوری اطلاعات آگاه است. می‌توان چنین مثال‌هایی را برای این موضوع در نظر گرفت: تغییر کاربر، اعمال خودکار امنیت در ماشین مجازی جدید، و یا صدور اجازه دسترسی به یک میزبان جدید تعریف‌شده در سرور نام دامنه (DNS).

- رویکرد مبتنی بر ریسک برای انتخاب کنترل‌های محافظتی

برای "نقاط اجرایی" متفاوت به محافظت‌های گوناگونی نیاز داریم. انتخاب نوع حفاظت به دارایی‌های بخش، مجوز کاربر و محیط تهدید، بستگی دارد. عمل‌کرد سیستم و محدودیت‌های عملیاتی نیز بایستی در نظر گرفته شوند.

نقش لایه کنترل انتخاب منطق کنترل امنیتی مناسب است بطوری‌که این منطق در هر "نقطه اجرایی" مرزی بخش‌ها اجرا می‌شود تا "کنترل‌دسترسی" و سیاست‌های "محافظت داده" اجرا و تهدیدات شناسایی‌شده، در نظر گرفته شوند.

اولین گام در انتخاب کنترل‌های امنیتی، انجام تجزیه و تحلیل ریسک (risk) برای هر بخش یا هر گروه از بخش‌ها است. ریسک به عنوان میزان شدت و احتمال وقوع حوادث امنیتی در یک تراکنش یا دارایی سازمان، تعریف می‌شود. چنین حوادث امنیتی شامل نقض قوانین امنیتی، آشکارسازی تهدیدات و جریان‌های نامناسب داده می‌باشد. درک ریسک یک چارچوب الویت‌بندی برای کنترل‌های امنیتی را فراهم می‌کند.

برای تعاملاتی که در مرز یک بخش قرار دارند، دسته‌های مختلف ریسک درنظر گرفته می‌شود. سطح ریسک را می‌توان براساس "رخداد"، "احتمال موفقیت" و "آسیب‌بالقوه" کدگذاری کرد. به عنوان مثال، یک درخواست HTTP خارج از باند می‌تواند مرتبط با یک نمونه طرح طبقه‌بندی ریسک به صورت بعدی

Risk	Risk description	Analysis for an outbound HTTP request
Insider	An authorized user performs an interaction that violates security policy	Is the in-segment user authorized to access the external service?
External attack	An external entity attempts to gain unauthorized access to assets or services	Could the external service be spoofed by an attacker?
Data access	An attacker reads or modifies data in transit or data at rest by accessing network or storage infrastructure	Is the network path for the interaction vulnerable to interception?
Data leakage	Sensitive data is transmitted to unauthorized users or written to removable media	Could significant amounts of data be uploaded to unauthorized locations?
Exploit	An attacker performs a protocol violation causing a system failure	What is the chance that a protocol violation will trigger a client exploit and malware download in the segment?
Malware	Malicious code delivered over the network or via removable I/O devices adversely impacts business assets	Could the request be indicative of malware behavior (e.g., connection to C&C server or drop zone)?
Denial of service	An interaction consumes excessive amounts of processing, storage or network capacity, denying service for authorized interactions	Could the rate, duration or bandwidth of requests conceivably impact the level of service for authorized interactions?

تحلیل شود.

ریسک ممکن است در یک سطح بالا در نظر گرفته شود و یا ممکن است مشروح روش‌های بالقوه حمله باشد. برای کاهش هر ریسک، مجموعه‌ای از "کنترل‌های امنیتی" تعریف شده‌است که آن را تا حد قابل قبولی برای سازمان‌ها کاهش می‌دهد.

در شکل C-۲، دید ساده‌ای از نگاشت ریسک برای حفاظت از داده‌ها، دیده می‌شود. هر سطر نمایانگر یک ریسک یا روش حمله دقیق (مثلا دریافت بدافزار از طریق یک ایمیل حاوی لینک)، و هر ستون نمایانگر یک بسته محافظتی کاهش‌دهنده (مثلا پیش‌گری تهدید پیش از تزریق) یا یک حفاظت خاص (مثلا فیلترینگ مبتنی بر اعتبارِ URLها) می‌باشد.

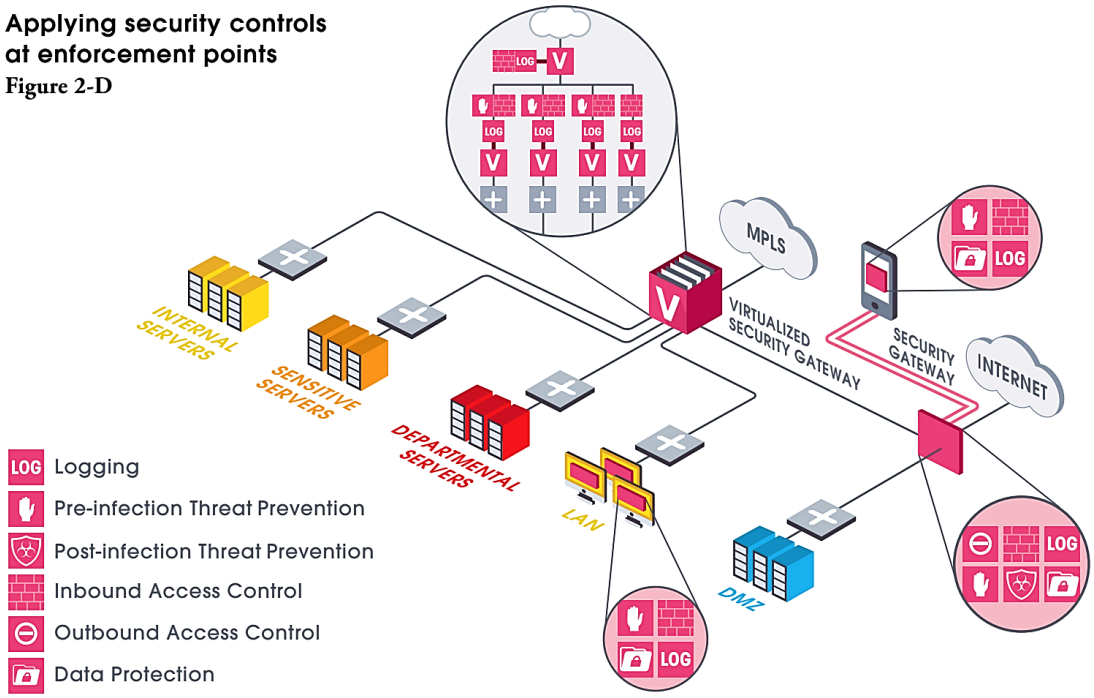
Mapping security controls to risks Figure 2-C

Risk	ACCESS CONTROL		THREAT PREVENTION		DATA PROTECTION
	Inbound	Outbound	Pre-	Post-	
Insider	✓	✓		✓	✓
External attack	✓		✓	✓	✓
Data access					✓
Data leakage		✓		✓	✓
Exploit	✓		✓		
Malware	✓	✓	✓	✓	
Denial of service	✓		✓		

لایه کنترل، کنترل‌ها را به نقاط اجرایی ارائه می‌دهد و بنابراین هرگونه خطر مرتبط با هرگونه تعامل در طول مسیر تعامل، قابل کنترل است.

Applying security controls at enforcement points

Figure 2-D



❖ لایه مدیریت:

لایه مدیریت به معماری "محافظت تعریف‌شده نرم‌افزاری"، روح می‌بخشد. با فعال‌سازی هر یک از اجزای معماری، این لایه به عنوان لایه رابط بین "مدیران امنیتی" و دولایه‌ی دیگر "محافظت تعریف‌شده نرم‌افزاری" عمل می‌کند.

لایه مدیریت "محافظت تعریف‌شده نرم‌افزاری" باید باز و ماژولار باشد و اجازه‌ی قابلیت مشاهده وضعیت امنیتی سازمان را صادر کند.

با پویایی شبکه‌ها، برنامه‌های کاربردی، میزبان‌ها، کاربران، نقش‌ها و تغییر محیط کسب و کار، پیکربندی‌های سازمانی به سرعت در حال توسعه هست. این موضوع در فضاهای مجازی تحت سرور مجازی‌سازی‌شده و SDN به شکل ویژه‌ای صدق می‌کند. در این فضاها لازم است که حفاظت‌ها، تغییرات سریع در سرور، هویت و مکان شبکه‌ها را دنبال کند.

زیرساخت‌های "مدیریت باز"، اجازه می‌دهد تا با استفاده از قابلیت‌های اتوماسیون، هماهنگ‌سازی سیاست امنیت لایه کنترل با محیط‌های پویا سازمانی از جمله مدیران شبکه ابری، پیکربندی پایگاه‌های‌داده، سیستم‌های موجودی دارایی و زیرساخت‌های مدیریت هویت را به انجام برساند.

مدیریت ماژولار "محافظت تعریف‌شده نرم‌افزاری"، تعریف دسترسی و سیاست‌های کنترل داده و فعال‌سازی "پیش‌گیری تهدید" را به طور جداگانه ممکن می‌سازد. سیاست‌های "پیشگیری تهدید" می‌تواند برروی ترافیک مجاز، سیاست‌های دسترسی و داده به طور خودکار اعمال شوند اما همچنین می‌تواند توسط افراد دیگر یا حتی با برون‌سپاری، مدیریت شود.

ماژولاریتی از لایه‌های سیاست و زیرلایه‌های مرتبط با بخش‌های مختلف شبکه نیز حمایت می‌کند و همگام با آن قابلیت اعطای مدیریت به ادمین‌های خاصی که می‌توانند بر روی همه‌ی آن‌ها کار کنند، ارائه می‌کند و به دو لیل، قابلیت مشاهده (visibility) لازم است: اول آگاهی از وضعیت و درک رخدادهای درون شبکه؛ و دوم پاسخ به حادثه و انجام عملی در رابطه با آن.

لایه مدیریت، رویدادهای نقاط اجرایی که در شبکه گسترش‌یافته‌اند را جمع‌آوری و ادغام‌کرده و به‌هم مرتبط می‌کند. تجسم real-time از نجیره‌ای از حوادث به پاسخ‌دهندگان به حادثه، ارائه شده است،

قابلیتی که اجازه شناسایی بردارهای حملات اولیه و متعاقبا میزبان‌های منفرد و داده‌های محرمانه را صادر می‌کند.

بررسی حادثه قادر است تا ویژگی‌های تهدید جدیدی را برای بدافزارها، رفتارهای تهدید و آدرس‌های شبکه مرتبط با تمامی حملات شناسایی‌شده، تولید کند. این ویژگی‌ها به طور خودکار به لایه کنترل، تغذیه (feed) و از آن‌جا به لایه اجرایی توزیع می‌شوند تا از سازمان محافظت کنند.