



دفتر تهران: خیابان خالد اسلامبولی (وزرا)
خیابان هفتسم، پلاک ۳۲، طبقه سوم
تلفکس: ۰۲۱-۸۸۱۰۵۰۰۸
تلفن دفتر تبریز: ۰۴۱-۳۳۳۷۰۰۱۰

CONTENTS

فهرست

۰۴	 درباره ما
راهکارهای تخصصی مرکز داده	
۰۸	 SERVER VIRTUALIZATION
۰۹	 VIRTUAL DESKTOP INFRASTRUCTURE
۱۲	 APPLICATION VIRTUALIZATION
۱۳	 STORAGE VIRTUALIZATION
۱۴	 NETWORK VIRTUALIZATION
۱۵	 BACKUP AND DATA RECOVERY
۱۸	 BUSINESS CONTINUITY
۲۰	 DATA CENTER MONITORING
۲۱	 SAN AND NAS STORAGES
۲۳	 FCOE NETWORK
۲۳	 TAPE ARCHIVING
راهکار های امنیت شبکه و داده	
راهکارهای امنیت داده	
۲۵	 DATA LOSS PREVENTION
۲۶	 ENCRYPTION
۲۶	 DATA BASE SECURITY
۲۷	 ENDPOINT SECURITY
راهکارهای امنیت شبکه	
۲۸	 GATEWAY SECURITY
۲۹	 WEB APPLICATION FIREWALL
۲۹	 VALIDATION & ID PROTECTION
۳۰	 ADVANCED THREAT PROTECTION
۳۱	 EMAIL SECURITY
۳۵	 مشاوره و نگهداری
۳۷	 مرکز آموزش هامون
۳۸	 گواهینامه ها و مجوزها
۳۹	 محصولات
۴۰	 چرا هامون؟



- راهکارهاک مرکز داده
- راهکار های امنیت شبکه و داده
- مشاوره و نگهداری
- مرکز آموزش

بیانیه مأموریت

ما از طریق ارائه راهکارهای فناوری اطلاعات و ارتباطات، کارایی و اثربخشی فرآیندهای کسب و کار مشتریان خود را ارتقاء بخشیده و موجبات صرفه جویی در اقتصاد کشور را فراهم می سازیم.

ما با اتکا به تجربه سازمان، بروزآوری دائمی مهارت و دانش کارکنان، ارتباطات نزدیک با راهبران جهانی، بهترین و امن ترین راهکارهای دسترسی به اطلاعات را از نقطه نظر کیفیت و قیمت در کوتاه ترین زمان ممکن به مشتریان ارائه خواهیم کرد.
ما برآنیم که با بهبود دائمی عملکرد خویش، رشد و توسعه پایداری را برای سازمان و ذینفعان تضمین نماییم.

پیام مدیرعامل

به نام خداوند جان و خرد
کزین برتر اندیشه برگزید

خداوند نام و خداوند جای
خداوند روزی و در بهمنای

خداوند کیوان و کردان سپهر
فروزنده ماه و ناهید و مهر

ما در شرکت پیشگامان فناوری اطلاعات هامون، خلاقیت و نوآوری را سرلوحه فعالیت های خود قرار دادیم و تلاش کردیم تا با بهره گیری از توان تخصصی خود، منشاء تحولی هرچند کوچک در عرصه فناوری اطلاعات، باشیم. رشد چشمگیر این شرکت در مدت زمانی بسیار کوتاه مدیون وفاداری، اعتماد و حمایت مشتریان خوب این مجموعه و تلاش شبانه روزی همکارانمان است.

ما تلاش کردیم تا بنیادی مستحکم در محیط چالش برانگیز امروزی بنا کنیم و مأموریت خود می دانیم تا این مسیر را در آینده ادامه داده و با گسترش روز افزون، هامون را به عنوان شرکتی پیشرو در زمینه فناوری اطلاعات، در عرصه های بین المللی معرفی نماییم.

ما هر روزه در محیط کسب و کار خود با چالش های جدیدی روبرو هستیم. سرعت و مقیاس تغییرات در این برهه زمانی بی سابقه است. ما برای غلبه بر این چالش ها، دست به ابتکاراتی زده ایم تا چشم اندازی وسیعتر نسبت به محیط پیرامون خود داشته باشیم و بتوانیم با سرعتی هرچه بیشتر تغییرات را شناسایی و به آن ها پاسخ دهیم.

می دانیم که هنوز در ابتدای راه هستیم اما متعهدیم که با تقویت توانایی های خود، در راه پیشبرد اهداف سازمان گام برداریم.

هادی حسین زاده – مدیر عامل

مقدمه:

شرکت پیشگامان فناوری اطلاعات هامون، با هدف ایجاد تحول در زمینه راهکارها و تجهیزات مبتنی بر فناوری اطلاعات، فعالیت خود را آغاز نمود. رشد چشمگیر شرکت هامون در طی مدت زمانی بسیار کوتاه مدیون وفاداری و حمایت مشتریانی است که مایلند برای تأمین نیازهای تخصصی و رو به رشد خود از خدمات، محصولات و پشتیبانی بی قید و شرط این شرکت بهره گیرند.

شرکت هامون با بهره گیری از کارشناسان متخصص، آکادمیک و با تجربه، در کنار کیفیت بی نظیر خدمات و پشتیبانی منحصر به فرد، پاسخی قاطع به حسن نیت مشتریان خود ارائه نموده است. هم اکنون شرکت هامون توانسته با برنامه ریزی، مدیریت دقیق و تسلط بر تمامی جنبه های فناوری اطلاعات و همچنین شناخت کافی از بازار، به عنوان شرکتی متخصص، صاحب نظر، رو به رشد و مشتری مدار شناخته شود. اخذ گواهینامه های ایزو در رابطه با "مشتری مداری" "مدیریت کیفیت"، "مدیریت شکایات" و گواهی نامه های متعدد "حسن انجام کار" مهر تأییدی بر این ادعا می باشد.

مهمترین فعالیت های هامون

شرکت هامون در راستای پاسخگویی به نیاز کشور در زمینه فناوری اطلاعات، و همچنین با در نظر گرفتن توان فنی و اجرایی این شرکت، فعالیت های خود را در چهار دسته اصلی تقسیم بندی کرده و با برنامه ریزی دقیق و مدیریت مستقل، اقدام به فعالیت نموده است.

راهکارهای ارائه شده توسط شرکت هامون به شرح ذیل می باشد:

*راهکارهای تخصصی مرکز داده شامل	*راهکارهای تخصصی امنیت شبکه و داده	*مشاوره و نگهداری
◀ مجازی سازی سرور	◀ پیشگیری از نشت اطلاعات	*مرکز آموزش
◀ مجازی سازی برنامه ها	◀ رمزنگاری اطلاعات	
◀ مجازی سازی ذخیره سازها	◀ حفاظت از پایگاه های اطلاعاتی	
◀ مجازی سازی دسکتاپ	◀ امنیت تجهیزات و کاربران نهایی	
◀ مجازی سازی شبکه	◀ امنیت ایمیل	
◀ پشتیبان گیری و بازیابی اطلاعات	◀ امنیت درگاه	
◀ طرح تداوم کسب و کار	◀ امنیت نرم افزارهای تحت وب	
◀ مانیتورینگ دیتاستر	◀ اعتبارسنجی و احراز هویت	
◀ ذخیره سازها	◀ حفاظت پیشرفته در برابر تهدیدات سایبری	

ارزش ها

- صداقت را سرلوحه کارمان قرار می دهیم.
- اعتماد و احترام به یکدیگر را باور داریم.
- مشتری مداری محور اصلی تصمیمات و اقدامات ماست.
- ایجاد محیط کاری سالم و دوستانه از افتخارات ماست.
- پیشرفت مبتنی بر خلاقیت و نوآوری در کانون توجه ماست.
- وظیفه شناسی و نظم و انضباط، فرهنگ کاری ماست.
- به کار و تصمیمات گروهی اعتقاد داریم و برای دستیابی به اهداف سازمانی از همکارانمان یاری می خواهیم.
- یادگیری و یاددهی از وظایف ماست.

DATA CENTER SOLUTION

راهکار هک مرکز داده

استفاده از تکنولوژی مجازی سازی تاثیر شگرفی بر روی سیستم های فناوری اطلاعات گذاشته است به طوری که این تکنولوژی کمک شایانی به سازمان ها در جهت رسیدن به اهداف سازمانی شان می کند.

قدرت معماری های مبتنی بر نرم افزار (SOFTWARE-DEFINED) باعث شده بسیاری از وابستگی ها و محدودیت های موجود در ساختارهای فیزیکی از بین رفته و به ما کمک می کند بتوانیم به صورت کامل و بهینه از سخت افزارهای موجود استفاده کنیم. همچنین به کمک این تکنولوژی ها استفاده از سیستم های فناوری اطلاعات بسیار مقرون به صرفه تر، توسعه پذیرتر و انعطاف پذیرتر شده است.

مزایای استفاده از تکنولوژی های مجازی سازی امروزه به حدی است که این تکنولوژی امروزه علاوه بر بحث مجازی سازی سرورها (SERVER VIRTUALIZATION) مباحث مجازی سازی شبکه (NETWORK VIRTUALIZATION) و همچنین (STORAGE VIRTUALIZATION) در بر می گیرد.

انواع مجازی سازی



مجازی سازی سرور



مجازی سازی دسکتاپ



مجازی سازی برنامه ها



مجازی سازی شبکه



مجازی سازی ذخیره ساز ها

DATA
CENTER
SOLUTIONS

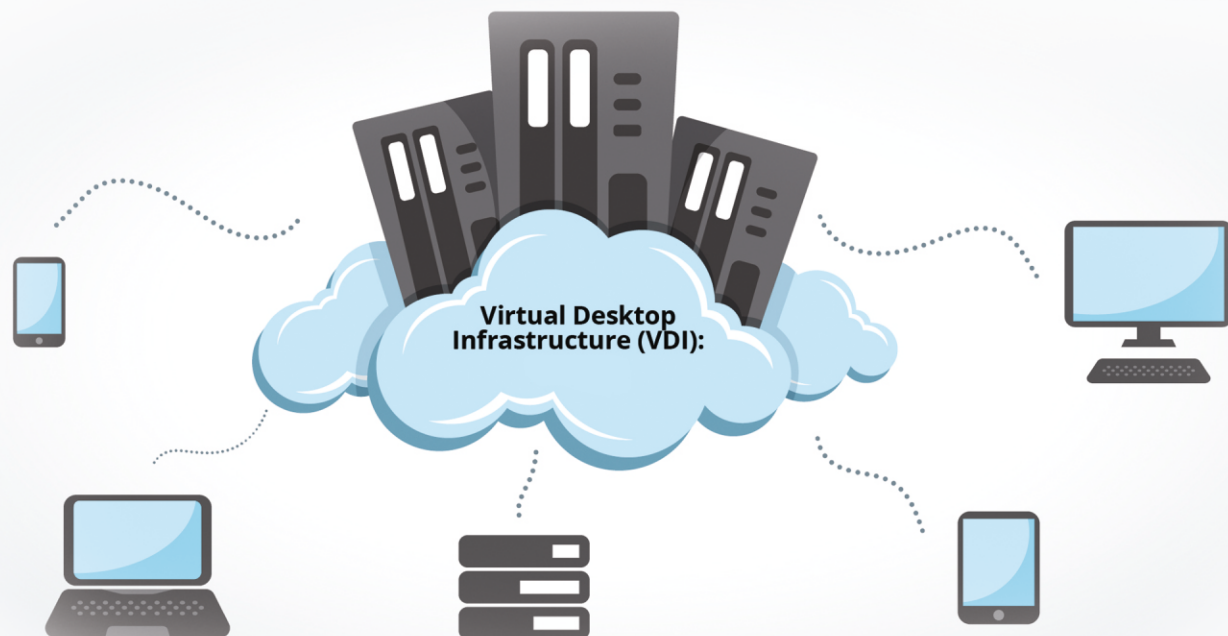
مجازی سازی دسکتاپ

DESKTOP VIRTUALIZATION

مجازی سازی دسکتاپ (DESKTOP VIRTUALIZATION) روشی جدید برای مدیریت محیط کاری کاربران ارائه می‌دهد. متدهای جدید ارائه دسکتاپ و نرم افزار به کاربر، انقلاب جدیدی در نحوه ارائه سرویس ها ایجاد کرده است. مجازی سازی دسکتاپ در حالت کلی باعث کاهش هزینه های سخت افزاری افزایش امنیت و افزایش کنترل روی کاربران می شود. VIRTUAL DESKTOP INFRASTRUCTURE (VDI) این امکان را برای مدیران شبکه فراهم می آورد تا دسکتاپ کاربران را بر روی زیرساختی مجازی، واقع در مرکز داده میزبانی و مدیریت کنند. این روش، سیستم عامل کامپیوترهای شخصی را از ماشین فیزیکی جدا می کند و ماشین مجازی حاصل را، به جای اینکه روی هارد دیسک کامپیوتر کاربر ذخیره کند، روی یک سرور مرکزی ذخیره می کند بنابراین وقتی کاربران در حال کار با ماشین خودشان هستند، همه برنامه ها و عملیات پردازشی و داده های استفاده شده توسط آنان روی سرور مرکزی اجرا و نگهداری می شود.

توسط این تکنولوژی، سیستم عامل کامپیوترهای شخصی از ماشین فیزیکی به ماشین مجازی تبدیل می شود و به جای اینکه پردازش بر روی کامپیوتر خود کاربر انجام شود، روی یک سرور مرکزی اجرا و ذخیره می شود. بنابراین وقتی کاربران در حال کار با ماشین خودشان هستند، تمام برنامه های مورد نیازشان به همراه عملیات پردازشی و داده های استفاده شده توسط آنان از روی سرور مرکزی اجرا و نگهداری می شود.

مجازی سازی دسکتاپ امکان دسترسی کاربران به کامپیوترهایشان با هر وسیله ای از قبیل کامپیوترهای شخصی، نوت بوک، SMART PHONE یا THIN CLIENT ها و ZERO CLIENT ها را می دهد. درک این فرآیند بسیار ساده است، به جای اینکه نسخه ای از سیستم عامل بر روی کامپیوتر کاربران به صورت محلی اجرا شود، بصورت مجازی در سرور اجرا خواهد شد و کاربران می توانند با استفاده از REMOTE DISPLAY PROTOCOL ها به کامپیوتر مجازی خود واقع در سرور وصل شده و سیستم عامل ویندوز ماشین خود (WINDOWS XP, VISTA, SEVEN, 10 و یا هر سیستم عامل دیگر) را به همراه کلیه نرم افزارهای نصب شده در آن اجرا کنند. با استفاده از این تکنولوژی کاربران می توانند از هر کلاینتی برای دسترسی به کامپیوتر خود استفاده کنند.



مجازی سازی سرور

SERVER VIRTUALIZATION

تکنولوژی مجازی سازی سرور (SERVER VIRTUALIZATION)، این امکان را برای مدیران سیستم فراهم می آورد که به کمک یک نرم افزار، یک سرور فیزیکی را به چندین سیستم مجازی کاملاً مستقل و ایزوله تبدیل کنند. این محیط های مجازی مستقل از هم با نام های VIRTUAL MACHINE, GUEST, INSTANCE, CONTAINER و غیره شناخته می شوند.

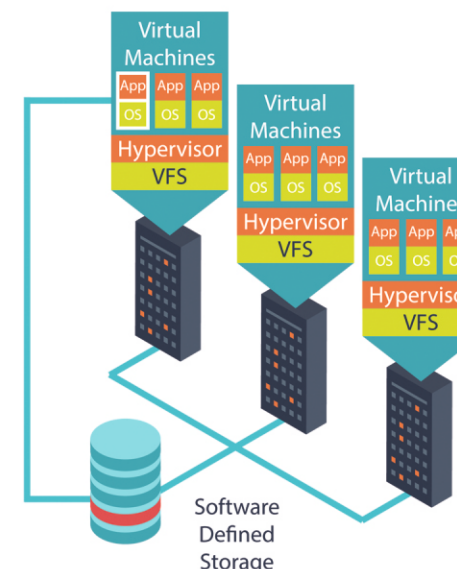
در هر دیتاستر به طور معمول تعداد زیادی سرور فیزیکی وجود دارد، که در بیشتر مواقع از این سرورها به صورت بهینه استفاده نمی شود. این عدم استفاده بهینه باعث هدر رفتن منابع گران قیمت سخت افزاری، سیستم های خنک کننده، مصرف برق و هزینه های نگهداری بالا می شود. مجازی سازی سرورها به این دلیل که اجازه می دهد چندین VIRTUAL SERVER که هر کدام دارای سیستم عامل و نرم افزارهای مربوط به خود هستند به صورت همزمان از منابع موجود به صورت اشتراکی استفاده کنند، موجب استفاده بهینه از منابع ارزشمند شما خواهد شد. VIRTUAL SERVER دقیقاً مانند سرورهای فیزیکی با سیستم عامل ها و نرم افزارهای شما رفتار خواهد کرد.

آیا سازمان شما به مجازی سازی سرور نیاز دارد؟

مجازی سازی سرور، به شما این امکان را می دهد که چندین و چند سیستم عامل و سرویس مختلف را بر روی یک سرور فیزیکی بصورت همزمان در اختیار داشته باشید. علاوه بر این در صورتی که به هر یک از موارد زیر در سازمان خود نیاز داشتید ناگزیر به استفاده از SERVER VIRTUALIZATION هستید:

- استفاده بهتر و بیشتر از نرم افزارها و سرویس های مختلف بدون نگرانی در مورد هزینه های سخت افزار، فضای فیزیکی و برق
- کاهش مدت زمانی که کارشناسان واحد آی تی درگیر راه اندازی، نصب، نگهداری و پشتیبانی از سرویس ها و نرم افزارهای مختلف هستند
- امکان استفاده از STORAGE VIRTUALIZATION که باعث کاهش DOWNTIME خواهد شد
- استفاده از SERVER VIRTUALIZATION اولین قدم سازمان شما در مهاجرت به محیطهای CLOUD خواهد بود.

نکته مهم این است که مجازی سازی سرورها چیزی بیشتر از صرفاً خرید سخت افزار و نصب چند نرم افزار است. مجازی سازی سرور یک تکنولوژی است که باید به صورت اصولی آن را فراگیرید.

SERVER
VIRTUALIZATION

مزایای اصلی مجازی سازی سرورها

- افزایش دسترسی پذیری سرورها
- کاهش هزینه های عملیاتی
- کاهش پیچیدگی های سرورهای فیزیکی
- افزایش کارایی نرم افزارها
- افزایش سرعت راه اندازی سرویس ها

* دسترسی در هر زمان، از هر کجا و با استفاده از هر دستگاهی

با پیاده سازی این تکنولوژی، کاربران می توانند در هر لحظه و از هر جایی بسته به سیاست سازمان و با استفاده از هر دستگاهی مانند لب تاپ، تبلت و ... به صورت کاملاً امن به دسکتاپ سازمانی متصل شده و با تجربه کاربری بسیار مناسبی از آن استفاده کند.

* کاهش هزینه های پشتیبانی و نگهداری

هزینه پشتیبانی از PC های سازمان یکی از شاخص ترین هزینه های IT می باشد. که با مهاجرت به سمت مجازی سازی دسکتاپ این هزینه ها به شدت کاهش می یابد.

* عدم وابستگی به سخت افزار

وابستگی سیستم عامل و برنامه های کاربران به سخت افزار به طور کامل حذف خواهد شد و کاربران با استفاده از هر سخت افزاری به صورت یکپارچه از دسکتاپ خود استفاده خواهند کرد. همچنین با استفاده از VDI امکان استفاده از نرم افزارهای قدیمی و NON-COMPATIBLE بر روی سیستم عامل های جدید فراهم می شود. همچنین امکان استفاده از نرم افزارهای 32 BIT روی سیستم های 64 BIT و بالعکس فراهم می شود.

* پهنای باند بسیار کم

به واسطه استفاده از پروتکل PCOIP میزان پهنای باند مورد استفاده هر کاربر برای اتصال به دسکتاپ خود کاهش می یابد و میزان آن به 32 تا 64 KBPS می رسد.

* امکان استفاده از (BYOD) یا دستگاههای شخصی کاربر

با استفاده از VDI این امکان برای شما فراهم می شود که دسکتاپ کاربران را حتی روی دستگاه های شخصی کاربران در اختیار آنها قرار دهید. در این حالت کاربران در خانه یا در هر جایی می توانند به دسکتاپ خود دسترسی داشته باشند، بدون اینکه نگران مسائل امنیتی آنها باشید.

* مزایا و ویژگی ها

VDI مخفف عبارت VIRTUAL DESKTOP INFRASTRUCTURE است و بیشتر از اینکه معرفی کننده یک محصول باشد معرفی کننده یک تکنولوژی است. شرکت های VMWARE و CITRIX به ترتیب با ارائه محصولات HORIZON VIEW و CITRIX VIRTUAL APPS AND DESKTOP از معروفترین ارائه دهنده گان تکنولوژی VDI در جهان هستند. در ادامه به برخی از مزایا و ویژگی های این تکنولوژی اشاره شده است :

* بهترین انتخاب برای محیط های کلاسی، فروشگاه ها و مراکز آزمایشگاهی

بهترین انتخاب برای محیط هایی که در آنها چندین کاربر به صورت اشتراکی از یک سخت افزار برای انجام وظایف خود استفاده می کنند، استفاده از این تکنولوژی است. در این محیط ها، دسکتاپ هر کاربر پس از اتمام کارش و ریستارت شدن سیستم، به حالت اولیه خود باز خواهد گشت.

* امکان مهاجرت ساده تر به سیستم عامل های جدید و بروزرسانی نرم افزار ها

با پیاده سازی این زیرساخت می توان کلیه دسکتاپ های سازمان را در طول چند ساعت به سیستم عامل های جدید ارتقا داد. همچنین این روند برای ارتقا نرم افزارها نیز وجود دارد که در این خصوص کاربر تنها با انجام یکبار LOGOFF و LOGON نرم افزارهای ارتقا یافته را در اختیار خواهد داشت. در این حالت ادمین شبکه به جای درگیر شدن برای نصب ویندوز و نرم افزارها، فقط کافیس GOLD IMAGE مربوط به VDI را آپدیت کند. نکته جالب توجه اینکه با انجام این ارتقا کلیه اطلاعات و همچنین پروفایل کاربر بدون هیچگونه تغییری باقی خواهد ماند.

* افزایش امنیت با متمرکز سازی دسکتاپ ها در دیتا سنتر

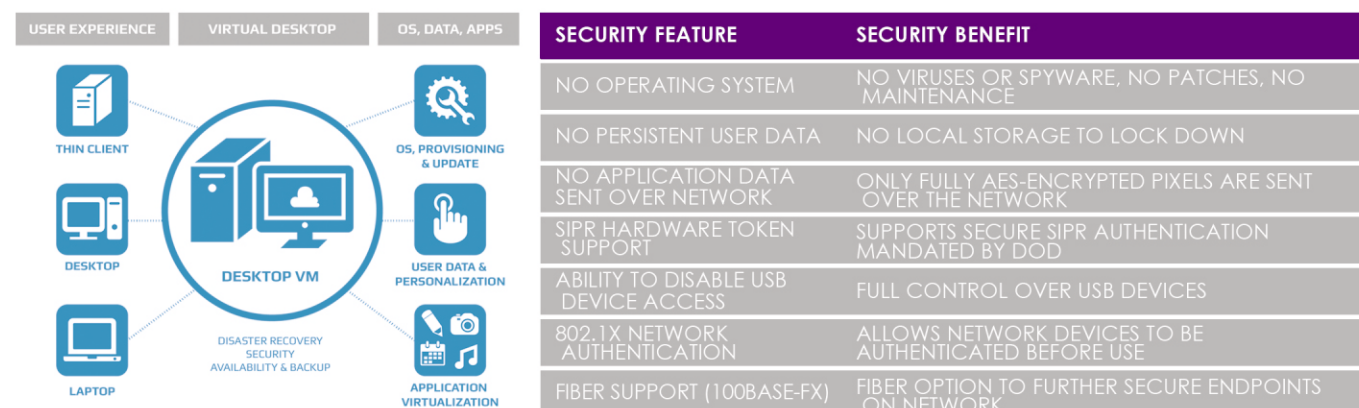
به دلیل تمرکز دسکتاپ کاربران درون دیتاسنتر، می توان دسکتاپ های سازمان را به اندازه سرورهای سازمان امن سازی نمود و مدیر سازمان این اطمینان را داشته باشد که کلیه کاربران بر اساس سیاست های سازمان به سرویس های سازمان دسترسی پیدا می کنند.

* ارتقا منابع دسکتاپ کاربران

شما به صورت پویا می توانید منابعی که در اختیار کاربران می گذارید را مدیریت کرده و کنترل نمایید. این ویژگی به شما اجازه می دهد در هر لحظه منابع کاربر را افزایش یا کاهش دهید.

* کاهش منابع پردازی

اشتراک منابع پردازی برای کلیه دسکتاپ ها این امکان را فراهم می آورد که با وجود استفاده کاربران از یک دسکتاپ مستقل منابع پردازی بر اساس نیاز به آنها تخصیص داده شود و این منابع به صورت شناور می تواند در حال تغییر باشد و کاربران تنها در صورت نیاز از آن منابع استفاده می کنند و در مواقعی که مورد استفاده قرار نمی گیرد، دسکتاپ های دیگر می توانند از آن استفاده کنند.



مجازی سازی استوریج

STORAGE VIRTUALIZATION

مجازی سازی استوریج (STORAGE VIRTUALIZATION) عبارت است از تجميع دیسک های موجود بر روی سرورها یا استوریج های مختلف به شکلی که این دیسک های مختلف به صورت تجميع شده و به صورت یک STORAGE DEVICE واحد نمایش داده شوند. این استوریج ها قابلیت مدیریت از یک نقطه و کنسول واحد را خواهند داشت.

این تکنولوژی با استفاده از یک نرم افزار امکان استفاده از دیسک های مختلف و تجميع آنها را به گونه ای فراهم می کند که این دیسک ها، به صورت یک STORAGE DEVICE واحد قابل استفاده در محیط های مجازی و توسط ماشین های مجازی هستند.

نرم افزاری که وظیفه ایجاد و مدیریت این فضا را بر عهده دارد درخواست های I/O مربوطه را از سمت سرورهای فیزیکی یا مجازی دریافت و آنها را بر روی دیسکی مناسب که جزئی از POOL ایجاد شده است ذخیره می کند. برای کاربری که از این محیط استفاده می کند هیچ تفاوتی بین VIRTUAL STORAGE و یا یک استوریج کاملاً مستقل فیزیکی به لحاظ I/O وجود نخواهد داشت.

دیسک هایی که برای این محیط استفاده می شوند، می توانند به صورت یک دیسک و یا چندین دیسک که به کمک RAID از تکنولوژی های RAID هم در این محیط استفاده کنید. PROTECTION استفاده می کنند، باشند. بنا براین شما این امکان را خواهید داشت که از تکنولوژی های RAID هم در این محیط استفاده کنید.

انواع STORAGE VIRTUALIZATION

دو مدل مختلف برای STORAGE VIRTUALIZATION وجود دارد.

- FILE-BASED
- BLOCK-BASED

مجازی سازی استوریج ها به روش FILE-BASED کاربردهای خاصی مثل استفاده به عنوان (NAS (NETWORK ATTACHED-STORAGE را دارد که از پروتکل های (SMB (SERVER MESSAGE BLOCK و NETWORK FILE SYSTEM (NFS استفاده می کنند.

اما اصلی ترین هدف استفاده از VIRTUAL STORAGE ها به صورت BLOCK-BASED است که کاربرد اصلی آنها در محیط های مجازی برای استفاده VIRTUAL MACHINE هاست.

مزایای استفاده از STORAGE VIRTUALIZATION

- بسیار مقیاس پذیر است
- امکان اضافه کردن یا کم کردن ساده ی فضای استوریج
- مدیریت آسان و کارآمد بر روی فضای موجود
- کاهش هزینه های سخت افزاری و منابع
- افزایش قابلیت اطمینان و کارایی
- افزایش انعطاف پذیری و قابلیت توسعه

مجازی سازی نرم افزارها

APPLICATION VIRTUALIZATION

مجازی سازی نرم افزارها (APPLICATION VIRTUALIZATION) تکنولوژی است که به کمک آن ادمین سیستم، دیگر نیازی به نصب نرم افزارها به صورت LOCAL بر روی سیستم کاربران نخواهد داشت.

از دید کاربران، نرم افزارهای کاربردی آنها دقیقاً همان کارایی قبلی را خواهد داشت به طوری که کاربر هیچ تفاوتی، به لحاظ کارایی، بین نرم افزاری که به صورت LOCAL روی سیستم او نصب شده بود و یا نرم افزاری که به کمک APPLICATION VIRTUALIZATION در اختیار او قرار می گیرد، احساس نمی کند. کاربران دقیقاً مانند قبل می توانند با نرم افزار، ماوس، کیبورد، پرینتر، یو اس بی دیوایس ها و سایر تجهیزات خود کار کنند.

ممکن است تفاوت های ظریف و نامحسوسی برای کاربران در بکارگیری این تکنولوژی وجود داشته باشد اما در نهایت کاربر همان تجربه کاری که قبلاً داشته را خواهد داشت.

نحوه کار APPLICATION VIRTUALIZATION چگونه است ؟

اگرچه روش های مختلفی برای استفاده از تکنولوژی APPLICATION VIRTUALIZATION وجود دارد، اما هدف ما در اینجا ارائه نرم افزارهای کاربردی و مورد نیاز کاربران به گونه ایست که مجبور به نصب آنها بر روی تک تک سیستم ها نباشیم. بلکه به جای آن تمامی نرم افزارهای مورد نیاز کاربر بر روی سرورهایی داخل دیتاستر سازمان نصب و سپس از داخل دیتاستر در اختیار کاربران قرار می گیرند.

اساساً، با استفاده از تکنولوژی APPLICATION VIRTUALIZATION و به کمک پروتکل های REMOTE DISPLAY مختلف مانند MICROSOFT REMOTEFX, CITRIX HDX, VMWARE VIEW PCOIP OR BLAST EXTREME، تصویر نرم افزارهای کاربردی در اختیار کاربر قرار می گیرد، به گونه ای که کاربر، همانند نرم افزارهایی که بر روی سیستمش و بصورت LOCAL نصب شده است، بتواند از آن ها استفاده کند. هر درخواستی که کاربر بر روی نرم افزار ارسال می کند، به سمت دیتاستر و جایی که نرم افزار در آن قرار دارد ارسال می شود.



مزایای استفاده از APPLICATION VIRTUALIZATION

• این تکنولوژی یکی از موثرترین و بهترین راهکارها برای سازمان ها در مورد نصب و نگهداری نرم افزارهای کاربران است. به گونه ای که یکی از مهم ترین مزایای این تکنولوژی این است که مدیران سیستم به جای اینکه مجبور باشند یک نرم افزار را بر روی سیستم تک تک کاربران نصب کنند، آن نرم افزار را یکبار بر روی یک سرور نصب کرده و آن را در اختیار کاربران قرار می دهند. همچنین این کار پروسه اعمال تغییرات و یا آپدیت نرم افزارها را بسیار آسانتر خواهد کرد.

• از طرف دیگر مدیران سیستم می توانند به کمک این تکنولوژی کنترل کاملی بر نرم افزار ها و دسترسی های کاربران به آن نرم افزارها داشته باشند. برای مثال در صورتی که بخواهید دسترسی یک کاربر به نرم افزار خاصی را بگیرید این کار به سادگی قابل انجام خواهد بود. بدون اینکه نیازی به UNINSTALL کردن آن نرم افزار از سیستم کاربر باشد.

• APPLICATION VIRTUALIZATION این امکان را برای شما فراهم خواهد کرد که بتوانید نرم افزارهایی را که باهم CONFLICT دارند و یا نرم افزارهایی که بر روی سیستم عامل های جدیدتر اجرا نمی شوند را بدون مشکل در هر محیطی و در کنار یکدیگر اجرا و استفاده کنید.

• شما می توانید به نرم افزارهای خود از طریق هر دستگاهی مانند PC, LAPTOP, TABLET AND MOBILE و هر سیستم عاملی مانند WINDOWS, LINUX, MAC, ANDROID AND IOS دسترسی داشته باشید. در صورتی که دستگاه شما به سرقت برود شما مطمئن خواهید بود که اطلاعات حیاتی سازمان شما بدون مشکل در دیتاستر ذخیره شده اند.

پشتیبان گیری و بازیابی اطلاعات

BACKUP AND DATA RECOVERY

به طور کلی به فرآیند ایجاد و ذخیره سازی یک نسخه کپی از اطلاعات، که در مواقع لزوم بتواند از سازمان در مقابل از دست رفتن اطلاعات محافظت کند فرآیند پشتیبانگیری و بازیابی اطلاعات گفته می شود. گاهی به این نوع بازیابی اطلاعات، بازیابی عملیاتی (OPERATIONALRECOVERY) نیز اطلاق می شود. بازگردانی اطلاعات می تواند در محل اصلی اطلاعات یا محلی جایگزین اتفاق بیفتند تا از آسیب و از دست رفتن اطلاعات جلوگیری کند.

اهمیت پشتیبانگیری و بازیابی اطلاعات در چیست ؟

هدف اصلی از نسخه های پشتیبان، ایجاد و نگه داری یک نسخه از اطلاعات اصلی سازمان و بازگردانی آنها در زمانی است که اطلاعات اصلی سازمان از بین رفته باشد. از دست رفتن اطلاعات سازمان ممکن است دلایل متعددی از جمله مشکلات نرم افزاری و سخت افزاری، خرابی دیتا، خطاها و خرابکاری های انسانی مانند ویروس ها و باج افزارها و یا پاک شدن تصادفی دیتا، داشته باشد. در چنین مواقعی که اتفاقات پیش بینی نشده باعث از بین رفتن دیتای شما می شود، نسخه های پشتیبان این امکان را برای شما فراهم خواهند کرد تا به زمان قبل از این اتفاق بازگردید و سرویس های شما به کار خود ادامه دهند. نگهداری دیتاها بر روی مدیاها و دستگاه های مختلف برای اطمینان از قابل بازگشت بودن دیتاهای حیاتی سازمان شما بسیار اهمیت دارند. این مدیاها و دستگاه های مختلف می توانند دستگاه های ساده ای مانند EXTERNAL DRIVE یا USB STICK ها و یا دستگاه های پیشرفته ذخیره سازی اطلاعات مانند DISK STORAGE , CLOUD STORAGE CONTAINER یا TAPE DRIVE ها باشند. این دستگاه های جایگزین می توانند در همان محلی که نسخه اصلی اطلاعات شما وجود دارد و یا در محلی به غیر از محل نگهداری اطلاعات اصلی شما باشد.

DISK-TO-DISK-TO-TAPE (D2D2T)

این روش یکی از روش های نگهداری و آرشیو اطلاعات است که طی آن نسخه های اول پشتیبان بر روی DISK STORAGE ها ذخیره می شوند و سپس یک نسخه از همین اطلاعات بر روی TAPE DRIVE ها کپی می شود.

سیستم های پشتیبانگیری بر روی سیستم های DISK BASED و TAPE BASED هر کدام مزایا و مشکلاتی دارند. در بسیاری از موارد برای سازمان ها بسیار اهمیت دارد که نسخه های پشتیبان موجود در مواقع ضروری بلافاصله و در کوتاهترین زمان ممکن در دسترس و قابل بازگردانی باشند. برای چنین سازمان هایی مدت زمان بازگردانی داده ها از روی TAPE DRIVE ها قابل قبول نیست. برای این سازمان ها، استفاده از دستگاه های DISK BASED بسیار اهمیت دارد. زیرا انتقال دیتا بر روی این دستگاه ها ۴ تا ۵ برابر بیشتر از دستگاه های TAPE است. از طرفی دیگر TAPE DRIVE ها به دلیل ظرفیت بالاتر و قیمت کمتر نسبت به دیسک ها، گزینه ای کاملاً به صرفه تر و اقتصادی تر از دیسک ها برای آرشیو اطلاعات و نگهداری آنها برای مدت زمان طولانی است. همچنین TAPE DRIVE این قابلیت را به شما خواهد داد که پس از کپی کردن اطلاعات، آن را از دستگاه جدا کرده و در محلی امن نگهداری کنید.

روش پشتیبانگیری D2D2T از مزایای DISK ها و TAPE ها به صورت همزمان استفاده می کند. این روش به شما به عنوان ادمین سیستم این اجازه را می دهد که ابتدا نسخه های پشتیبان خود را بر روی دیسک ذخیره کنید، به این ترتیب در مواقع ضروری به سرعت می توانید به فایل های پشتیبان خود دسترسی داشته و آنها را بازیابی کنید. همچنین می توانید یک نسخه از فایل های پشتیبان را بر روی TAPE کپی کنید. به این ترتیب و با استفاده از TAPE DRIVE این امکان فراهم می شود که بتوان یک نسخه از اطلاعات را به خارج از محل اصلی، منتقل کرد. این مسئله برای سناریوهای بازیابی از حادثه (DISASTER RECOVERY) بسیار اهمیت دارد.

مجازی سازی شبکه

NETWORK VIRTUALIZATION

مجازی سازی شبکه، تکنولوژی است که امکان ایجاد یک شبکه مجازی را به گونه ای فراهم می کند که این شبکه مجازی از تجهیزات سخت افزاری و لایه سخت افزار شبکه جدا باشد. در طی یک دهه گذشته بسیاری از سازمان ها به صورت گسترده به سمت تکنولوژی مجازی سازی سوق پیدا کرده اند و تکنولوژی مجازی سازی شبکه، یکی از این تکنولوژی هاست. تکنولوژی مجازی سازی شبکه، این امکان را فراهم می کند که بتوان سرویس ها و ارتباطاتی را که در گذشته توسط تجهیزات فیزیکی برقرار می شدند، در قالب یک شبکه مجازی ارائه داد. مجازی سازی شبکه علاوه بر ارائه سرویس های لایه ۲ و ۳ مانند روتینگ و سوئیچینگ میتواند سرویس های مربوط به لایه های ۴ تا ۷ نظیر FIREWALL و LOAD BALANCING را هم فراهم آورد. مجازی سازی شبکه بسیاری از چالش هایی را که امروزه در دیتاسنتر ها با آنها مواجه هستیم، برطرف می کند و به سازمان ها اجازه می دهد سرویس های شبکه را بدون درگیری با پیچیدگی های سخت افزار و بر حسب نیاز توسعه، پیاده سازی و مدیریت کرد.

اعمال مجازی سازی بر روی شبکه

زمانی که شما مجازی سازی شبکه را انجام می دهید، مجازی سازی یک دیدگاه منطقی مبتنی بر نرم افزار، از سخت افزارها و نرم افزارهای تجهیزات شبکه ای شما مانند روتر ها، سوئیچ ها و غیره ایجاد می کند. تجهیزات فیزیکی شبکه، تنها وظیفه ی انتقال PACKET ها را بر عهده خواهند داشت، درحالیکه شبکه مجازی به صورت هوشمند وظیفه ایجاد و مدیریت سرویس های مختلف شبکه را بر عهده دارد. این کار باعث آسانتر شدن مدیریت سرویس های شبکه بدون درگیر شدن با پیچیدگی های سخت افزار را فراهم می کند.

مزایای مجازی سازی شبکه
ایجاد بهره وری بهتر از سیستم شبکه
بالا بردن سرعت تبادلات
راحتی دسترسی به شبکه
صرفه جویی در هزینه
ایجاد تجمیع سرویس های سازمان در یک بخش
پشتیبانی و مدیریت بهتر شبکه
یکپارچه سازی منابع داخل شبکه
کم شدن هزینه نگهداری و همین طور نیروی انسانی



BACKUP AND DATA RECOVERY

برای دستیابی به بهترین نتیجه در مورد نسخه های پشتیبان، پشتیبانگیری از اطلاعات باید به صورت منظم و بر اساس زمانبندی مشخصی انجام پذیرد. فاصله ی زمانی زیاد بین نسخه های پشتیبان، امکان از دست رفتن اطلاعات در بازه های زمانی مورد نظر سازمان را بالا می برد. نگهداری نسخه های متعدد از فایل های پشتیبان، با اینکه نیاز به فضای ذخیره سازی زیادی دارد، اما به شما این اطمینان و انعطاف پذیری را می دهد که در مواقعی که دیتای شما به دلیل خرابی و یا خرابکاری و ... از بین رفته است، اطلاعات خود را به هر زمانی که مایل بودید بازگردانید.

OPERATIONAL RECOVERY VS. DISASTER RECOVERY

تهدیدات بسیار متعددی وجود دارند که موجودیت هر سازمان را تهدید می کند، یکی از این تهدیدات از بین رفتن اطلاعات است. از دست رفتن اطلاعات می تواند پیامدهای متعددی برای سازمان داشته باشد از جمله از دست دادن زمان، از دست دادن ثروت، از دست دادن فرصت ها و ... به عبارتی شما برای پیشگیری و اجتناب از، از دست دادن زمان، ثروت و فرصت ها نیاز به راهکاری دارید که در حوادث پیش بینی نشده به سرعت قابلیت بازیابی از حادثه را برای شما فراهم آورد. این بازگردانی کسب و کار شما می تواند به دو شکل DISASTER RECOVERY و یا OPERATIONAL RECOVERY باشد، اما اینکه شما به کدامیک از آنها نیاز دارید؟ پاسخ این پرسش هر دو است.

بسیاری از سازمان ها از نسخه های پشتیبان خود برای بازیابی اطلاعات در هنگام حوادث پیش بینی نشده استفاده می کنند. در حالی که واژه پشتیبانگیری و بازیابی اطلاعات (BACKUP AND RECOVERY) با واژه بازیابی از حادثه (DISASTER RECOVERY) دارای تفاوت هایی است.

OPERATIONAL RECOVERY (BACKUP AND RECOVERY)

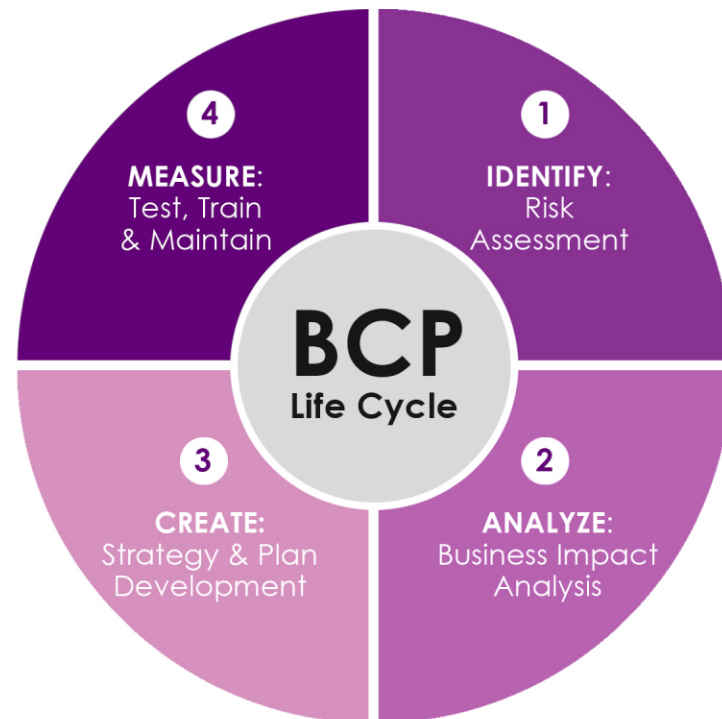
نسخه های پشتیبان به شما کمک می کنند تا در مواقعی که دیتای اصلی شما دچار مشکل می شوند، با جایگزینی آنها با نسخه های قبلی که در فایل های پشتیبان وجود دارند، سیستم را به حالت عادی برگردانید. نسخه های پشتیبان شامل نسخه های مختلفی از فایل ها، به صورت (POINT-IN-TIME) می باشد که به شما این امکان و انعطاف پذیری را می دهد که به هر زمانی که نیاز داشتید برگردید یا از این نسخه ها به عنوان آرشیو اطلاعات استفاده کنید. برخی سازمان ها با توجه به ماهیتشان نیاز به نگهداری و آرشیو اطلاعات برای زمان های طولانی دارند با این حال، با توجه به نوع سازمان، ممکن است نسخه های جدیدتر اهمیت بیشتری نسبت به نسخه های خیلی قدیمی تر داشته باشند.

DISASTER RECOVERY

راهکارهای بازیابی از حادثه به سازمان کمک می کند تا در مواقعی که دیتاسنتر و یا سخت افزارها با مشکل جدی مواجه می شوند تمامی سرویس ها بر روی دیتاسنتر یا سخت افزار دیگری که از قبل برای این حوادث پیش بینی کرده اید، بلافاصله شروع به کار کنند. در حقیقت در بحث DISASTER RECOVERY زمانی که شما با خرابی نرم افزار، سخت افزار و یا از دست رفتن دیتاسنتر مواجه می شوید کل سرویس های شما بر روی دیتاسنتر دوم شما با فاصله ی زمانی بسیار کم شروع به سرویس دهی خواهند کرد. زمانیکه مشکل دیتا سنتر اصلی شما رفع شده و مجددا شروع به کار کند شما این قابلیت را خواهید داشت که سرویس ها را مجدداً به سایت اصلی، بازگردانید. در حقیقت بر خلاف نسخه پشتیبان، DISASTER RECOVERY اطلاعات را بر روی دیتاسنتر دوم MIRROR می کند که نتیجه این کار اجتناب از، از دست رفتن اطلاعات و بازیابی سرویس ها در عرض چند دقیقه است.

برای مثال تکنولوژی هایی مانند MIRRORING این امکان را فراهم می آورند که بتوانید همواره یک نسخه UP-TO-DATE از اطلاعات خود را در یک مکان فیزیکی جداگانه نگهداری کنید. اینکار باعث خواهد شد در صورتی که یکی از محل های نگهداری اطلاعات دچار مشکل شد، یک نسخه SYNC شده از اطلاعات را در دسترس داشته باشید.

انجام تحلیل های اثرات تجاری (BUSINESS IMPACT ANALYSIS) می تواند ضعف های احتمالی و همچنین تأثیر یک فاجعه بر روی هر یک از واحدها را نشان دهد. گزارشات BIA به سازمان این امکان را می دهد که سرویس ها و سیستم های حیاتی خود را شناخته و در تدوین طرح تداوم کسب و کار، آنها را در اولویت قرار دهد.



هر طرح تداوم کسب و کار از سه المان اساسی تشکیل شده است: انعطاف پذیری، بازیابی و احتمال وقوع

- یک سازمان با شناسایی سرویس ها و سیستم های حیاتی خود و همچنین در نظر گرفتن احتمال وقوع هر حادثه، می تواند انعطاف پذیری خود را افزایش دهد. در نظر گرفتن تمامی جوانب یک حادثه و آمادگی برای هر سناریویی می تواند در زمان وقوع حائثه انعطاف پذیری شما را افزایش دهد
- بازگردانی هر چه سریعتر سرویس ها در زمان وقوع حادثه بسیار پر اهمیت است. شناسایی سرویس ها و سیستم های حیاتی و با اولویت بالاتر در زمان وقوع حادثه و اقدام به بازیابی سرویس ها از اهمیت بالایی برخوردار است.
- در نظر گرفتن احتمال وقوع هر حادثه و انجام سناریوهای مختلف قبل از وقوع حوادث می تواند کمک فراوانی برای سازمان شما در مواجهه با حوادث مختلف باشد. تعیین و تبیین وظایف به افراد موجب مشخص شدن وظایف هر فرد در هنگام وقوع حوادث می شود این وظایف می تواند شامل تعویض سخت افزارهای آسیب دیده، ارزیابی خسارت، برقراری ارتباط با پیمانکاران برای مشاوره و باشد.



تداوم کسب و کار

BUSINESS CONTINUITY

BUSINESS CONTINUITY عبارت است از توانایی سازمان برای تداوم کسب و کار خود در حین یا پس از به وقوع پیوستن حوادث. در واقع BUSINESS CONTINUITY به مجموعه ای از فرآیندها و دستورالعمل ها اطلاق می شود که توسط یک سازمان پیاده سازی می شود تا سازمان بتواند بعد یا در هنگام بروز یک فاجعه یا DISASTER به کار خود و روند فعالیتی روزمره خود ادامه دهد. با استفاده از پیاده سازی یک طرح تداوم کسب و کار یا BCP، سازمان ها در واقع به دنبال حفاظت از سرویس های حساس و حیاتی خود هستند تا بتوانند بعد از بروز فاجعه یا DISASTER این سرویس ها را بلافاصله به مدار برگردانند و تجارت و کسب و کار خود را ادامه دهند.

این نوع طراحی و برنامه ریزی، به سازمان اجازه می دهد تا بتواند سرویس ها را به سرعت بازیابی و به سطح عملیاتی کامل خود در سریعترین زمان و با بالاترین کیفیت ممکن برساند. در BCP معمولاً تمامی فرآیندهای حساس تجاری سازمانی و همه عملیات های مهم تجاری تحت پوشش قرار می گیرند BCP شامل تعداد متعددی از عوامل غیر قابل پیش بینی مانند، سیل، زلزله، توفان، آتش سوزی، حملات سایبری و ... می شود. BCP برای تمامی سازمان ها با هر اندازه و از هر نوعی، بسیار پر اهمیت است. با اینکه حفظ و تداوم کسب و کار در هر شرایطی برای سازمان های بزرگ بسیار حیاتی است اما این امر برای تمامی سازمان ها ممکن است امکانپذیر نباشد.

اولین قدم در تدوین طرح تداوم کسب و کار این است که تصمیم بگیرید کدام سرویس یا عملکرد سازمان شما تحت هیچ شرایطی نباید تحت تاثیر قرار بگیرد و باید به کار خود ادامه دهد. زمانی که سرویس ها و کامپوننت های حیاتی سازمان شما مشخص گردید، می توانید در مورد مکانیزم های حفظ و نگهداری آن سرویس ها تصمیم گیری کنید.

مانیتورینگ دیتا سنتر

DATA CENTER MONITORING

مانیتورینگ دیتا سنتر عبارت است از نظارت، مدیریت و انجام اقداماتی در دیتاسنتر، تا اطمینان حاصل شود که وضعیت دیتا سنتر مطابق با شرایط و نیازمندی های سازمان است. این پروسه شامل اقداماتی است که به صورت MANUAL یا با استفاده از ابزارهایی و بصورت اتوماتیک انجام می شود تا دیتا سنتر بهترین عملکرد را داشته باشد. انجام اقدامات فوق، این اطمینان را می دهد که تمامی سرویس ها بدون وقفه و مشکل در اختیار سرویس گیرندگان قرار می گیرد.

نظارت بر مراکز داده، فرآیندی متشکل از اقدامات گسترده است که تمرکز آن بر روی کلیه زیر ساخت مرکز داده است. به طور معمول نظارت بر مراکز داده توسط ابزارهای اتوماتیکی انجام می گیرد و آمار و گزارشات دقیقی از وضعیت و کارایی مرکز داده در اختیار شما قرار می دهند که شما، به عنوان ادمین سیستم، می توانید با استفاده از این گزارشات، نسبت به رفع مشکلات موجود اقدام نمائید.

به طور معمول نظارت بر مراکز داده شامل موارد زیر می شود:

- نظارت بر سرورهای موجود در دیتاسنتر به لحاظ کارایی (PERFORMANCE)، امنیت و سایر موارد
- نظارت و مدیریت بر تجهیزات شبکه و ارتباطی و رفع مشکلات مربوط به این تجهیزات
- اطمینان از در دسترس بودن تمامی تجهیزات شبکه اعم از سرورها، تجهیزات شبکه، استوریج ها و سرویس ها

نحوه عملکرد و ویژگی های سیستم های مانیتورینگ:

سیستم های مانیتورینگ این امکان را فراهم می کنند تا بتوان کلیه تجهیزات موجود در دیتاسنتر را به صورت متمرکز مدیریت کرد. این سیستم ها به شما اجازه می دهند تا با استفاده از پروتکل های SNMP, HTTPS و سایر پروتکل ها به تجهیزات دیتاسنتر متصل شده و اطلاعات آنها را دریافت و آنها را پیکربندی کنید.

- این سیستم ها می توانند به صورت REAL-TIME اطلاعات مربوط به تجهیزات را دریافت و آنها را تجزیه و تحلیل کند.
- نرم افزارهای مانیتورینگ می توانند اطلاعات را تحلیل و پیش از بروز حوادث ناگوار شما را از احتمال وقوع آنها آگاه سازند.
- امکان دریافت و تحلیل و فیلتر کردن اطلاعاتی که برای شما حائز اهمیت است.
- تحلیل و آنالیز اطلاعات دریافتی که به شما در پیش بینی تجهیزات و سرویس های مورد نیاز خود در آینده بسیار کمک خواهد کرد.
- استفاده از پروتکل های مختلف از جمله SNMP, HTTPS, MODBUS, BACNET, WIEGAND, RF که امکان ارتباط با تمامی تجهیزات را فراهم می کند.

تکنولوژی ذخیره سازی

SAN AND NAS STORAGE

تکنولوژی ذخیره سازی (SAN) STORAGE AREA NETWORK یکی از پر کاربردترین تکنولوژی های ذخیره سازی برای سیستم های حساس سازمانی و سرویس هایی است که نیاز به THROUGHPUT بالا و LATENCY پایین دارند.

پیشرفت روز افزون تکنولوژی های ذخیره سازی SAN و همچنین استفاده از ذخیره سازی های ALL-FLASH باعث افزایش PERFORMANCE و کاهش LATENCY در این ذخیره سازها شده است. ذخیره سازی متمرکز داده ها بر روی SHARED STORAGE ها این امکان را به سازمان ها می دهد تا از متدها و ابزارهای مناسب برای مباحث امنیتی، DATA PROTECTION و DISASTER RECOVERY استفاده کنند.

SAN ها ذخیره سازهایی هستند که به صورت BLOCK-BASED کار می کنند و این قابلیت را دارند که سرورها را با استفاده از یک ارتباط پر سرعت به LUN های ایجاد شده روی خودشان متصل کنند. یک LUN مجموعه ایست از BLOCK ها که از ترکیب چندین دیسک ایجاد شده و برای استفاده در اختیار یک سرور قرار میگیرد. بنابراین سرور میتواند این LUN را در اختیار گرفته و با فایل سیستم خود FORMAT و مانند دیسک های LOCAL روی خود سرور برای ذخیره سازی اطلاعات از آن استفاده کند.

موارد استفاده از SAN STORAGE ها

معمولا SAN STORAGE ها به دلیل PERFORMANCE بالای که دارند در محیط هایی مورد استفاده قرار می گیرند که از نرم افزارهای بسیار PERFORMANCE-SENSITIVE استفاده می کنند. نرم افزارهایی مانند :

- ORACLE DATABASES
- LARGE VIRTUALIZATION DEPLOYMENTS USING VMWARE, KVM, OR MICROSOFT HYPER-V
- MICROSOFT SQL SERVER DATABASES
- LARGE VIRTUAL DESKTOP INFRASTRUCTURES (VDIS)
- SAP OR OTHER LARGE ERP OR CRM ENVIRONMENTS

آشنایی با پروتکل های مورد استفاده SAN STORAGE ها

• FIBRE CHANNEL PROTOCOL (FCP) : متداول ترین و پر استفاده ترین پروتکل مورد استفاده در شبکه های SAN پروتکل FC است. پروتکل FC می تواند دستورات SCSI را بر روی کابل های فیبر منتقل نماید. حدود ۷۰ تا ۸۰ درصد SAN STORAGE ها در دنیا از این پروتکل استفاده می کنند

• (ISCSI) INTERNET SMALL COMPUTER SYSTEM INTERFACE : بعد از FC دومین پروتکل پر کاربرد مورد استفاده در شبکه های SAN پروتکل ISCSI است که می تواند دستورات SCSI را داخل فریم های اترنت ENCAPSULATE کرده و از طریق شبکه مبتنی بر IP منتقل نماید. حدود ۱۰ تا ۱۵ درصد SAN STORAGE ها در دنیا از این پروتکل استفاده می کنند.

• (FCOE) FIBRE CHANNEL OVER ETHERNET : تنها ۵ درصد SAN STORAGE های موجود در دنیا از این پروتکل برای ارتباط استفاده می کنند. FCOE به عنوان یک پروتکل استاندارد این اجازه را به شما می دهد که بتوانید فریم های FIBER CHANNEL را بر روی لینک های ETHERNET منتقل کنید. که اینکار الزام وجود شبکه های جداگانه برای LAN و SAN را از بین خواهد برد.

FCOE NETWORK

دیتا سنتر ها به صورت معمول تشکیل شده اند از یک شبکه ETHERNET LAN و یک شبکه اختصاصی SAN (FC) FIBER CHANNEL. اما با استفاده از تکنولوژی FCOE این امکان فراهم می شود که این دو شبکه مجزا را در یک بستر یکپارچه قرار دهیم. FCOE به عنوان یک پروتکل استاندارد این اجازه را به شما می دهد که بتوانید فریم های FIBER CHANNEL را بر روی لینک های ETHERNET منتقل کنید. که اینکار الزام وجود شبکه های جداگانه برای LAN و SAN را از بین خواهد برد. در شبکه های LAN از NIC و در شبکه های SAN از HBA به عنوان کارت رابط شبکه استفاده می شود اما در تکنولوژی FCOE هر دوی این تجهیزات تبدیل به یک کارت به نام CNA می شوند که به تنهایی قادر است هم ترافیک موجود در LAN و هم ترافیک موجود در شبکه SAN را انتقال دهد.

ذخیره سازی مبتنی بر TAPE

TAPE ARCHIVING

ذخیره سازی و نگهداری اطلاعات بر روی TAPE DEVICE ها یکی از مقرون به صرفه ترین و مطمئن ترین روش های نگهداری اطلاعات است. هزینه ای که برای ذخیره سازی هر گیگابایت اطلاعات بر روی TAPE ها انجام می دهید قابل قیاس با هزینه دیسک ها نیست. اما استفاده از TAPE ها فقط کپی اطلاعات روی آنها و نگهداری آنها نیست. نگهداری و آرشیو اطلاعات بر روی TAPE نیازمند طراحی و برنامه ریزی است تا در صورت نیاز امکان بازیابی اطلاعات از روی TAPE فراهم باشد.

با توجه به تمرکز بیشتر سازمان ها بر پشتیبانگیری اطلاعات بر روی دیسک ها، VIRTUAL TAPE LIBRARY ها و سایر ذخیره سازهای مبتنی بر دیسک به نظر می رسد که تکنولوژی TAPE تکنولوژی قدیمی و از رده خارج است اما واقعیت چیز دیگری است و ذخیره سازهای مبتنی بر TAPE هنوز هم کاربردهای مخصوص به خود را دارند.

نسخه های پشتیبانی که از اطلاعات گرفته می شود برای اهداف مشخصی نگهداری می شوند:

- نسخه هایی که برای بازیابی فایل ها و پوشه ها، بلافاصله بعد از زمانی که بنا به دلیلی دیتای اصلی دچار مشکل شود، گرفته می شوند، باید همواره در دسترس بوده و قابلیت بازگردانی دیتای از دست رفته را در کوتاهترین زمان ممکن داشته باشند.
- نسخه هایی که برای کاربردهای کوتاه مدت و برای ۹۰ روز یا کمتر نگهداری می شوند، باید قابلیت بازگردانی یک یا چند فایل و همینطور قابلیت بازگردانی کل سیستم را در طول مدت چند دقیقه یا چند ساعت داشته باشند.
- نسخه هایی که برای کاربردهای بلند مدت و آرشیو اطلاعات از چندین ماه تا همیشه استفاده می شوند. برای نگهداری چنین اطلاعاتی استفاده از دیسک ها به هیچ وجه توجیه اقتصادی ندارد و بهترین گزینه استفاده از TAPE DEVICE هاست.

مزایای استفاده از TAPE

- **ظرفیت بالا:** TAPE CARTRIDGE ها در حال حاضر با استفاده از تکنولوژی LTO قابلیت نگهداری 30 ترابایت دیتا را بر روی یک CARTRIDGE دارند.
- **کارایی بالا:** با سرعت انتقال ۱ ترابایت داده در هر ساعت، اکنون می توانید اطلاعات خود را در عرض چند ثانیه و یا چند دقیقه بازیابی کنید.
- **هزینه کمتر نسبت به دیسک**
- **مصرف انرژی کمتر:** مطالعات نشان می دهد دستگاه های TAPE مصرف برق و تولید گرمای کمتری نسبت به دیسک ها دارند.
- **قابلیت انتقال:** با استفاده از TAPE می توانید به سادگی اطلاعات خود را بر روی TAPE ذخیره کرده و آن را به مکانی دیگر و مطمئن منتقل کنید.
- **قابلیت اطمینان بالاتر:** میزان خطاهای موجود بر روی TAPE ها به مراتب کمتر از دیسک هاست، همچنین TAPE ها از برخی خطراتی که دیسک ها را تهدید می کنند، مانند ویروسی شدن، مصون هستند.
- **طول عمر بالاتر**
- **قابلیت سازگاری:** دستگاه های TAPE قابلیت کار کردن با مجموعه ی عظیمی از نرم افزار های مختلف مثل BACKUP EXEC, NETBACKUP و VEEAM BACKUP AND REPLICATION و غیره را دارند.

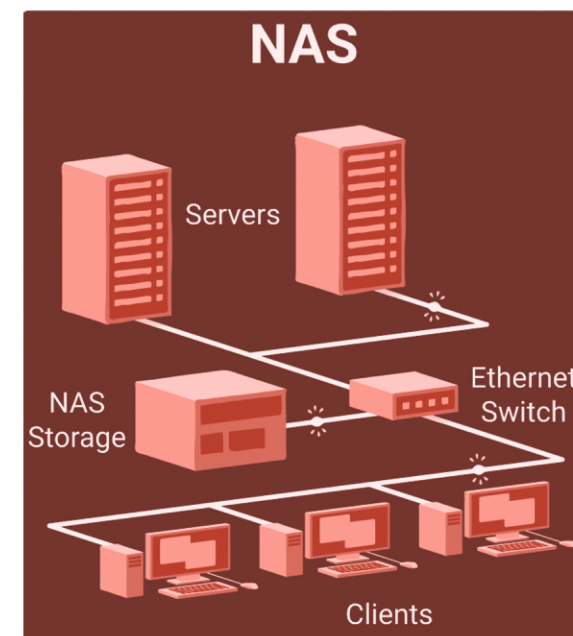
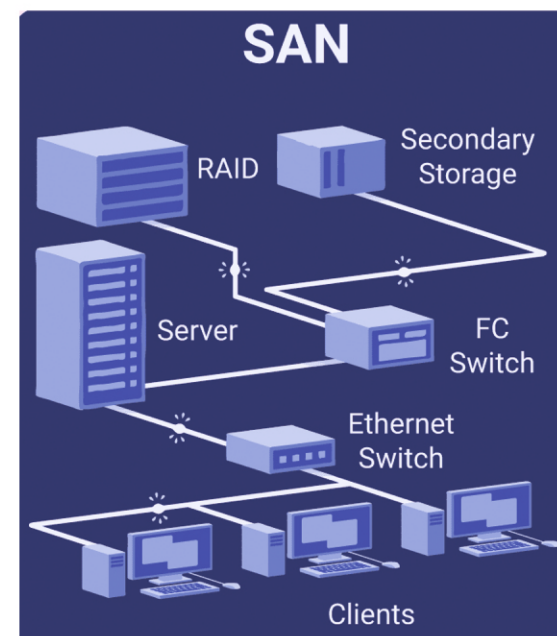
مقایسه ذخیره سازها

SAN VS. NAS

SAN ها و NAS ها دستگاه هایی هستند که امکان ذخیره سازی متمرکز داده و به اشتراک گذاری آنها بین چندین سرور را فراهم می آورند. با این حال NAS ها دستگاه هایی ETHERNET BASED هستند در حالی که SAN ها قابلیت کار با ETHERNET و FIBER CHANNEL را دارند. علاوه بر این در حالی که SAN ها بر روی افزایش PERFORMANCE و کاهش LATENCY متمرکز شده اند NAS ها بیشتر بر روی افزایش قدرت مدیریت، استفاده آسانتر و کاهش قیمت تمام شده تمرکز دارند. NAS ها بر روی خود یک سیستم عامل دارند که وظیفه مدیریت دستگاه را بر عهده می گیرد که در حقیقت NAS ها را به یک FILE SERVER که بر روی یک سیستم عامل WINDOWS یا LINUX پیاده سازی شده است شبیه می کند.

یک شبکه SAN در حالت کلی از سه کامپوننت اصلی تشکیل شده است: کابل ها، HBA ها که بر روی STORAGE و هاست ها قرار می گیرند و سوئیچ ها (SAN SWITCH) که ارتباط هاست ها و STORAGE را فراهم می کنند.

SAN SWITCH ها دستگاه هایی هستند که هاست ها را به LUN هایی که در داخل SAN STORAGE ایجاد شده متصل می سازند و وظیفه انتقال ترافیک های SAN را بر عهده دارد. اکثر SAN SWITCH ها به صورت FIBER CHANNEL کار می کنند که مورد استفاده اکثر SAN STORAGE های موجود در بازار است. SAN SWITCH ها با بررسی و مشخص کردن فرستنده و گیرنده اطلاعات را منتقل می کنند.



INFORMATION PROTECTION AND CYBER SECURITY SOLUTIONS

راهکار های محافظت از اطلاعات و امنیت سایبری

پیشگیری از نشت اطلاعات

DATA LOSS PREVENTION

حفاظت از اطلاعات و اجرای سیاست های مربوط به آن در محیط های سازمانی هرگز آسان نبوده است. اما امروزه با چالشهای جدیدی در این زمینه روبرو هستیم. اطلاعات حساس از طریق محیط های ابری و دستگاه های قابل حمل نظیر موبایل و تبلت از محیط حفاظت شده شبکه خارج می شوند. تعداد حملات هدفمند سایبری رو به افزایش است و مجرمان سایبری از روش های جدید و موثرتری برای عبور از لایه های امنیتی سنتی و سرقت اطلاعات سازمان ها استفاده می کنند. تمامی این عوامل باعث می شوند محافظت از اطلاعات سازمانی در برابر نشت و یا سرقت اطلاعات بیش از پیش مشکل باشد. پس چگونه میتوان اطلاعات سازمانی را در این محیط پر چالش مدیریت و محافظت نمود؟ و یک استراتژی موفق و کامل برای حفاظت از اطلاعات در برابر مسائلی چون تخریب محدوده های امنیتی، افزایش روزافزون حملات و تعامل با رفتار و انتظارات کاربران چگونه باید باشد؟

DATA LOSS PREVENTION که به اختصار DLP نامیده می شود با رویکردی جامع به مساله حفاظت از اطلاعات و با در نظر گرفتن واقعیت های محیط های ابری و موبایل که امروزه مورد استفاده سازمان ها می باشد، به سوالات فوق پاسخ می دهد. با DLP شما می توانید:

- * به تمامی مکان هایی که اطلاعات شما در آن ذخیره شده اند نظیر محیط های ابری، موبایل، شبکه، ایستگاه های کاری و ذخیره سازها پی ببرید.
- * چگونگی استفاده از اطلاعات و اینکه آیا کاربران اطلاعات در داخل یا خارج از شبکه هستند نظارت کنید.
- * اطلاعات خود را صرف نظر از نحوه استفاده و یا محیط ذخیره شده از نشت و یا سرقت محافظت نمایید.

رویکرد و تکنولوژی های جدید در محصول DLP قابلیت سازمان ها در حفاظت از اطلاعات را به محدوده فضای ابری و دستگاه های همراه گسترش می دهد. این به شما این امکان را می دهد تا سیاستهای امنیتی و انطباق با استاندارد های امنیت اطلاعات را فراتر از محدوده شبکه خود گسترش دهید. همچنین با استفاده از امکاناتی همچون روش های نصب مطمئن، ابزارهای مدیریت سیاست و وقایع بصری و پوشش همه جانبه تمامی مجراهای اطلاعاتی پر خطر، هزینه تمام شده پیاده سازی کمتری را برای سازمان ایجاد میکند.

DLP for Endpoint

DLP for Network

DLP for Email Gateway

DLP for Web Gateway

INFORMATION PROTECTION AND CYBER SECURITY

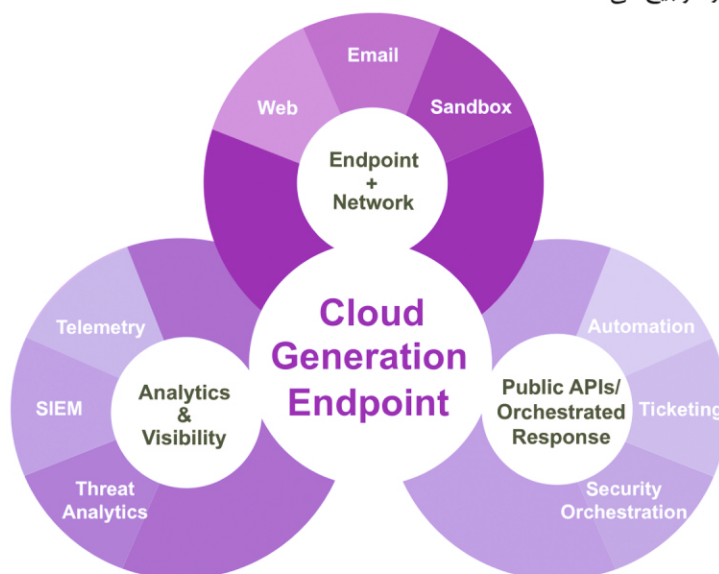


امنیت تجهیزات و کاربران نهایی

ENDPOINT SECURITY

امروزه، با تحول و رشد پیوسته محیط های فناوری اطلاعات، حمله کنندگان سایبری از روش های بسیار پیچیده تری جهت نفوذ به شبکه های رایانه ی و تجهیزات نهایی (EndPoints) که آخرین خط دفاعی می باشند، استفاده می کنند. در حالیکه حملات باج افزارهایی نظیر WannaCry و Petya شیوع بسیاری یافته است سازمان ها بسیار بیشتر نگران اینگونه حملات و خسارات و اختلالات ناشی از آن می باشند. علاوه بر این حمله کنندگان استفاده از تکنیک های جدیدی نظیر حملات file-less (استقرار در حافظه به جای هارد دیسک) و "living off the land" (استفاده از ابزار های موجود در رایانه جهت حمله) را گسترش داده اند که باعث تهدیدات جدی تری می گردند.

با توجه به این موضوع چه راهکاری برای مقابله با حملات سایبری می تواند موثر باشد؟ مدیریت چندین محصول با فناوری های گوناگون جهت محافظت در برابر انواع مخاطرات می تواند چالش برانگیز باشد. خصوصاً آنکه گستره جغرافیایی استفاده از آنها وسیع و سیستم عامل و پلتفرم های مورد محافظت مختلف باشند. با محدودیت منابع و بودجه، کارشناسان امنیت استفاده از محصولات یکپارچه، با مدیریت آسان و فناوری های سازگار که سطح امنیت را بصورت سرتاسری افزایش می دهد را ترجیح می دهند.



رمزنگاری اطلاعات

ENCRYPTION

محافظت از اطلاعات بر روی تمام سیستم ها و ذخیره سازهای قابل حمل

ENDPOINT ENCRYPTION

GATEWAY EMAIL ENCRYPTION

FILE SHARE ENCRYPTION

DESKTOP EMAIL ENCRYPTION

حفاظت از پایگاه های اطلاعاتی

DATABASE SECURITY

امکانات امنیت پایگاه های اطلاعاتی که توسط تولید کنندگان سیستم های مدیریت پایگاه داده رابطه ای در اختیار استفاده کنندگان قرار می گیرد تنها بخش کوچکی از تصویر کلی امنیت پایگاه های اطلاعاتی می باشد. درحالیکه برخی از قابلیت های امنیتی حساس در پلاتفرم های RDBMS موجود پیاده سازی شده اند، بسیاری از سرویس های حساس در خصوص امنیت پایگاه های اطلاعاتی بزرگ در این پلاتفرم ها وجود ندارند. از این رو درخواست جهت ابزارهای امنیت پایگاه های اطلاعاتی که توسط سایر تولید کنندگان ارائه می گردد، وجود دارد.

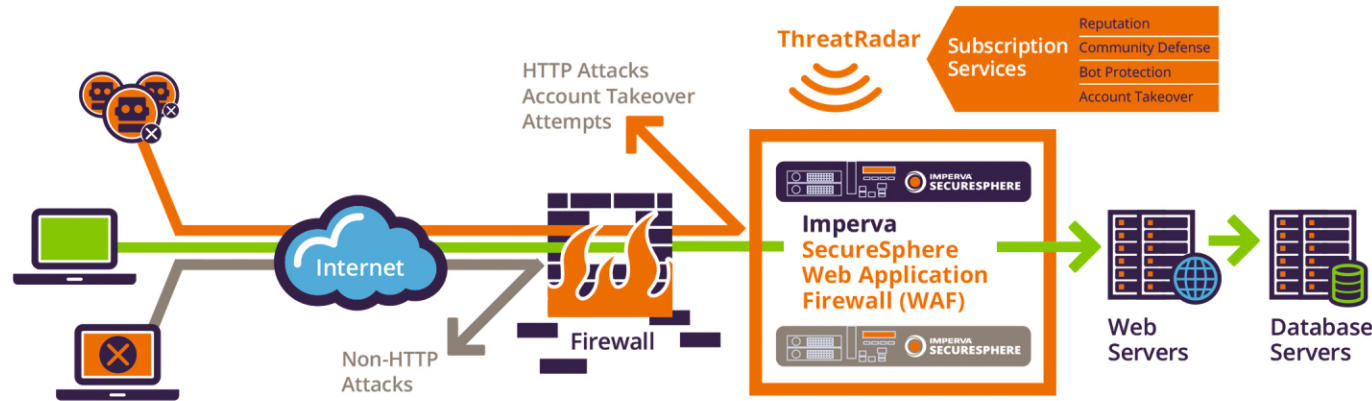
سطح امنیتی که توسط این محصولات امنیت پایگاه های اطلاعاتی ارائه می گردد، بخصوص در موارد ارزیابی آسیب پذیری پایگاه داده ، رمزنگاری، انطباق پایگاه داده، مدیریت داده های آزمایشی، نشانه گذاری و پوشش داده بسیار فراتر از سطحی است که توسط تولید کنندگان پلاتفرم های RDBMS به مشتریان ارائه می گردد. در نتیجه، دلایل زیادی برای سازمان ها وجود دارد تا به استفاده از این محصولات روی آورند. از آنجا که نرم افزارها و فرآیندهای سازمانی گوناگونی متکی به پایگاه های اطلاعاتی هستند، نیازمندی های آنها برای افزایش سطح امنیت پایگاه داده توسط این محصولات نیز مختلف می باشد.

- ▶ DATABASE ACTIVITY MONITORING
- ▶ DATABASE VULNERABILITY ASSESSMENT
- ▶ ENCRYPTION
- ▶ DATABASE COMPLIANCE
- ▶ TEST DATA MANAGEMENT
- ▶ TOKENIZATION
- ▶ DATA MASKING

امنیت نرم افزارهای تحت وب

WEB APPLICATION FIREWALL

راهکارهای WAF جهت حفاظت نرم افزارهای تحت وب در برابر حملات مختلفی از جمله INJECTION ATTACKS و حملات DOS در لایه APPLICATION و همچنین تشخیص ترافیک های غیر معمول به وب سرورها مود استفاده قرار می گیرد. همچنین نظارت و کنترل دسترسی به نرم افزارهای تحت وب و جمع آوری لاگ های دسترسی به سرور وب از قابلیت های راهکار های WAF می باشد.



اعتبار سنجی و احراز هویت

VALIDATION & ID PROTECTION

جلوگیری از دسترسی غیر مجاز به اطلاعات حساس و برنامه های تحت شبکه حملات پیچیده صورت گرفته بیانگر این نکته هستند که شیوه استفاده از کلمه های عبور برای جلوگیری از نشت اطلاعات، نفوذ به شبکه های سازمانی و سرقت شناسه های کاربری کافی نمی باشد. مجموع شناسه های کاربری به سرقت رفته در سال ۲۰۱۵ با رشد ۲۳ درصدی به رقم ۴۲۹ میلیون مورد رسید که تبعات آن شامل خسارات مالی، از دست رفتن اعتبار کسب و کارها و سرقت دارایی های با مالکیت معنوی از شرکت ها بوده است. راهکار های پیشرو، کاربر پسند و قدرتمند اعتبار سنجی و احراز هویت با پشتیبانی از فضای ابری جهت ارائه سرویس احراز هویت می باشد که می تواند دسترسی ایمن به اطلاعات حساس و نرم افزارهای کاربری را در هر زمان و هر کجا و با استفاده از هر دستگاهی، ارائه نماید. یک راهکار اعتبار سنجی و احراز هویت به شما کمک می کند تا از دسترسی های غیر مجاز به شبکه و نرم افزار های کاربردی های حساس جلوگیری نمایید، سازمان خود را با استانداردهای حفاظت از اطلاعات سازگار کنید و بهترین شیوه های امنیت سایبری را پیاده سازی نمایید. همچنین این راهکار شما را قادر می سازد تا امنیت سازمان خود را هم زمان با تامین دسترسی های کاربران داخل و خارج از سازمان، همکاران تجاری، پیمانکاران و تامین کنندگان و مشتریان حفظ نمایید.

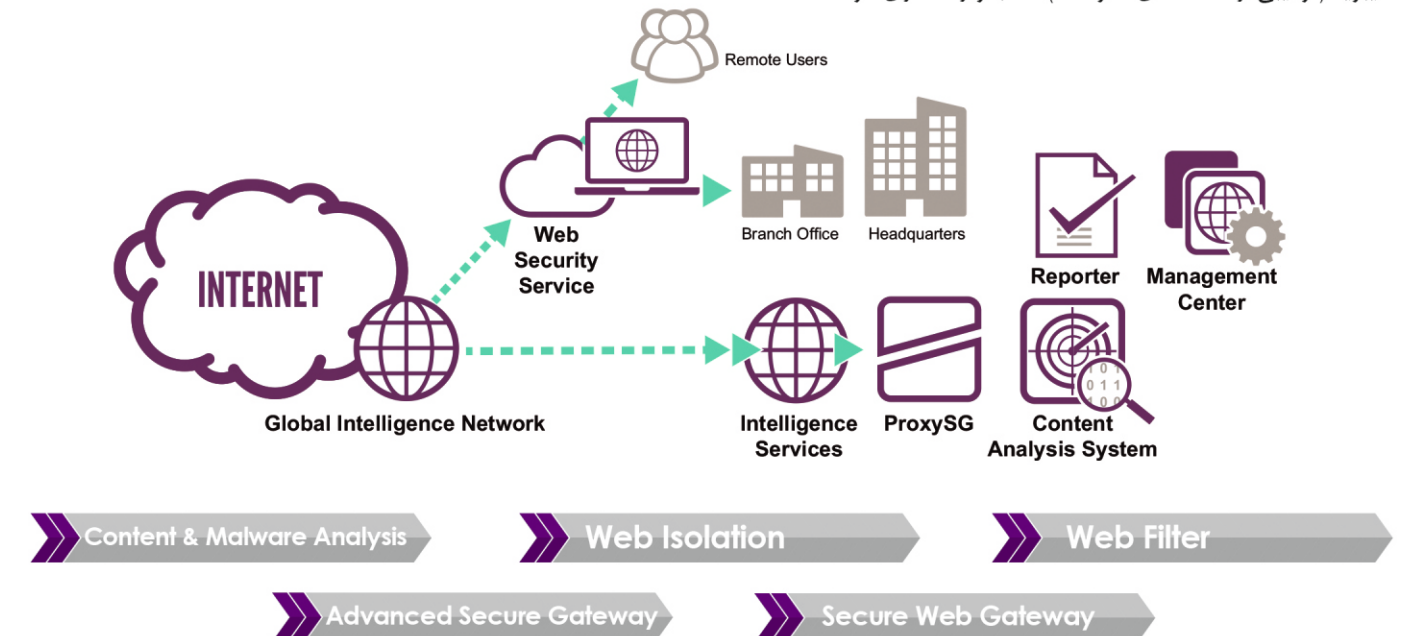
NETWORK SECURITY SOLUTION

راهکار های امنیت شبکه

امنیت درگاه

GATEWAY SECURITY

درگاه های امنیت وب با استفاده از URL FILTERING، دفاع پیشرفته در برابر مخاطرات سایبری و موتورهای ضد بد افزار برای محافظت از کاربران اینترنت سازمان در برابر تهدیدات موجود در اینترنت و همچنین کمک به سازمان در جهت اعمال سیاست های مدیریتی در خصوص استفاده از اینترنت، مورد استفاده می باشند. راهکارهای درگاه امنیت وب می توانند به صورت تجهیز سخت افزاری و یا به صورت مجازی سازی شده و همچنین بصورت سرویس فضای ابری و همچنین هیبرید (ترکیبی از حالت های ذکر شده) نصب و راه اندازی گردند.



امنیت ایمیل

EMAIL SECURITY

امنیت ایمیل، شامل کلیه انواع ایمیل های سازمانی، ایمیل های مبتنی بر ابر و یا ایمیل های ترکیبی، با درک واضح و واقع بینانه ای نسبت به آنچه ممکن است اتفاق بافتد، آغاز می شود. ایمیل رایج ترین راه در میان مجرمان سایبری برای نفوذ به شبکه سازمان ها و گسترش تهدیدات امنیتی است. بر اساس گزارشات مختلف منتشر شده، بسیاری از سازمان ها بصورت مداوم و از طریق ایمیل های تجاری حاوی بدافزارها، مورد حمله قرار گرفته اند و در 71% موارد، گروه های مهاجم از حملات فیشینگ برای هدف حمله قرار دادن سازمان ها، استفاده کرده اند.

با افزایش تعداد این حملات، مقابله با آن ها نیز افزایش یافته است. شناسایی و متوقف کردن حملات پیشرفته و ZERO-DAY ها، در مقایسه با تهدیدات قدیمی تر، بسیار دشوار است و آنتی ویروس های استاندارد مبتنی بر امضاء، عملاً در مقابل آن ها ناکارآمد هستند. این حملات پیچیده عموماً از DOMAIN SPOOFING و پیوندهای مخرب تعبیه شده در ایمیل ها برای گسترش استفاده می کنند.

برای بسیاری از سازمان ها امنیت ایمیل حیاتی بوده و به لطف راهکارهای جامع برای کنترل زیرساخت ایمیل، می توانند از امنیت آن اطمینان حاصل کنند.



حفاظت پیشرفته در برابر تهدیدات سایبری

ADVANCED THREAT PROTECTION

امروزه اکثر سازمان های بزرگ محیط های IT گسترده ای دارند که پیچیدگی آن به شکل فزاینده ای رو به افزایش است. در بسیاری از این سازمان ها راهکارهایی جهت انجام وظایف خاص پیاده سازی شده اند. بنابراین این سازمان ها نیاز به راهکاری جهت محافظت سیستم ها دارند که بیشترین بازدهی و بالاترین سطح محافظت در تمام لایه ها را با یکپارچگی با دیگر راهکارهای امنیت IT در جهت به اشتراک گذاری اطلاعات و هماهنگی در پاسخگویی به رخدادهای شبکه فراهم نماید.

در پلاتفرم دفاع سایبری یکپارچه (INTEGRATED CYBER DEFENSE PLATFORM) محصولات امنیتی (چه به صورت استقرار در شبکه محلی و یا در فضای ابری) با یکدیگر در ارتباط هستند تا کاربران، اطلاعات، پیغام ها و فضای وب را با هماهنگی کامل محافظت نمایند.

*امنیت سرور و ایستگاه کاری (ENDPOINT SECURITY)
ENDPOINT DETECTION AND RESPONSE (EDR)

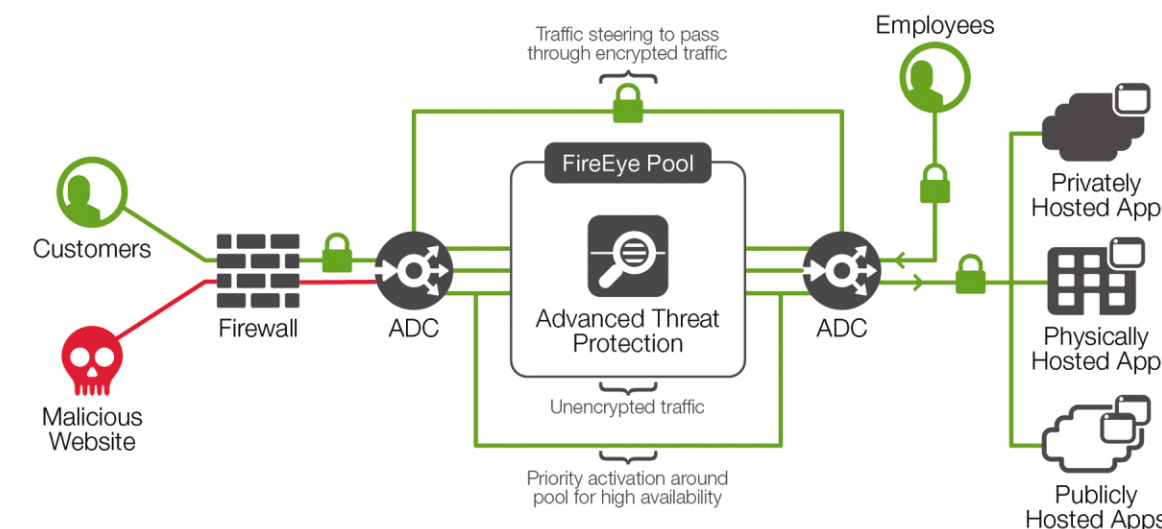
*تحلیل محتوا و بد افزارها (CONTENT & MALWARE ANALYSIS)

*حفاظت پیشرفته برای ایمیل (ADVANCED THREAT PROTECTION FOR EMAIL)

*مدیریت ترافیک رمز گذاری شده (ENCRYPTED TRAFFIC MANAGEMENT)

*امنیت درگاه وب (SECURE WEB GATEWAY)
WEB ISOLATION , WEB FILTER

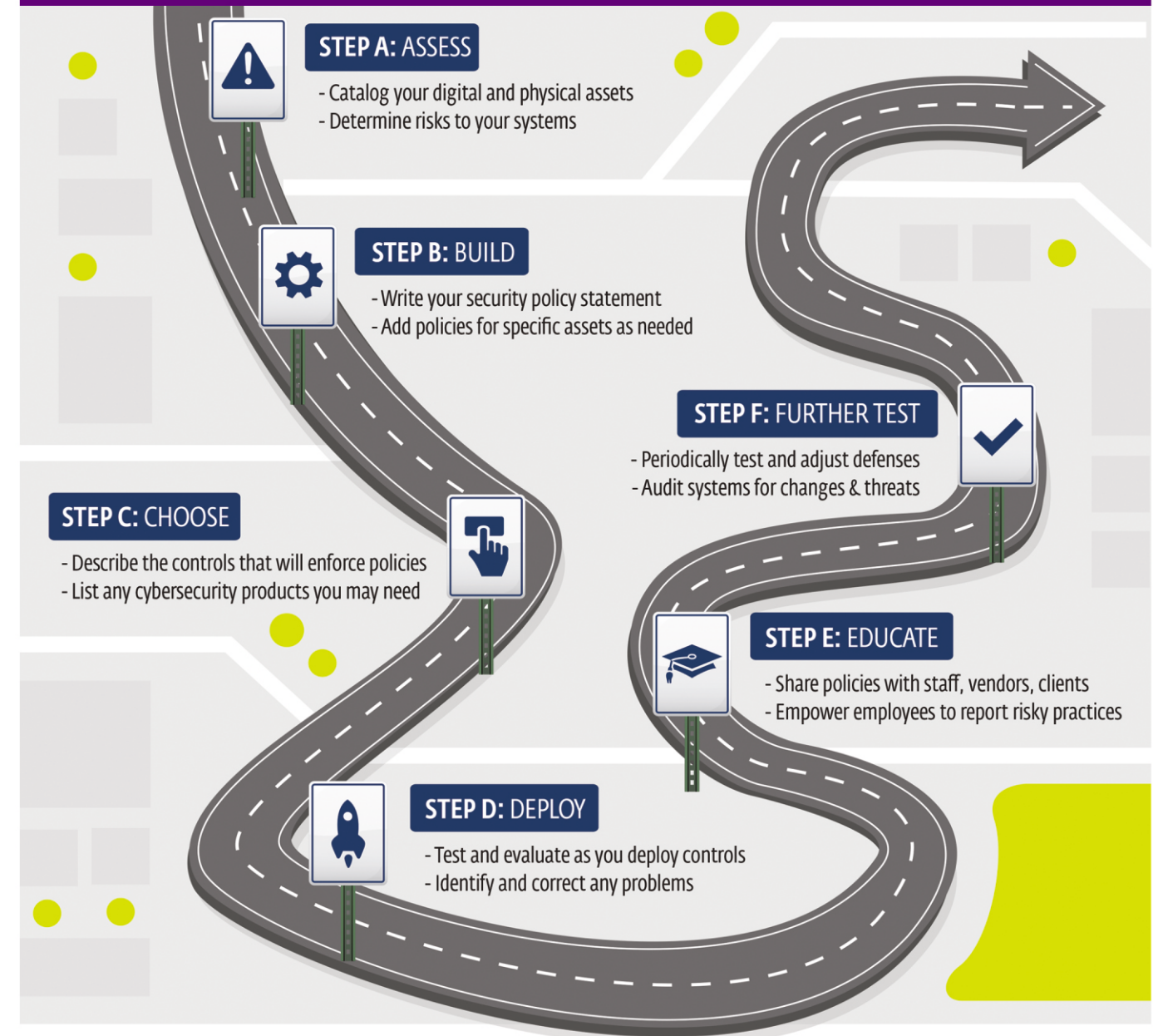
*امنیت نرم افزارهای تحت وب (WEB APPLICATION FIREWALL)



INFORMATION PROTECTION



CYBERSECURITY ROAD MAP



CONSULTATION AND MAINTENANCE

مشاوره و نگهداری

شرکت هامون با بکارگیری شیوه های استاندارد مبتنی بر ISO و ITIL و با بهره گیری از سال ها تجربه و توان فنی خود، آماده ارائه کلیه خدمات مشاوره، طراحی اجرا، پشتیبانی و تأمین امنیت می باشد.

مدیریت ما با هدف پیشبرد نوآوری بگونه ایست که تضمین می کند ایده درست در زمان درست اجرا می شود، تا توانایی های سیستم موجود را بطور مداوم به حداکثر بهره وری ارتقاء دهد. علاوه بر آن، جهت تطابق با نیازهای خاص هر مشتری، ما متعهد می شویم کلیه مراحل برنامه ریزی، طراحی، اجرا، آموزش، پشتیبانی و تعمیر و نگهداری را بصورت کامل انجام دهیم.



CONSULTING AND MAINTENANCE

HAUMOUN TRAINING CENTER

مرکز آموزش هامون

شرکت پیشگامان فناوری اطلاعات هامون جهت دستیابی به اهداف خود مبنی بر ایجاد تحول در زمینه فناوری اطلاعات، اقدام به تأسیس مرکز آموزش هامون نموده است. این مرکز در نظر دارد با برگزاری دوره های آموزشی تخصصی و بروز، با محوریت ارتقاء دانش در این حوزه، گامی هر چند ناچیز در این راستا بردارد. امید است بتوانیم زمینه شکوفایی این حوزه از صنعت و فناوری را بیش از پیش فراهم نماییم. مرکز آموزش هامون در گام اول، موفق به دریافت مجوز آموزش کارکنان دولت از سازمان مدیریت و برنامه ریزی کشور شده است و با بهره گیری از اساتید مجرب حوزه فناوری اطلاعات کشور، اقدام به برگزاری دوره های آموزشی تخصصی در زمینه های ذیل نموده است:

مراکز داده

امنیت شبکه

مجازی سازی و ذخیره سازی

لینوکس

سیسکو

مدیریت فناوری اطلاعات

این مرکز آموزش آمادگی دارد تا دوره های سازمانی را در محل آموزشگاه و یا سازمان بنا به درخواست مشتری، با استفاده از اساتید منتخب هر حوزه، برگزار نماید.

HAUMOUN TRAINING CENTER



Linux

EMC²
where information lives

CISCO

VoIP

vmware

hp



CERTIFICATES & PERMISSIONS

گواهینامه ها و مجوز ها

مجاز آموزش کارکنان دولت	عضویت در شورای عالی انفورماتیک
گواهینامه ثبت اندیکای افتا	عضویت در نظام صنفی رایانه ای کشور
گواهینامه استاندارد کیفیت (ISO 9001)	پروانه کسب از اتحادیه کامپیوتر
گواهینامه استاندارد مدیریت کیفیت (ISO 10002)	عضویت در سامانه تدارکات الکترونیکی دولت
گواهینامه استاندارد رضایتمندی مشتری (ISO 10004)	تأییدیه وزارت نیرو
گواهی صلاحیت ایمنی کارکنان	تأییدیه وزارت نفت

چرا هامون؟

WHY HAUMOUN

۱. ما راهکارهای تخصصی متناسب با نیاز شما را ارائه می دهیم
۲. شما پشتیبانی بی قید و شرط ما را خواهید داشت
۳. ما در کوتاهترین زمان به نیازهای شما پاسخ خواهیم گفت
۴. شما به راحتی می توانید با ما ارتباط برقرار کنید
۵. ما امنیت و محرمانگی اطلاعات شما را حفظ خواهیم کرد
۶. شما مهارت و تجربه ما را همراه خواهید داشت
۷. ما به شما تجهیزات اوريجینال را ارائه خواهیم داد
۸. شما تعهد ما را خواهید داشت
۹. ما مستندسازی را دوست داریم.
۱۰. شما با کارشناسان همه فن حریف ما طرف هستید

We are always by your side...

