دسترسی ZERO TRUST SECURE برای بخش تولیدی[1] کارخانه‌های هوشمند

۵ مرحله برای ایمن‌سازی و خدمت‌دهی دستگاه‌های اینترنت اشیاء[2] صنعتی به منظور به حداکثررسانی زمان‌کار[3]

اثرات تجاری ناشی از مدت زمان از کارافتادگی[4] ناگهانی

اینترنت ۰. ۴ از اینترنت اشیاء صنعتی، رایانش ابری[5]، سیستم‌های فیزیکی سایبری و محاسبات شناختی برای افزایش بهره‌وری تولیدی استفاده می‌کند.

با افزایش بخش تولیدی کارخانه‌های هوشمند، سهام کارخانه افزایش می‌یابد.

۸۲ درصد از شرکت‌ها مدت زمان از کارافتادگی ناگهانی را در طی سه سال گذشته تجربه کرده‌اند.

[1] FACTORY FLOOR
[2] Industrial Internet of Things
[3] Uptime
[4] Downtime
[5] cloud computing

مدت زمان از کارافتادگی ناگهانی برای هر شرکت به اندازه ۲۶۰۰۰۰ دلار در هر ساعت هزینه بر است.

نمایانی[6] برای صنعت ۴.۰

دسترسی امن (Secure Access) با پروفایل‌بندی یا ترسیم دستگاه‌ها و استقرار نمایانی شبکه‌ای پیچیده آغاز می‌گردد. که این موضوع شامل سیستم‌های اینترنت اشیاء صنعتی در بخش تولیدی کارخانه است. ممکن است تولید سازمان از نقاط پایانی غیرامن یا ناشناخته مورد حمله قرار بگیرد.

تحقیق Deloitte-MAPI در سال ۲۰۱۶ دریافت که یک سوم تولیدکنندگان هیچگونه ارزیابی از ریسک‌های سایبری در مورد سیستم‌های کنترل صنعتی (ICS) که در بخش تولیدی کارخانه‌ها فعالیت داشته‌اند را انجام نداده‌اند.

[6] Visibility

تامین زمان فعالیت[7] کارخانه‌ها

ایمن‌سازی دستگاه‌های اینترنت اشیاء صنعتی ترسیم شده از بخش تولیدی کارخانه با فایروال‌های[8] محیطی نسل بعدی. ایجاد سیاست‌ها و قوانینی که اجازه ورود یا رد ترافیک به هر کدام از دستگاه‌ها می‌دهیم و فراهم‌سازی دسترسی از راه‌دور دستگاه‌های اینترنت اشیا صنعتی برای تشخیص و تعمیر سریع خرابی.

اتوماسیون برای IT و OT

آن دسته از سیستم‌های اینترنت اشیاء صنعتی بخش تولیدی کارخانه‌ها که ترسیم و کشف شده‌اند (SCADAها، PLCها و HMIها) به طور خودکار برای فایروال‌های نسل بعدی تامین شده‌اند. این فرآیند به طور چشمگیری باعث کاهش هزینه‌های عملیاتی IT / OT می شود و در عین حال سبب بهبود زمان کار تولید می‌شود.

[7] Uptime
[8] firewalls

«سازمان‌های CIO و فناوری اطلاعات با توجه به اینکه شرکت های بیشتری در راستای هماهنگی IT / OT کار می‌کنند، در راستای تقویت روابط و تغییر فرهنگ سازمانی در حال فعالیت هستند». «برای این مهم نیاز به ترکیبی مهارت‌های سنتی IT و OT و توسعه مالکیت فکری جدید داریم ...»

کریستین استینسترووپ[۹]، تحلیلگر برجسته و همکار گارتنر[۱۰]

احراز هویت[۱۱] برای تعمیر کارخانه

کاربران و دستگاه‌هایی که نیاز به دسترسی به دستگاه‌های اینترنت اشیا صنعتی بخش تولیدی کارخانه دارند بر اساس نقاط پایانی و نقش متخصصان پیش از اتصال به شبکه مورد احراز هویت قرار می‌گیرند.

[9] Kristian Steenstru
[10] Gartner
[11] Authentication

دسترسی امن توسط سیاست

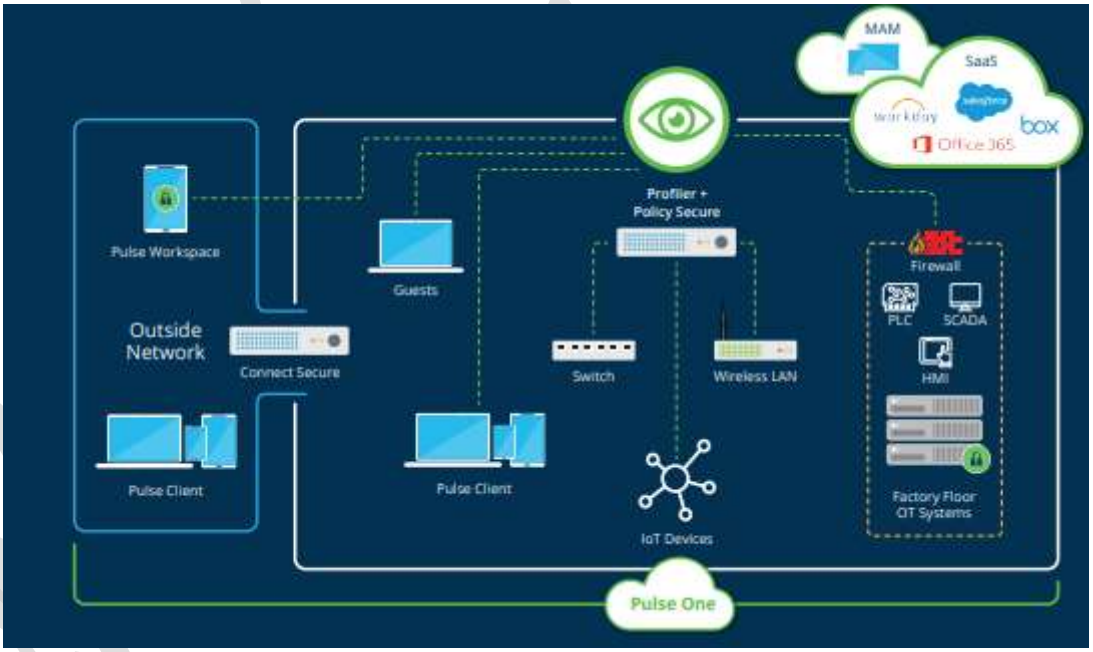
پیمان‌کاران پشتیبان، دسترسی راه‌دور ایمن به بخش‌های تولیدی دارای مشکل دسترسی پیدا می‌کنند مانند SCADA، PLC، و سایر حسگرهای اینترنت اشیاء صنعتی.

سیاست‌ها برای دسترسی محلی و از راه‌دور بر اساس نقش کاربر، دستگاه مورد استفاده، نوع دسترسی مورد نیاز و منابع مبتنی بر اینترنت اشیاء صنعتی هدف است.

آدرس: یوسف آباد- میدان جهاد- خیابان بیستون- خیابان فتحی شقاقی- پلاک ۹۳- طبقه دوم - واحد ۵
تلفن:۱-۸۸۳۵۳۴۰۰-۰۲۱
فکس: ۸۹۷۸۴۲۷۱

راه‌حل دسترسی امن (Secure Access)

Pulse Policy Secure و Pulse Connect Secure داده‌های محتوایی کاربران را به دسترسی شبکه و برنامه‌های کاربردی گره زده است و به خواسته‌های نظارتی و حسابرسی رسیدگی می‌کند. Pulse Secure Profiler دستگاه‌های سطح تولیدی را می‌یابد و تطبیق امنیتی پیش از اتصال را بر روی آنها انجام می‌دهد. هنگامی که با نسل بعدی فایروال‌های محبوب مستقر شوند، Pulse Policy Secure اقدام به تامین اطلاعات جلسه کاربر می‌کند و امنیت مبتنی بر محیط اضافه را ارائه می‌دهد. راه‌حل‌های Pulse Secure Access به شکل مرکزی از طریق Pulse One مدیریت می‌شوند.



برای اطلاعات بیشتر به آدرس www.pulsesecure.ir مراجعه کنید

رایان نیک تجهیز
شماره ثبت: ۴۹۸۸۱۱

آدرس: یوسف آباد- میدان جهاد- خیابان بیستون- خیابان فتحی شقاقی- پلاک ۹۳- طبقه دوم - واحد ۵
تلفن:۱-۸۸۳۵۳۴۰۰-۰۲۱
فکس: ۸۹۷۸۴۲۷۱