Zero Trust com Isolamento Dinâmico

UNISYS | Securing Your Tomorrow®

Ameaças estão por toda parte. Confiança é um passivo. E os ambientes de TI das empresas são muito complexos.

Toda empresa deve estar vigilante o tempo todo

As empresas enfrentam atualmente um cenário muito desafiador no campo da cibersegurança.

Ameaças estão por toda parte. Confiança é um passivo. E os ambientes de TI das empresas são muito complexos.

Malfeitores estão cada vez mais sofisticados em seus ataques. Muitos deles agora usam poderosas ferramentas de exploração que antes estavam disponíveis apenas para países. E, em alguns casos, os criminosos trabalham juntos para compartilhar ou trocar ferramentas, informações e dados roubados.

Esse desafio é ainda mais agravado por perímetros amorfos, más posturas de segurança, o número cada vez maior de endpoints conectados e o uso de equipamentos pessoais no trabalho.

Ameaças existem do lado de fora, mas é pouco provável que já não tenham invadido sua empresa. Isso significa que é importante estar vigilante o tempo todo.

Não se pode assumir que qualquer conexão ou comunicação entre elementos dentro da empresa possa ser confiável. É preciso considerar seu ambiente como se já estivesse comprometido.

E é necessário controlar, inspecionar e autorizar todas as comunicações, dispositivos e indivíduos.

Isso é o que a abordagem Zero Trust lhe permite fazer.

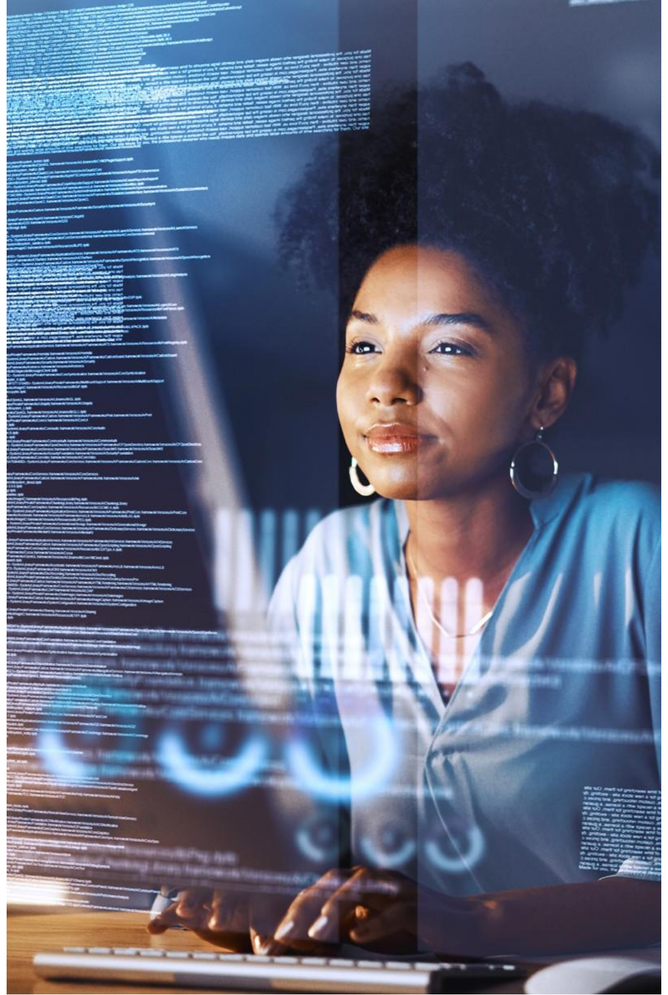
Zero Trust é a melhor maneira de enfrentar o atual cenário de ameaças

A abordagem Zero Trust permite às empresas proteger seus ativos críticos, onde quer que estejam. Isso é importante porque usamos atualmente um grande e crescente número de dispositivos. E empresas distribuídas, além do número cada vez maior de dispositivos conectados, dificultam a definição dos perímetros das redes.

Esse método assume confiança zero em todas as entidades - usuários, dispositivos, aplicações ou pacotes - independentemente com quem, com o que ou a que ponto elas se relacionem nas redes das empresas.

Zero Trust

- Define a superfície protegida
- Mapeia fluxos de transação
- Reduz a superfície de ataque da rede por meio da criação de zonas granulares
- Permite que as organizações criem políticas de segurança baseadas em processos de negócios
- Permite reação mais rápida diante de incidentes



A ameaça já está dentro da empresa

Filmes de terror costumam ter o mesmo enredo previsível. O personagem principal acha que o bandido está do lado de fora, mas, de fato, já está dentro de casa.

A cibersegurança nas empresas segue uma linha semelhante.

Tradicionalmente, as ameaças vêm de fora das empresas. Por esse motivo, organizações dedicam tempo e esforços na defesa de perímetros fixos. Muitas ainda fazem isso.

No entanto, muitas vezes os malfeitores já invadiram as redes das empresas, e o fato é que elas ainda nem sabem disso. É preciso estar atento e preparado para conter e erradicar essas ameaças.

As empresas ainda são lentas para reagir

Uma vez dentro das empresas, os invasores se movem rapidamente. É preciso ser mais rápido do que eles.

E quanto mais tempo se leva para identificar e combater eventos de cibersegurança, mais tempo os hackers têm para produzir estragos e expandir seu alcance. É uma corrida contra o tempo.

No entanto, as equipes de TI perdem tempo tentando determinar o que aconteceu, como aconteceu, o que fazer e como lidar com tais eventos.

A reação típica dos grupos de TI nesses casos é identificar violações e vulnerabilidades, analisá-las, gerar chamados de suporte e, em seguida, agir contra elas. Cada etapa desse processo é muito manual. Isso torna a identificação e a contenção de eventos de cibersegurança propensas a erros e difíceis de administrar. E tudo leva muito tempo.

Parte do problema vem do fato de as arquiteturas de segurança serem complexas e dos controles de segurança estarem isolados em silos. Isso eleva os custos, diminui a eficácia e torna tudo mais lento.

O Ponemon Institute diz que o tempo médio para detectar uma violação é de 197 dias. A reação normalmente leva outros 69 dias. Basta fazer as contas para reconhecer como o processo é lento.

As organizações precisam ser mais ágeis

As empresas também costumam demorar para reconhecer e solucionar vulnerabilidades - principalmente aquelas que tentam passar por cima da TI.

Hoje, não é incomum ver funcionários instalarem software em seus dispositivos, que depois se conectarão às redes das empresas. Esse ato, em si, pode ser uma violação da política corporativa. Além disso, os aplicativos podem introduzir vulnerabilidades que serão exploradas futuramente pelos hackers.

Os integrantes das equipes de TI podem reconhecer o software que está gerando as vulnerabilidades e alertar outras pessoas sobre a ameaça, porém esse processo é, tipicamente, ineficiente e demorado. Também pode acontecer de não resolver adequadamente as vulnerabilidades.

Por exemplo, um funcionário instalou um programa em seu laptop. A equipe de segurança tomou conhecimento disso por meio da varredura diária da rede. Após 48 horas, o funcionário recebeu um email alertando-o sobre o problema.

Em um ambiente de TI típico, essa seria considerada uma resposta rápida e sofisticada.

Entretanto, é fácil ver o que há de errado nesse cenário. Demorou horas para identificar a vulnerabilidade e dias para obter os detalhes do indivíduo que poderia agir. Além disso, a equipe de segurança deixou para o funcionário desinstalar o programa problemático.

Essa resposta pode parecer completamente aceitável em uma perspectiva histórica, mas o fato é que, se não agir rapidamente para fechar as brechas de cibersegurança - e não estiver preparada para reagir diante de um evento desse tipo, fora de controle -, a empresa pode perder clientes, receita, valor de mercado e a reputação conquistada arduamente. Será preciso gastar tempo e dinheiro para reduzir os danos, em vez de usar esses recursos para expandir os negócios. E a reputação será certamente afetada - colocando todo o trabalho em risco.

Se não agir rapidamente, a empresa poderá perder clientes, receita, valor de mercado e a reputação conquistada arduamente.

Ação rápida requer uma mudança fundamental

A maior parte das atuais tecnologias de cibersegurança se concentra principalmente na detecção e na prevenção. Elas enviam alertas às equipes de TI, sem propor um meio de ação. As soluções que permitem que especialistas em segurança tomem alguma medida, em geral, envolvem muito planejamento, esforços e decisões complexas antes que seja possível agir.

Hoje, a abordagem típica de cibersegurança se baseia no chamado pensamento System 2. As soluções desse tipo são complexas, ineficientes e lentas. Não são a maneira ideal de lidar com eventos catastróficos, como acessos não autorizados e falhas de cibersegurança, que são convites a ataques.

Tais situações exigem ação rápida, caso contrário, ao assumirem o controle de um dispositivo, os hackers podem expandir rapidamente seu alcance para outros ativos - elevando exponencialmente o escopo da destruição.

Isso exige o chamado pensamento System 1, que envolve respostas rápidas e automáticas para decisões cotidianas e mudanças de circunstância.

É exatamente assim que o Unisys Dynamic Isolation™ funciona.

Isolamento dinâmico age rapidamente sobre ameaças de cibersegurança

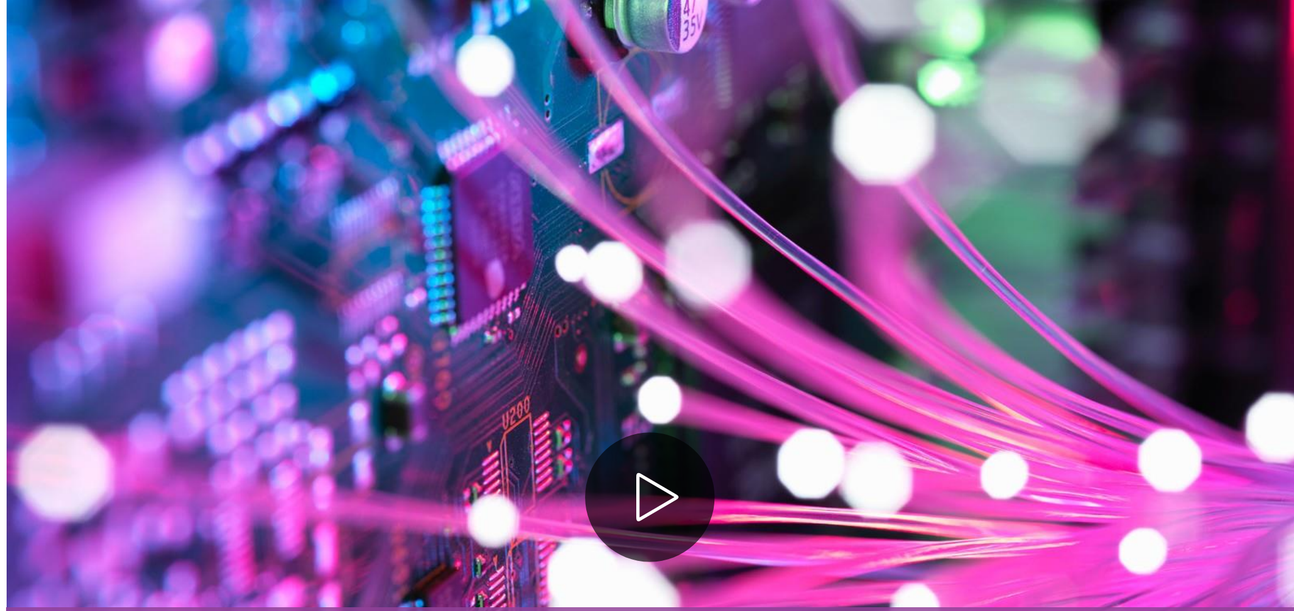
O Unisys Dynamic Isolation faz a mediação de todas as conexões entre endpoints por meio de pré-autenticação, pré-autorização e criptografia com a finalidade de reduzir ainda mais a superfície de ataque. Isso não afeta as operações normais dos endpoints, a menos que precisem ser acionados.

Ao isolar outros dispositivos e serviços de endpoints comprometidos, o Unisys Dynamic Isolation cria áreas seguras. Com o Unisys Dynamic Isolation, alguns processos podem continuar sendo executados dentro de perímetros seguros, sem preocupação com a propagação de riscos para outras partes da empresa. Essa é uma maneira de conter ameaças e manter os negócios funcionando que é muito mais eficaz do que deixar dispositivos fora de operação, colocando os sistemas completamente off-line.

O Unisys Dynamic Isolation pode trabalhar automaticamente, mas também oferece a opção de controle manual. Dessa forma, é possível receber e avaliar recomendações no console de gerenciamento de segurança de preferência para aprovar e iniciar o isolamento imediato.

A solução controla, reduz ou remove caminhos de acesso entre cargas de trabalho, diminuindo efetivamente a superfície de ataque. É uma resposta dinâmica baseada em perfis de usuário, cargas de trabalho, níveis de ameaça, contextos de negócios e postura de segurança. Também utiliza sistemas de clientes para detectar, prevenir e analisar tráfego de redes - permitindo que as empresas maximizem o retorno sobre investimentos já realizados em soluções de segurança.

Com o Unisys Dynamic Isolation, empresas como a sua podem reagir rápida e automaticamente com políticas de segurança personalizadas. Dessa forma, é possível reduzir o tempo médio de resposta a ameaças e também a superfície e a velocidade dos ataques. Evita-se assim perder tempo precioso reconfigurando redes e acessando fisicamente os dispositivos.



O Unisys Dynamic Isolation oferece uma maneira de conter ameaças muito mais eficaz do que deixar dispositivos fora de operação, colocando os sistemas completamente off-line.

Aqui está um exemplo de como a ação rápida funciona

Esse exemplo deve tornar mais claro o modo como o isolamento dinâmico entra em cena.

Digamos que um laptop na rede da empresa comece a executar uma verificação do ambiente. Esse comportamento, em geral, é o primeiro sinal de que um endpoint foi comprometido.

Apenas um pequeno grupo de usuários finais e endpoints na organização realiza verificações regularmente. E a primeira coisa que os invasores fazem ao entrar em um novo ambiente de TI é avaliar seus arredores. É por isso que as varreduras de rede feita por endpoints servem como sinal vermelho.

Nesse caso, a empresa já está um passo atrás do malfeitor. Então, ganhar tempo é essencial.

Assim que o comportamento anômalo - a varredura da rede - é detectado, o Unisys Dynamic Isolation é implantado em segundos, aplicando políticas de segurança ao endpoint para isolá-lo da rede.

O Dynamic Isolation também abre canais entre o laptop - ou qualquer endpoint que esteja apresentando comportamento anômalo - e a equipe de resposta a incidentes de segurança. Dessa forma, é possível investigar e aplicar correções. Isso pode envolver a remoção do malware, por exemplo.

Depois que o sistema automatizado ou a equipe de TI fizer as correções, o isolamento dinâmico restaura o acesso total do laptop à rede da empresa. Esse é um passo importante para fechar o ciclo e permitir a otimização de recursos.

Ao mesmo tempo, o isolamento dinâmico mantém os negócios funcionando

É importante notar que o isolamento dinâmico é diferente da quarentena.

O isolamento dinâmico permite que os endpoints continuem funcionando mesmo quando estão no modo de segurança. Ao contrário, as soluções de quarentena congelam completamente os endpoints.

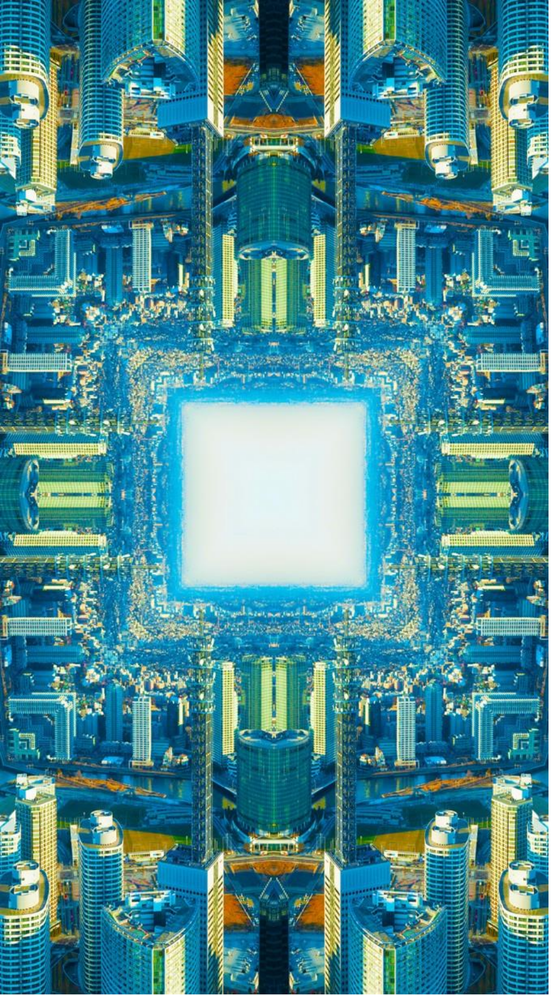
No exemplo citado, isso significa que o funcionário com o laptop poderia continuar trabalhando mesmo depois que o isolamento dinâmico entrasse em vigor. O funcionário não precisaria ficar ocioso enquanto o laptop não voltasse à normalidade, e a empresa não sofreria perda de produtividade.

O fato de o isolamento dinâmico não interromper os processos de negócios é ainda mais interessante quando o endpoint envolvido é um servidor.

Imagine que a empresa é um varejista on-line e que um servidor responsável pelo sistema de pagamentos inicie uma varredura da rede. Você poderia paralisar o servidor, mas perderia receita.

Uma abordagem melhor seria usar o isolamento dinâmico para separar apenas a porta ou o protocolo com comportamento anômalo. E continuar realizando as transações de venda normalmente.

Com o isolamento dinâmico, as empresas podem, pela primeira vez, atender às exigências de segurança, ao neutralizar ameaças, e às de negócios, ao manter as operações em dia.



Desempacotando os componentes da arquitetura de isolamento dinâmico

Em termos de arquitetura, o isolamento dinâmico emprega dois componentes principais: o controlador e o aplicador do isolamento dinâmico.

O controlador é o cérebro do isolamento dinâmico que analisa os eventos de cibersegurança. Com base nas regras definidas pela empresa, o controlador decide se é apropriado emitir uma solicitação ao aplicador para que o isolamento dinâmico seja efetivado.

O trabalho do aplicador é garantir que as políticas de segurança do isolamento dinâmico sejam aplicadas nos endpoints. O painel de controle do Unisys Stealth™ atua como um aplicador do isolamento dinâmico.

Ao olhar dentro do controlador de isolamento dinâmico, verá mais dois componentes em operação. Um é o analisador; o outro, o orquestrador. O analisador compara o evento de segurança não autorizado com as regras de correlação predefinidas da empresa e com outros eventos passados. O orquestrador permite que o aplicador faça a interface com outros componentes do sistema de isolamento dinâmico por meio de uma série de APIs.

Isso é fundamental porque o controlador desempenha um papel importante antes e depois do isolamento dinâmico. É responsabilidade do controlador dinâmico informar a equipe de incidentes de segurança, a ferramenta de incidentes de segurança e o sistema, de que as regras de isolamento dinâmico foram ativadas, por que foram ativadas e quais usuários foram envolvidos e impactados por esse evento específico. A equipe de resposta a incidentes de segurança fica responsável por enviar ao controlador de isolamento dinâmico um alerta de que o evento de segurança foi neutralizado e agora já é apropriado desfazer o isolamento.

É importante observar que todas as ações do controlador e do aplicador de isolamento dinâmico podem ser automatizadas. A intervenção humana é necessária apenas se as equipes de resposta a incidentes de segurança a exigirem.

Por que as empresas escolhem o Unisys Dynamic Isolation

O Unisys Dynamic Isolation é um serviço completo que trabalha com a plataforma Stealth. É o único no mercado capaz de reagir em casos de eventos de cibersegurança, aplicando políticas em menos de 30 segundos. Stealth garante à solução a capacidade de isolar, criptografar e ocultar endpoints dos olhos dos invasores, e também isolar ameaças em qualquer ponto da rede rapidamente.

O isolamento dinâmico analisa comportamentos, fornecendo uma maneira simples e eficaz de proteção contra ameaças atuais e futuras. Permite que as empresas maximizem o retorno sobre investimentos realizados nas atuais soluções de segurança.

Os diretores de segurança da informação podem contar com a flexibilidade e o controle do Unisys Dynamic Isolation, para criar regras personalizadas de isolamento com base nos requisitos de negócios. Essa solução da Unisys também garante às empresas recursos integrados que possibilitam reagir às ameaças de forma automática e rápida, em vez de inundar as equipes de segurança com alertas sem capacidade de reação.

O Unisys Dynamic Isolation usa a rede existente como transporte e cria redes de sobreposição isoladas criptograficamente da infraestrutura subjacente e uma das outras. Esse processo é dinâmico. Não é necessário alterar a infraestrutura existente. E pode funcionar de maneira totalmente automatizada.

Este é o único produto disponível atualmente no mercado com esses recursos exclusivos.

Resumindo...

Proteger as empresas é um imperativo para os negócios, mas enfrentar as ameaças de hoje é um desafio. A proliferação de dispositivos conectados, a crescente complexidade dos ambientes de TI e o cenário das ameaças em evolução tornam o desafio ainda maior. E isso significa que não é mais possível confiar em métodos antigos e que fazem manualmente as ações de monitoramento, identificação, análise e resposta aos eventos e ameaças de cibersegurança.

Contando com a Unisys, as empresas podem observar, entender, isolar e reagir diante de ameaças usando uma única plataforma integrada e automatizada. Como resultado, podem reduzir riscos, aumentar a produtividade e a lucratividade e gerar confiança entre clientes e demais stakeholders.