QUAIS SOLUÇÕES DE SEGURANÇA

vão proteger sua empresa das ameaças cibernéticas?

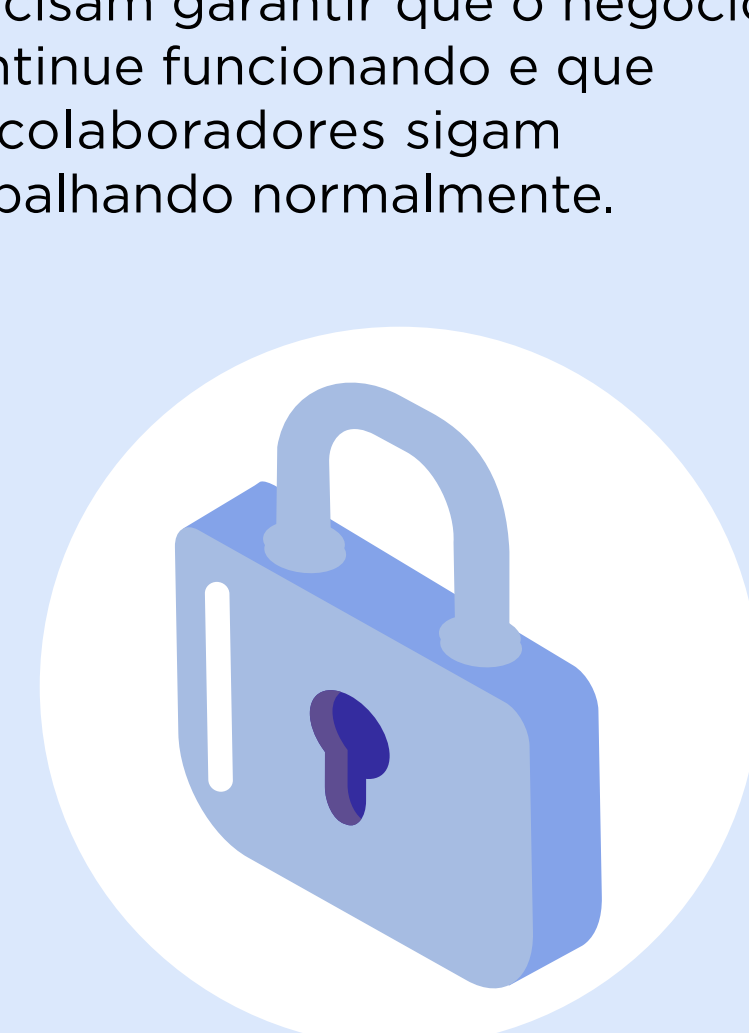
A pandemia do novo coronavírus trouxe o tema segurança para a lista de prioridades do mundo corporativo. De uma hora para a outra, as empresas tiveram de lidar com o desafio de ampliar a segurança do negócio para a casa de seus colaboradores.

Confira a seguir as soluções
que podem prevenir e proteger sua empresa de ataques cibernéticos durante esse período de transformação.

VPNAAS

O QUE FAZ
Uma rede virtual privada (VPN, na sigla em inglês) que fornece um túnel criptografado na internet, conectando o usuário à rede da empresa e permitindo que ele tenha acesso aos recursos como se estivesse dentro do escritório.

POR QUE É IMPORTANTE PARA O MOMENTO?
Muitas companhias precisaram adotar o *home office*, mas a maioria não tem uma infraestrutura adequada para isso. No entanto, precisam garantir que o negócio continue funcionando e que os colaboradores sigam trabalhando normalmente.



43%

Das empresas adotaram o *home office* devido ao coronavírus.

Fonte: *Valor Econômico*

ANTI-DDOS

O QUE FAZ
Se seu negócio começa a receber um volume incomum de tráfego, a ferramenta é capaz de desviá-lo para analisar se cada pacote de dados é legítimo ou não. Assim, é possível manter a disponibilidade do site, da plataforma e da VPN.

POR QUE É IMPORTANTE PARA O MOMENTO?
A pandemia impulsionou vendas em e-commerce, assim como o acesso aos sistemas de uma empresa por meio de uma VPN. Isso pode atrair *hackers* a lançar um ataque coordenado para sobrecarregar os servidores e paralisar as operações.

ANÁLISE DE VULNERABILIDADE E TESTE DE INVASÃO

O QUE FAZ
Essa solução procura possíveis vulnerabilidades em seus sistemas e coleta informações sobre os métodos de intrusão utilizados, sugerindo ações para mitigar os riscos. Assim, é possível descobrir vulnerabilidades e eliminar essas brechas de segurança antes que um incidente aconteça.

POR QUE É IMPORTANTE PARA O MOMENTO?
Com muitos sistemas e aplicações na nuvem, sua empresa vai precisar reforçar ainda mais as camadas de segurança, uma vez que esse ambiente será acessado, em sua maior parte, de forma remota.

24 bilhões

Foi o número de tentativas de ataques sofridas por empresas brasileiras em 2019.

Fonte: *Fortinet*

CYBER INTELLIGENCE

O QUE FAZ
A solução vai buscar na rede pública (internet, fóruns, redes sociais, *deep web*) toda e qualquer informação sobre sua empresa e funcionários-chave. Tem como objetivo identificar e antecipar possíveis ameaças para diminuir o impacto de ataques.

POR QUE É IMPORTANTE PARA O MOMENTO?
Muitas empresas foram forçadas a adaptar seus modelos de negócio devido ao coronavírus, o que pode trazer uma maior vulnerabilidade. Para os *hackers*, é uma oportunidade de criar sites maliciosos e perfis falsos de executivos nas redes sociais e de encontrar brechas para vazar dados sensíveis (da empresa, dos clientes e de seus funcionários).

MDM

O QUE FAZ
A solução monitora, gerencia e protege os dispositivos móveis usados por sua empresa. Assim, é possível definir quais aplicações o colaborador pode instalar ou executar.

POR QUE É IMPORTANTE PARA O MOMENTO?
O *home office* traz uma nova realidade para as empresas: as informações, que até então eram armazenadas em um ambiente interno e controlado, agora circulam fora das companhias. O MDM é importante para evitar ou reduzir os impactos de incidentes de segurança.

56%

Dos CISOs acham desafiador criar mecanismos de defesa contra o comportamento dos colaboradores.

Fonte: *Cisco*

CLOUD WEB GATEWAY

O QUE FAZ
É um servidor proxy na nuvem que, ao ser configurado, pode impedir que os colaboradores remotos acessem páginas específicas (como redes sociais, sites maliciosos etc.). Assim, sua empresa consegue manter a política de acesso à internet mesmo fora do ambiente corporativo.

POR QUE É IMPORTANTE PARA O MOMENTO?
Muitas empresas contam com um servidor proxy, mas com funcionamento restrito ao ambiente interno. Com o *home office* virando regra, é preciso aumentar os protocolos de segurança para evitar ataques e roubo de informações a partir de acesso a sites maliciosos e e-mails suspeitos.

ENDPOINT SECURITY

O QUE FAZ
É uma solução de segurança para todos os dispositivos da sua empresa, de notebooks a servidores. A ferramenta de gerenciamento de segurança em tempo real traz proteção antivírus, anti-malware, anti-adware, firewall de desktop, bloqueio de sites e filtragem de conteúdo.

POR QUE É IMPORTANTE PARA O MOMENTO?
Como os colaboradores passaram a trabalhar de casa, sua empresa pode perder o controle do acesso aos seus dados pelo mau uso do funcionário. Com a solução, é possível gerenciar todas as máquinas de forma remota por meio de um acesso web.

24 milhões

Total de variantes de malwares únicos identificados em 2019.

Fonte: *Kaspersky*

SEGURANÇA DE APLICAÇÃO

O QUE FAZ
A solução vai analisar todas as etapas do ciclo de vida de uma aplicação — do código-fonte ao lançamento — para identificar brechas e riscos. Assim, é possível incorporar controles de segurança e reduzir a exposição a riscos de ciberataques.

POR QUE É IMPORTANTE PARA O MOMENTO?
O cenário atual exige mais camadas de segurança para aplicações críticas de um negócio. Identificar as fraquezas em todo o seu ciclo de desenvolvimento é uma maneira de estar em conformidade com leis de proteção de dados e garantir uma utilização segura aos usuários.

UM TIME ALERTA 24 POR 7

Todas as soluções de segurança deste infográfico são apoiadas por um modelo de gestão conhecido como **Managed Security Service (MSS).**

Em vez de esperar que um ataque aconteça, o time de especialistas em segurança da **Embratel atua de forma preventiva e proativa** para evitar que a continuidade do seu negócio seja prejudicada, ainda mais em um momento em que todos estão mais vulneráveis.

Embratel
SUA EMPRESA NO PRÓXIMO NÍVEL