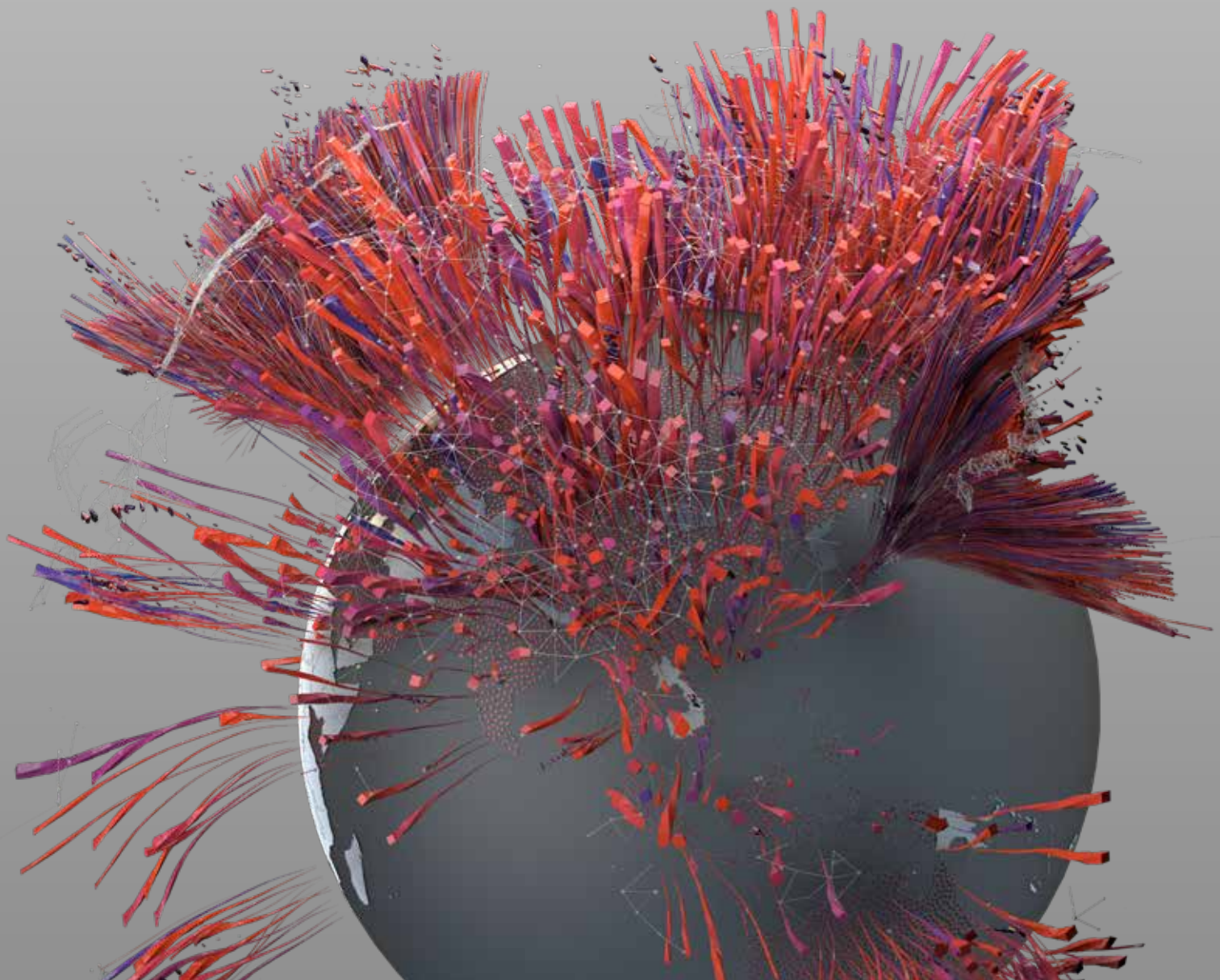
TREND MICRO™

Um estudo global

MAPEAMENTO DA SUPERFÍCIE DE ATAQUE DIGITAL:

Por que as organizações estão lutando para gerenciar o risco cibernético

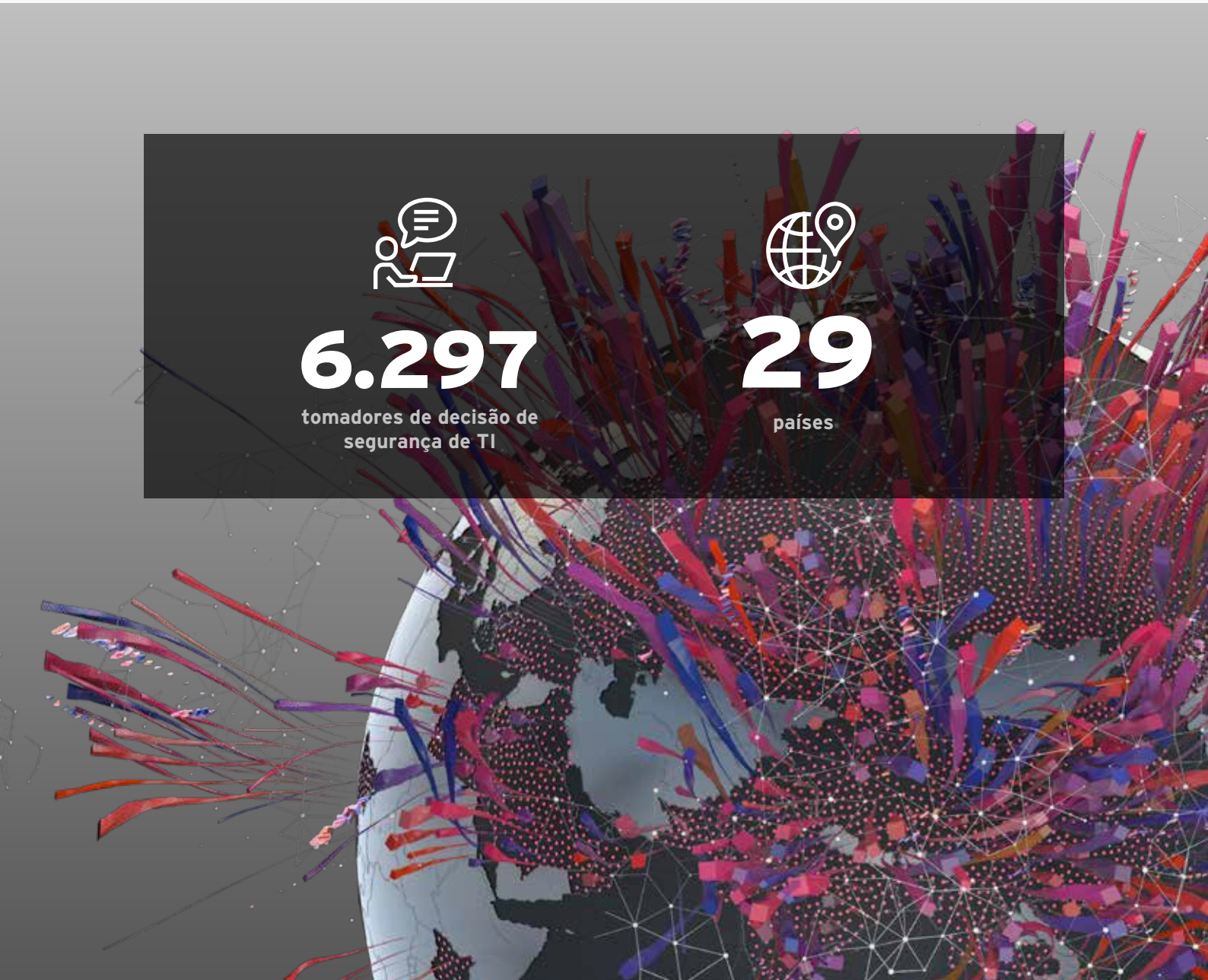


Introdução

Existe uma dinâmica simples, mas poderosa, que impulsiona o risco cibernético para a maioria das organizações hoje. Quanto mais eles investem em infraestrutura digital e ferramentas para impulsionar o crescimento sustentável, mais eles podem se expor a ataques. De acordo com especialistas, a transformação digital durante a pandemia levou muitas organizações a um "ponto de inflexão" tecnológico do qual nunca mais retornarão. Resumindo, o futuro dos negócios é digital – do trabalho híbrido às experiências do cliente baseadas em nuvem. Isso cria um desafio para os CISOs.

Esse desafio geralmente é articulado em termos da superfície de ataque digital, ou seja, a coleção de aplicações, sites, infraestrutura em nuvem, servidores locais, tecnologia operacional (OT) e outros elementos que são frequentemente expostos a agentes remotos de ameaças. Os riscos associados ao ataque podem ser mitigados se as organizações tiverem visibilidade de todos esses ativos, calcularem com precisão sua exposição ao risco e, em seguida, tomarem medidas para proteger a superfície de ataque. No entanto, muitos lutam para fazê-lo.

Para saber mais, a Trend Micro contratou a Sapio Research para realizar uma pesquisa em abril de 2022. Ela entrevistou 6.297 tomadores de decisão (3.138 tomadores de decisão de TI e 3.159 tomadores de decisão de negócios) em 29 países: Reino Unido, Bélgica, República Tcheca, Holanda, Suécia, Noruega, Finlândia, Dinamarca, França, Alemanha, Suíça, Áustria, EUA, Itália, Canadá, Taiwan, Japão, Cingapura, Austrália, Índia, Polônia, Hong Kong, Malásia, Filipinas, Indonésia, México, Colômbia, Chile.



Como os agentes mal-intencionados visam a superfície de ataque

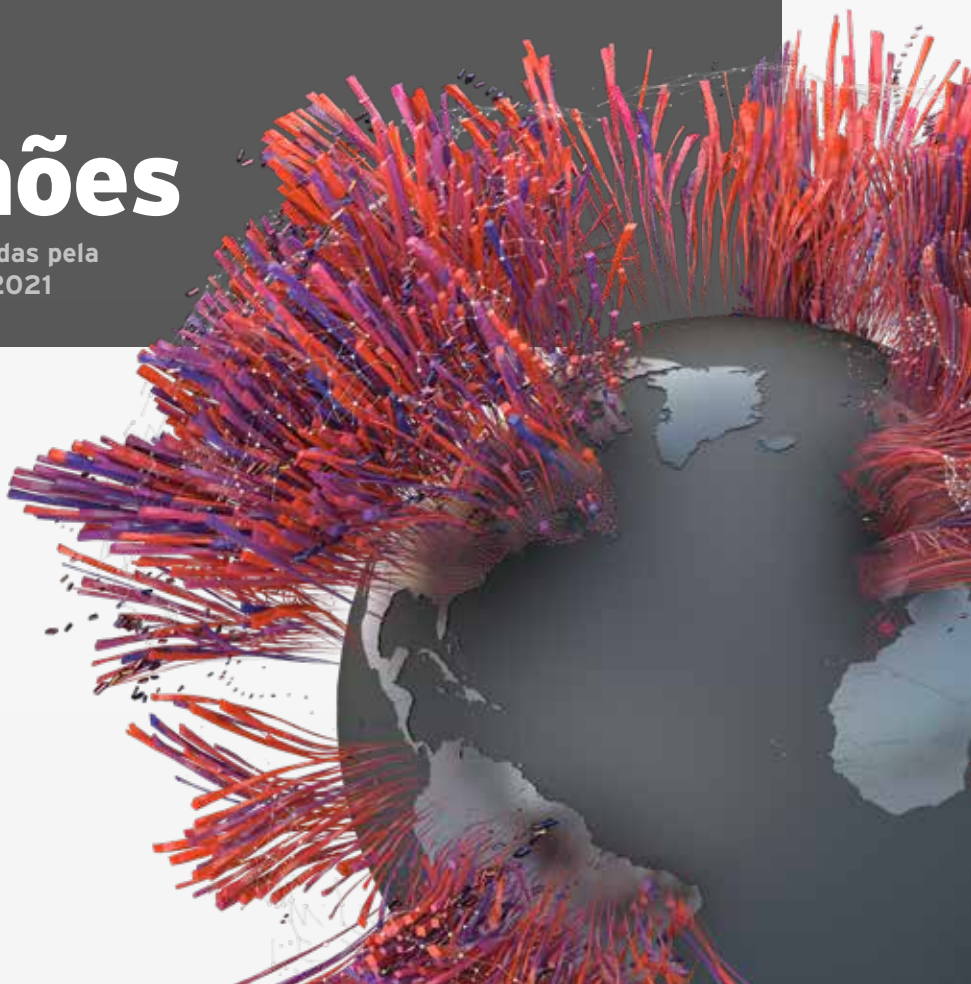
Como destaca o último relatório anual de cibersegurança da Trend Micro para 2021, os agentes de ameaças implantam uma variedade de táticas, técnicas e procedimentos (TTPs) para atingir vários elementos da superfície de ataque corporativo das organizações vítimas. Estes incluíram:

- **Caixas de entrada de e-mail**
- **IoT endpoints**
- **Aplicações Móveis**
- **Remote desktop protocol (RDP) endpoints**
- **Virtual private networks (VPNs)**
- **PCs**
- **Sites**
- **Servidores**
- **Certificados**
- **Serviços de nuvem pública**
- **Infraestrutura e serviços da cadeia de suprimentos**

Eles fizeram isso por meio de phishing, explorações de vulnerabilidades, comprometimento de serviços mal configurados e outras técnicas – para implantar ransomware, cavalo de troia, ladrões de informações, botnets e muito mais. E eles foram surpreendentemente persistentes no ano passado. Somente a Trend Micro bloqueou mais de 94 bilhões dessas ameaças para os clientes em 2021. Muitas outras organizações, sem dúvida, não tiveram tanta sorte.

94 bilhões

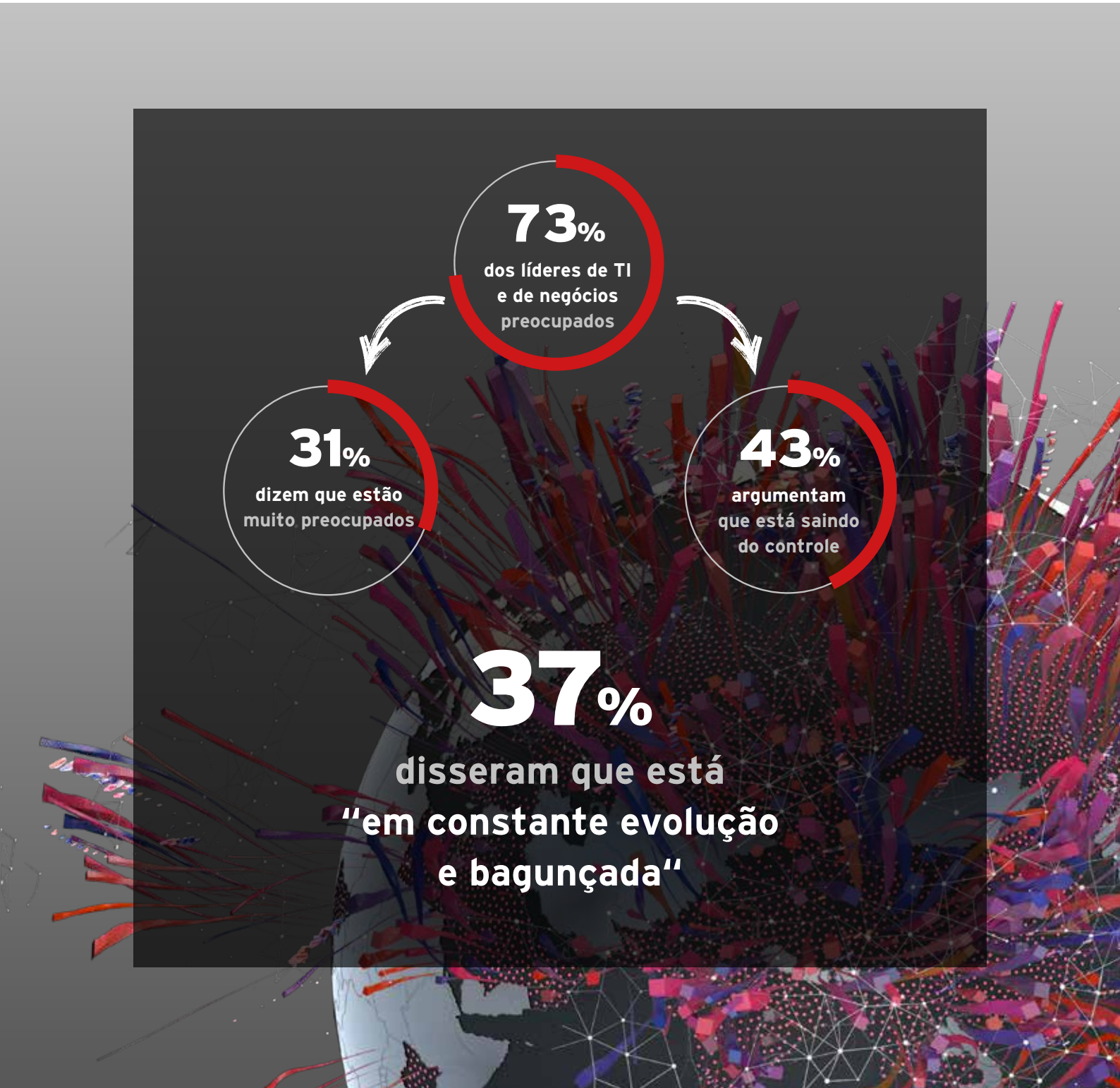
de ameaças bloqueadas pela Trend Micro em 2021



As organizações estão preocupadas

Com estatísticas como essas, talvez não seja surpreendente que quase três quartos (73%) dos líderes de TI e de negócios que pesquisamos estejam preocupados com o tamanho de sua superfície de ataque digital. Um terço (31%) diz estar "muito preocupado". Ainda há mais. Cerca de 43% vão ainda mais longe, argumentando que a superfície de ataque está ficando fora de controle.

Há uma sensação de que grandes investimentos em modernização de TI nos últimos anos criaram um impulso cada vez mais difícil de gerenciar. Quando solicitados a descrever sua superfície de ataque, a resposta mais popular para os entrevistados (37%) foi que ela está "em constante evolução e bagunçada". Isso sugere o desafio que as equipes de segurança enfrentam: uma superfície de ataque que está se expandindo fora de controle. Na verdade, apenas metade (51%) dos entrevistados afirma ter definido completamente sua superfície de ataque. Ganhar visibilidade desse tipo é certamente o primeiro passo para mitigar efetivamente o risco.



O desafio da visibilidade

Infelizmente, quase dois terços (62%) dos líderes de TI e de negócios com quem conversamos admitem que têm pontos cegos na tentativa de proteger sua superfície de ataque. Em média, as organizações que respondem têm apenas uma visibilidade estimada de 62% em sua superfície total de ataque. No entanto, mesmo isso é apenas um palpite. A probabilidade é que seja ainda menor.

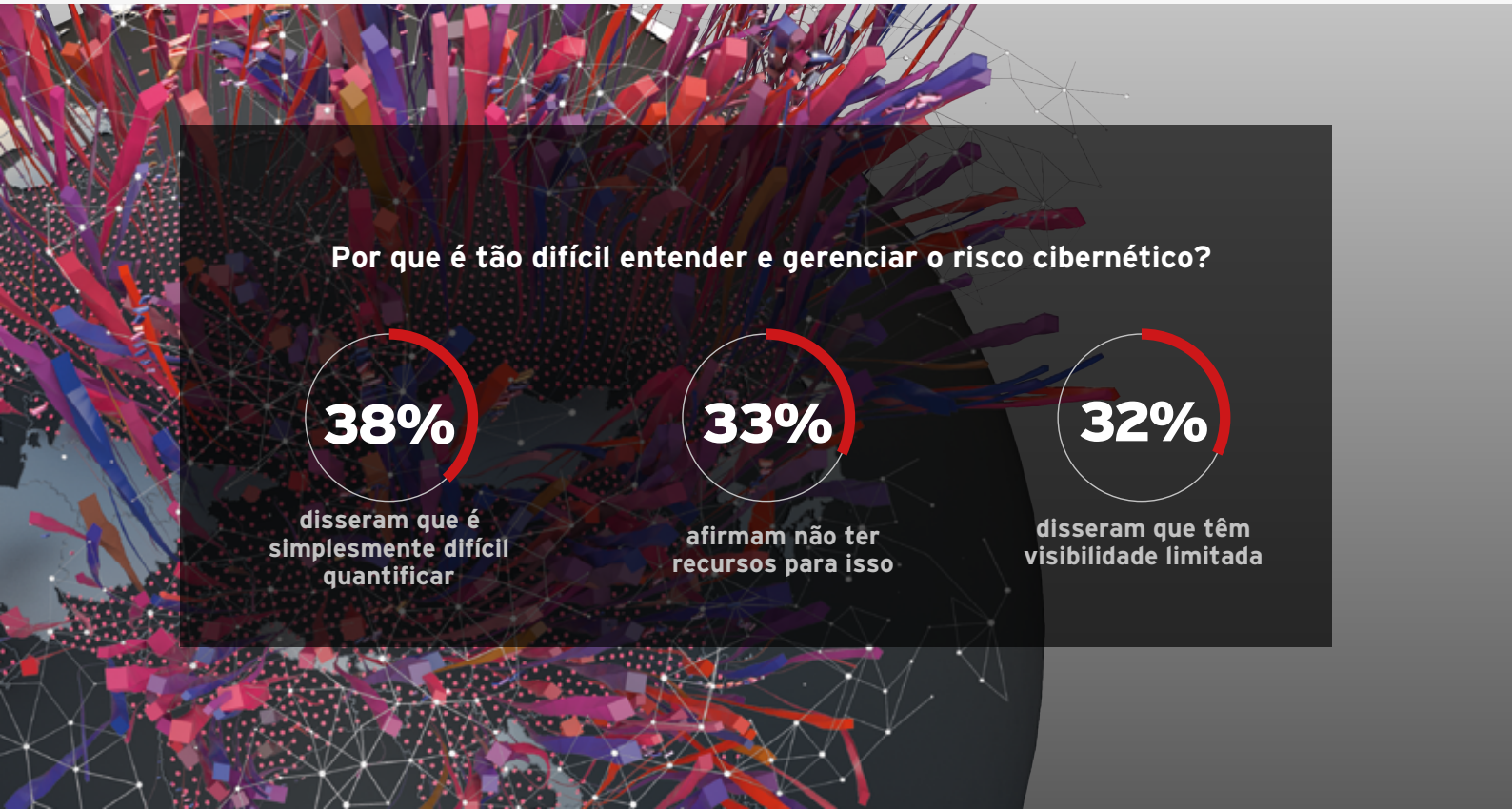
Os ativos de nuvem são compreensivelmente considerados a área onde as organizações têm menos insights (37%), seguidos por redes (34%) e ativos de usuários finais (29%). Na nuvem, a mudança é a única constante. VMs, contêineres e outros ativos aparecem e desaparecem com uma frequência impressionante. Os usuários de negócios podem ignorar completamente a TI ao configurar novas iniciativas digitais. E a inovação contínua dos fornecedores de plataformas significa que todo o edifício é construído sobre areias em constante mudança.

As organizações que operam além-fronteiras também são afetadas. Dois terços (65%) dos entrevistados afirmaram que o fato de serem globais torna o gerenciamento da superfície de ataque mais desafiador. No entanto, um quarto (24%) ainda está mapeando seus ambientes manualmente e 29% está fazendo isso regionalmente, o que corre o risco de criar silos de informações.

Vamos analisar alguns dos principais motivos pelos quais a visibilidade da superfície de ataque é tão desafiadora hoje:

- As organizações não têm as ferramentas certas para obter visibilidade de todos os seus ativos
- CISOs e suas equipes têm muitas ferramentas, criando silos de informações
- Cadeias de suprimentos opacas
- Um ambiente em constante fluxo: especialmente na nuvem, onde os ativos são dinâmicos e intermitentes
- O tamanho, a complexidade e a natureza distribuída dos ambientes de TI modernos
- Inovação tecnológica constante, especialmente de fornecedores de nuvem
- Unidades de negócios investindo em novos produtos e serviços sem avisar a TI (shadow IT)
- Uma explosão de endpoints de trabalho remoto e shadow IT durante a pandemia

Muitos desses desafios foram confirmados por respostas à nossa pergunta: "Por que é tão difícil entender e gerenciar o risco cibernético?" O maior número de entrevistados disse que é simplesmente difícil quantificar (38%). Um terço (33%) afirma não ter recursos para isso e um número semelhante (32%) que tem visibilidade limitada. Reclamações de muitas ferramentas (30%) e alertas (27%) ilustram a necessidade de uma abordagem unificada baseada em plataforma. Um quinto (21%) falou de silos de dados.



O problema de gerenciar riscos

O objetivo de obter visibilidade e controle da superfície de ataque digital é, em última análise, entender e gerenciar melhor o risco cibernético. No entanto, mais da metade (54%) das organizações com as quais conversamos admitem que seu método de avaliação da exposição ao risco não é sofisticado o suficiente. Menos da metade (45%) afirma ter um processo completamente bem definido para isso.

Parte disso provavelmente se deve à falta de investimento nas ferramentas certas. No entanto, estratégia e processo também são importantes. Mais de um terço (35%) dos entrevistados admitem apenas revisar ou atualizar a exposição ao risco a cada mês ou menos. E menos de um quarto (23%) o faz diariamente. Dado o ritmo da inovação tecnológica, a taxa de investimento digital e a velocidade com que o cenário de ameaças está evoluindo, avaliações regulares são essenciais para obter visibilidade total e controle aprimorado sobre a superfície de ataque.

Talvez não seja surpreendente que, quando perguntados sobre qual é o maior desafio no gerenciamento da superfície de ataque digital, os entrevistados tenham mais probabilidade de responder: manter-se atualizado com as mudanças constantes (39%).

Construindo uma organização mais consciente dos riscos

Então, como os CISOs podem construir uma organização mais consciente dos riscos?

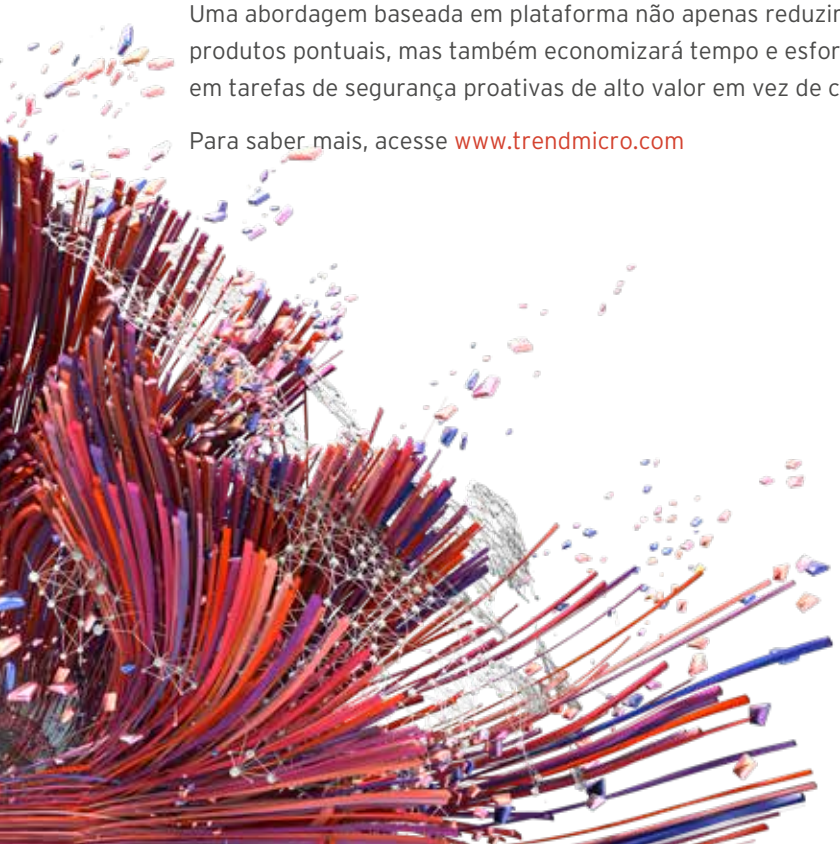
Tudo se resume a três passos importantes:

1) Obtenha visibilidade de todos os ativos e vetores de ataque
2) Use esses dados para calcular continuamente a exposição ao risco
3) Invista nos controles certos para mitigar esse risco

O benefício de uma abordagem baseada em plataforma aqui deve ser claro. Se a plataforma for extensa o suficiente para cobrir toda a superfície de ataque – de e-mail e endpoints a redes e nuvem – ela ajudará a eliminar silos de dados e fornecerá visibilidade abrangente dos ativos. Essa mesma plataforma pode ser configurada para fornecer proteção contínua desses ativos por meio de ferramentas e técnicas de prevenção, detecção e resposta, para minimizar as lacunas de segurança e melhorar a tomada de decisões.

Uma abordagem baseada em plataforma não apenas reduzirá os gastos com renovação e gerenciamento de produtos pontuais, mas também economizará tempo e esforço das equipes de TI, liberando-as para trabalhar em tarefas de segurança proativas de alto valor em vez de combate a incêndios com cadeira giratória.

Para saber mais, acesse www.trendmicro.com



TREND MICRO™

A mudança global dos clientes da Trend Micro de segurança local para segurança baseada em SaaS.
Criado com dados reais pelo artista Brendan Dawes.