Reduzindo a Complexidade da Cibersegurança

Uma Abordagem Crítica para uma Segurança Cibernética com Foco em Prevenção

ESET®

Digital Security
Progress. Protected.

Sumário

Introdução

O software "devorou o mundo" há muitos anos — e continuará digerindo-o, impulsionado por inovações como a ascensão da inteligência artificial. Infelizmente, os avanços em software continuam introduzindo riscos críticos para os negócios, que as organizações já têm dificuldade em gerenciar. As equipes de segurança enfrentam um trabalho cada vez mais difícil do que o necessário. O culpado? **A complexidade da cibersegurança**.

Mesmo empresas menores, com estruturas de TI teoricamente mais simples, não escapam do dilema da complexidade. Por exemplo, a escassez generalizada de profissionais qualificados torna o gerenciamento de ferramentas complexas ainda mais desafiador. Além disso, o trabalho remoto — agora comum à maioria dos negócios — amplia a superfície de ataque e a complexidade da TI de formas imprevisíveis, por meio de dispositivos pessoais e redes domésticas inseguras.

É fundamental que as equipes de TI e segurança encontrem formas mais eficazes e integradas de lidar com essa complexidade e enfrentar as ameaças multifacetadas e em constante evolução que surgem diariamente.

Para abordar essa questão, a ESET elaborou este white paper, oferecendo insights essenciais sobre os principais desafios enfrentados pelas organizações na luta contra a complexidade da cibersegurança.

E, mais importante ainda, apresenta estratégias práticas e orientações para o sucesso. Entre outras coisas, você vai descobrir como os seguintes pontos podem ajudar a reduzir a complexidade cibernética:

80%

das empresas

reconhecem que o uso de múltiplas soluções pontuais prejudica a eficiência de suas equipes na detecção, resposta e recuperação de incidentes.

Fonte: *2024 CISCO Cybersecurity Readiness Index, 2024*.

- **IA e automação,** que ajudam a aprimorar as habilidades das equipes de segurança e a reduzir o esforço manual, ao mesmo tempo em que aumentam a produtividade.
- **Proteção holística e em múltiplas camadas,** fornecida a partir de uma única plataforma, para combater ameaças de forma proativa e ampliar a visibilidade sobre o ambiente
- **Terceirização de parte das operações de segurança (SecOps)** para um provedor especializado em **Detecção e Resposta Gerenciada (MDR)**

- **Abordagem de confiança zero (zero trust),** que pode mitigar riscos relacionados ao trabalho remoto e ao acesso a dados

Enfrentar a complexidade cibernética é uma das primeiras etapas para implementar uma abordagem de cibersegurança com foco em prevenção, criada para minimizar os riscos ao lidar com processos, soluções ou até serviços de segurança mal desenhados.

O objetivo é criar uma operação de segurança eficaz, fortalecendo a resiliência cibernética sem compromissos.

Entendendo a Complexidade da Cibersegurança

O que exatamente significa "complexidade" no contexto da cibersegurança? Existem diversas facetas para isso. Pode significar:

1 **Quantidade e tipo de ferramentas de segurança** que as equipes de TI precisam gerenciar, além dos processos que devem seguir para manter a organização segura.

2 Da mesma forma, pode se referir aos s**istemas de TI distribuídos e heterogêneos** que as equipes devem defender — desde **telefones móveis, passando por computadores até redes inteiras na nuvem**, amplificadas pelo trabalho remoto.

3 E, claro, isso pode significar o c**enário de ameaças em rápida evolução**, com o qual muitas equipes internas de segurança têm dificuldade para acompanhar..

Na verdade, um dos maiores desafios enfrentados por esses profissionais de segurança de TI, frequentemente sobrecarregados e com poucos recursos, é a velocidade com que surgem novas táticas, técnicas e procedimentos (TTPs) dos agentes de ameaça.

Além disso, o trabalho deles se torna muito mais difícil devido à necessidade de lidar com dados isolados, ferramentas difíceis de usar e orçamentos limitados, enquanto enfrentam uma superfície de ataque extensa e em expansão.

Como é a Cibersegurança

No geral, a complexidade é uma grande inimiga da cibersegurança. Por isso, entender como ela pode impactar um negócio típico é o primeiro passo para superá-la. Ela pode ser percebida principalmente em:

MÚLTIPLAS FERRAMENTAS E SOLUÇÕES

A cibersegurança muitas vezes é tratada tardiamente pelos líderes empresariais. Isso é lamentável, pois os gastos reativos após um incidente ou violação geralmente são fragmentados e levam ao investimento em soluções pontuais, que atendem apenas a um único caso.

Assim, em vez de **resolver a causa raiz de uma violação**, essas soluções podem focar apenas em um aspecto da estrutura de segurança, tornando as tarefas diárias da equipe de TI mais difíceis. Isso obriga as equipes de segurança a trabalhar em ambientes "gira-cadeira", tendo que alternar constantemente entre diferentes telas e portais de gerenciamento.

Empresas de médio porte com 1-5 licenças possuem, em média

51

soluções

em uso em toda organização.

Fonte: *Pentera: The State of Pentesting Survey 2024*.

Empresas de grande porte com 10 licenças possuem, em média

58

soluções

em uso em toda organização

Fonte: *Pentera: Tje State of Pentesting Survey 2024*.

Seja como for, as ameaças invariavelmente se escondem nas lacunas de interoperabilidade e visibilidade que essas ferramentas criam. Além disso, grande parte do tempo da equipe de TI é gasto aprendendo novas ferramentas, em vez de resolver problemas importantes. Segundo relatos, a empresa média opera com dezenas de soluções de segurança, e a maioria planeja aumentar o número de fornecedores em sua pilha nos próximos anos.

COMPLEXIDADE DAS FERRAMENTAS DE SEGURANÇA

O problema não é apenas o número excessivo de ferramentas de segurança. Frequentemente, as ferramentas que as empresas já possuem são muito complexas, com interfaces pouco intuitivas ou fluxos de trabalho ineficazes. Isso pode **prejudicar a produtividade** de equipes que já estão com pessoal reduzido e fazer com que os profissionais de TI **não consigam aproveitar todos os recursos** disponíveis.

Em outros casos, soluções de nível corporativo, como o SIEM, são adquiridas mas acabam sendo pouco utilizadas, pois a empresa não consegue dedicar os recursos necessários para configurá-las e gerenciá-las de forma contínua.

TRABALHO REMOTO E TSPD (TRAGA SEU PRÓPRIO DISPOSITIVO)

A complexidade vai além das ferramentas de segurança de uma organização. Hoje, mais empresas do que nunca se beneficiam da flexibilidade que o trabalho remoto oferece aos seus colaboradores. Nos Estados Unidos, cerca de um terço dos profissionais em cargos gerenciais, profissionais e outros relacionados trabalham de casa.

Isso geralmente resulta em funcionários mais satisfeitos e produtivos, além de possíveis reduções nos custos com escritórios e instalações. No entanto, também expõe essas organizações a riscos cibernéticos adicionais.

O trabalho remoto significa que os funcionários podem estar acessando sistemas a partir de dispositivos e laptops desprotegidos ou desatualizados, possivelmente por meio de redes domésticas ou públicas inseguras. Isso pode **comprometer senhas corporativas e abrir um caminho desprotegido** para que agentes maliciosos acessem redes e dados da empresa.

73%

dos líderes de TI em cargos de VP e C-suite

acreditam que trabalhadores remotos representam um risco maior do que os funcionários presenciais.

Fonte: *OpenVPN: OpenVPN Quick Poll Remote Workforce*

Proteger esse ambiente de computação distribuída pode gerar uma sobrecarga adicional de gerenciamento e dor de cabeça, especialmente ao considerar a quantidade de dispositivos internos e externos que uma empresa precisa monitorar simultaneamente.

UM CENÁRIO DE AMEAÇAS EM RÁPIDA EVOLUÇÃO

O cenário de ameaças está em constante transformação. À medida que os defensores das redes e os fornecedores de segurança continuam desenvolvendo proteções, seus adversários encontram novas maneiras de ultrapassá-las, em uma corrida armamentista sem fim. Os agentes maliciosos têm a vantagem do fator surpresa e precisam ter sorte apenas uma vez para penetrar em uma rede corporativa ou em um repositório de dados.

93%

das companhia

sofrem uma violação de segurança cibernética devido as fragilidades em sua cadeia de suprimentos/ fornecedores terceiros em 2023.

Fonte: *WSJ Pro Cybersecurity Research: Third-Party Cyber Risk Management Primer*.

768

CVEs foram publicamente reportadas

como exploradas em um ambiente real em 2024, marcando um aumento de 20% em relação a 2023.

Fonte: *VulnCheck: 2024 Trends in Vulnerability Exploitation*.

Eles contam com várias formas de fazer isso, graças aos investimentos contínuos em infraestrutura de nuvem, software, APIs e outras tecnologias digitais, que abrem novas portas para ataques.

O número de vulnerabilidades e exposições comuns **recém-descobertas** (CVEs) atingiu níveis recordes nos últimos anos, enquanto novas táticas, técnicas e procedimentos (TTPs) alimentados por inteligência artificial devem aumentar o volume e o impacto de ataques como o ransomware.

Cadeias de suprimentos complexas introduzem oportunidades adicionais para que os adversários alcancem seus alvos, e senhas roubadas continuam sendo o calcanhar de Aquiles. O uso de credenciais roubadas esteve presente em quase um terço (31%) das violações na última década, todos esses fatores podem ser um desafio até mesmo para empresas com bons recursos de segurança.

FALTA DE HABILIDADES E LACUNAS EM CIBERSEGURANÇA

Outro problema enfrentado por empresas de pequeno e médio porte é que raramente contam com pessoal suficiente em suas equipes de TI dedicados exclusivamente à cibersegurança. Atualmente, o déficit de profissionais em cibersegurança é de quase cinco milhões de profissionais, um aumento de 19% em relação ao ano anterior. Organizações menores, que não conseguem competir com os salários oferecidos por grandes empresas, muitas vezes acabam perdendo talentos.

A falta desses profissionais qualificados é agravada por restrições orçamentárias — que tendem a impactar mais fortemente as PMEs do que as grandes corporações, além de ferramentas e processos de segurança que exigem muita mão de obra e comprometem a produtividade. Equipes sobrecarregadas também estão mais propensas a cometer erros. A falta de habilidades representam outro desafio.

Apenas um quarto (26%) dos recrutadores entrevistados pela ISACA acreditam que ao menos metade dos candidatos está bem qualificada, computação em nuvem (47%) e controles de segurança (35%) estão entre as três principais áreas com maior carência de habilidades.

À medida que a tecnologia continua a evoluir e se tornar mais complexa, o perigo é que as habilidades em segurança de TI não acompanhem esse ritmo, dando ainda mais vantagem aos agentes de ameaça.

SOBRECARGA DE DADOS

Do ponto de vista das operações de segurança (SecOps), o **grande número de soluções pontuais** utilizadas por muitas organizações **pode gerar dados e alertas** em uma velocidade avassaladora, sobrecarregando os analistas a ponto de dificultar a priorização com precisão.

Isso pode levar algumas equipes a perderem tempo com falsos positivos, enquanto falsos negativos passam despercebidos e causam danos. Também pode provocar estresse e esgotamento, aumentando ainda mais a pressão sobre os colegas que permanecem na equipe.

47%

dos trabalhadores digitais

tiveram dificuldades em encontrar as informações necessárias para desempenhar suas funções de forma eficaz, devido ao número crescente de aplicações utilizadas no ambiente de trabalho em 2023.

Fonte: *Gartner Press Release, Gartner Survey Reveals 47% of Digital Workers Struggle to Find the Information Needed to Effectively Perform Their Jobs, 2023*.

46%

dos respondentes

com responsabilidades em cibersegurança descreveram o quadro atual da equipe de segurança cibernética de sua organização como "parcialmente desfalcado" em 2023.

Fonte: *ISACA's Global Cybersecurity State Report 2023*.

Priorizando a Prevenção para Vencer a Complexidade

Enfrentar esse tipo de complexidade não é fácil. Mas, com uma abordagem focada na prevenção como princípio orientador, está ao alcance de qualquer empresa. Por que a prevenção faz mais sentido?

Porque, ao focar em construir resiliência nos sistemas por meio de uma melhor ciber-higiene, bloqueando ameaças diretamente e detectando e contendo rapidamente aquelas que conseguem passar, as organizações têm mais chances de mitigar riscos antes que eles se agravem.

Trata-se de fortalecer a primeira linha de defesa, porque a prevenção é sempre melhor (e mais barata) do que a correção.

No entanto, a prevenção exige uma segurança robusta, mas fácil de operar — altamente automatizada, pronta para uso imediato, livre de manutenção e projetada com foco em pequenas e médias empresas — com um preço compatível. Em resumo, deve-se priorizar a simplicidade em vez da complexidade. Com isso em mente, veja como enfrentar os desafios de complexidade citados acima.

CONSOLIDAÇÃO DE FERRAMENTAS Uma resposta simples ao excesso de ferramentas é consolidar a segurança com foco em prevenção em uma única plataforma de um fornecedor confiável. É exatamente isso que a plataforma **ESET PROTECT** oferece, por exemplo. A partir de um único painel de controle, ela protege todo o ambiente de TI — desde endpoints e servidores até dispositivos móveis, aplicações em nuvem e e-mails.

A proposta é entregar prevenção, detecção e busca proativa por ameaças em um único local — fechando brechas de segurança e reduzindo a carga de trabalho das equipes de TI, que já operam sob pressão.

Além disso, há integrações perfeitas com produtos de terceiros que aumentam ainda mais o valor da plataforma, reduzindo a necessidade de alternar entre múltiplas interfaces (“ambientes tipo cadeira giratória”).

As tecnologias multicamadas, *como HIPS, Advanced Memory Scanner, UEFI Scanner, Deep Behavioral Inspection, Botnet Protection* e *DNA Detections*, atuam em conjunto como o ESET LiveSense. Elas desempenham uma ampla gama de funções a partir de uma única plataforma: bloqueio de malwares, identificação de comportamentos suspeitos e proteção contra botnets e ameaças ao firmware UEFI, entre outras.

INTERFACE DO USUÁRIO SIMPLIFICADA Ferramentas de cibersegurança nem sempre são complexas de usar. **A ESET PROTECT** prioriza um design amigável e uma aparência consistente em toda a sua ampla gama de funcionalidades.

A implantação é extremamente simples graças ao seu design baseado em nuvem. O console de administração pode ser acessado de qualquer dispositivo, em qualquer lugar, e os painéis e relatórios podem ser personalizados conforme as necessidades de cada organização.

Um alto grau de automação integrada torna a experiência do usuário ainda mais fluida, enquanto recursos baseados em IA, como o **Incident Creator** e o **ESET AI Advisor**, otimizam o trabalho dos analistas de operações de segurança (SecOps).

ABORDAGEM ZERO TRUST Quando se trata de ambientes de TI distribuídos, baseados em nuvem e dispositivos móveis, a abordagem **Zero Trust** é a melhor forma de mitigar riscos. Essa ideia se baseia em um princípio simples: **não confie em ninguém por padrão**.

Essa abordagem envolve a verificação frequente de todos os usuários e dispositivos, a implementação de políticas de acesso com privilégios mínimos, segmentação de rede, monitoramento contínuo, criptografia robusta e muito mais.

O modelo Zero Trust trabalha para manter controles de acesso rigorosos, sendo projetado para reduzir as chances de agentes mal-intencionados acessarem redes corporativas e recursos em nuvem — e, caso consigam, limitar significativamente sua capacidade de causar danos.

A **ESET PROTECT** oferece diversos recursos para apoiar a abordagem Zero Trust, desde *Gerenciamento Integrado de Segurança* e *Proteção de Endpoints* até *Criptografia de Disco Completo, Cloud Sandbox, Proteção de Aplicações em Nuvem* e muito mais.

DETECÇÃO E RESPOSTA GERENCIADAS (MDR) A escassez de profissionais qualificados em cibersegurança é um desafio difícil de superar sem ações amplas e de longo prazo por parte de governos e instituições de ensino. No entanto, uma medida que as organizações podem adotar para mitigar esse problema é *terceirizar partes de suas operações* — especialmente aquelas em que há alternativas de *alto valor e custo acessível*.

O **ESET PROTECT MDR** oferece exatamente essa opção. Ele elimina a necessidade de investimentos altos em tecnologia de operações de segurança (SecOps), bem como em contratação e treinamento contínuo de pessoal.

Ainda melhor: garante que *analistas especializados da ESET*, atualizados com as pesquisas mais recentes e com inteligência de ameaças, estejam *monitorando continuamente os ambientes dos clientes, 24 horas por dia, 7 dias por semana, o ano todo* — realizando hunting e detecção proativa de ameaças, enquanto a equipe interna de TI pode focar em outras prioridades importantes.

Além disso, o MDR da ESET pode reduzir drasticamente o tempo médio de detecção de ameaças: de *277 dias (ou 16 horas em um SOC profissional)* para menos de *30 minutos* — diminuindo significativamente as chances de uma violação de dados e suas consequências a longo prazo.

DEFESA PROATIVA Os agentes de ameaça podem até parecer estar com todas as cartas na mão. Mas, ao utilizar *inteligência artificial* na nuvem, nos endpoints e em toda a rede, as organizações conseguem analisar grandes volumes de dados — identificando proativamente comportamentos suspeitos e contendo ameaças antes que causem qualquer impacto.

É exatamente isso que o **ESET PROTECT** oferece ao combinar a telemetria do cliente com a ESET Threat Intelligence, desenvolvida por especialistas mundialmente reconhecidos da empresa. O resultado: insights globais exclusivos aplicados a todos os endpoints da rede.

AUTOMAÇÃO E INTELIGÊNCIA ARTIFICIAL (IA) Na verdade, a inteligência artificial (IA) e o aprendizado de máquina (ML) podem ter um papel fundamental na r*edução da complexidade da cibersegurança* para as empresas.

Diante da sobrecarga de dados e alertas que afeta muitos analistas de operações de segurança (SecOps), *assistentes baseados em IA Generativa (GenAI)* podem oferecer *insights*

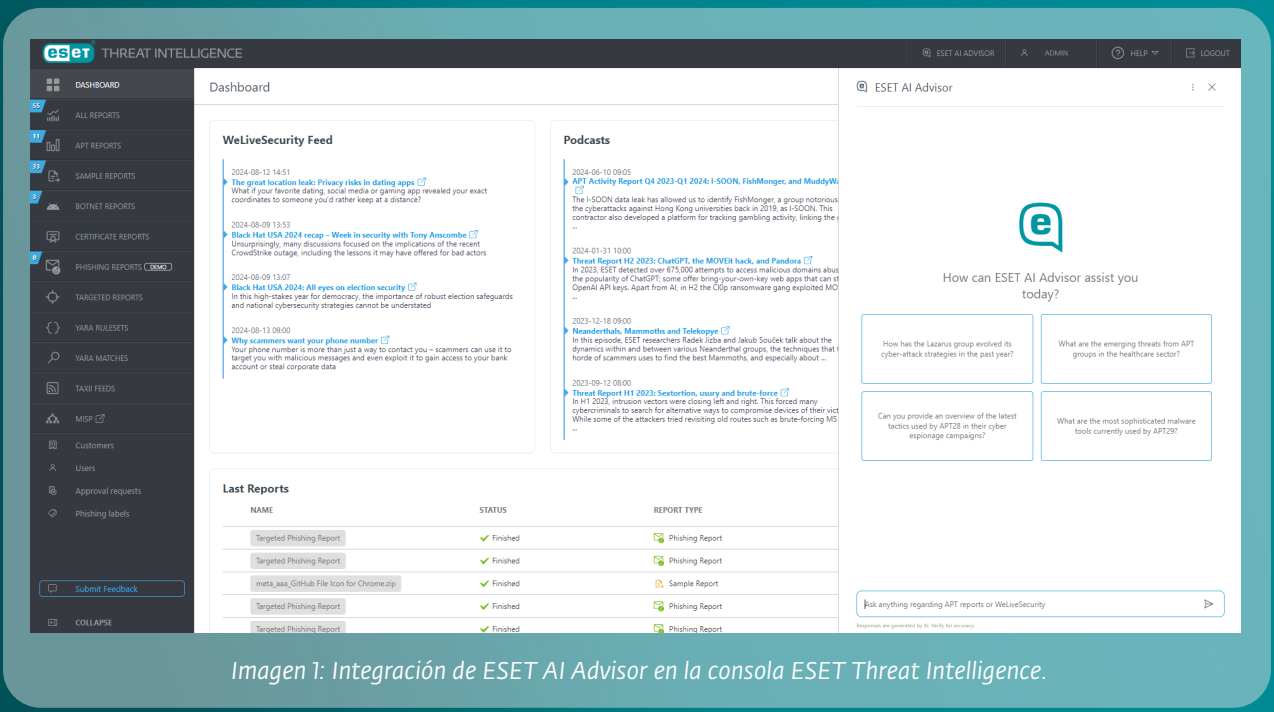

Imagen 1: Integración de ESET AI Advisor en la consola ESET Threat Intelligence.

intuitivos a partir de grandes volumes de dados, permitindo uma *melhor priorização dos alertas* e tomadas de decisão mais embasadas.

É exatamente isso que o **ESET AI Advisor** faz — integrando-se de forma fluida ao fluxo de trabalho diário para ajudar as equipes de SecOps a *otimizar o uso do XDR e da inteligência de ameaças*. Ao fazer isso, também *ajuda a preencher lacunas de habilidades*, interagindo com os analistas em *linguagem natural*.

A *automação inteligente*, frequentemente impulsionada por IA, também *reduz a carga de trabalho* das equipes de segurança ao assumir tarefas manuais e repetitivas, como aplicação de patches e resposta a incidentes.

A plataforma **ESET PROTECT** vem repleta de *fluxos de trabalho automatizados* para minimizar erros humanos, *melhorar os resultados em segurança* e permitir que os *recursos limitados da equipe se concentrem nas atividades mais importantes* — tudo isso enquanto reduz a complexidade cibernética. Em muitos casos, os administradores de TI nem precisam acessar a plataforma diretamente.

Conclusão: A Simplicidade Gera Resultados

A maioria das empresas mais ambiciosas está totalmente focada em *crescimento sustentável*, mas isso só pode ser alcançado se houver uma base sólida e segura. A sofisticação das ameaças modernas e a complexidade dos sistemas de TI e das infraestruturas de segurança das próprias empresas tornam esse objetivo ainda mais desafiador. A *escassez de profissionais qualificados* e as *lacunas na segurança* agravam ainda mais o problema.

Isso representa uma *ameaça significativa aos negócios*. Um relatório da PwC afirma que a *complexidade cibernética* pode gerar *perdas financeiras relacionadas a vazamentos de dados, dificuldades para inovar* e *redução da resiliência operacional*.

Por isso, *simplificar deve ser uma prioridade para os líderes de TI*. Felizmente, há muitas oportunidades acessíveis para isso. Ao *consolidar prevenção, detecção e caça proativa de ameaças* em uma *plataforma única, intuitiva e altamente automatizada*, como a **ESET PROTECT**, as equipes de TI podem *eliminar a complexidade e otimizar seus recursos internos*.

Além disso, é possível *contar com serviços gerenciados*, como o **ESET MDR**, para reduzir ainda mais a complexidade das operações de segurança. Ao adotar essa abordagem proativa, as empresas serão capazes de *bloquear a maioria das ameaças de imediato e identificar e conter rapidamente o restante*.

O **ESET PROTECT** é a *solução completa* para essa abordagem focada na prevenção. Ela *reduz a complexidade da gestão* e ainda oferece um suporte robusto — fornecendo *tudo o que sua empresa precisa hoje*, além de uma plataforma segura para terceirizar **XDR** e implementar iniciativas de **Zero Trust** no futuro. Em resumo, trata-se de um *roteiro enxuto para um futuro mais simples e seguro*.

Explore os benefícios dos serviços MDR da ESET, que combinam inteligência artificial com expertise humana para alcançar uma detecção de ameaças incomparável e resposta rápida a incidentes — eliminando a necessidade de manter especialistas em segurança internamente.

Esta é a ESET

Defesa proativa. Nosso negócio é minimizar a superfície de ataque.

Mantenha-se um passo à frente das ameaças cibernéticas conhecidas e emergentes com nossa abordagem focada em prevenção, impulsionada por *IA e expertise humana*.

Experimente *proteção de classe mundial*, graças à nossa i*nteligência cibernética global* interna, compilada e analisada por mais de *30 anos*, o que alimenta nossa extensa rede de P&D, liderada por pesquisadores renomados da indústria.

A **ESET** protege o seu negócio para que ele possa desbloquear todo o potencial da tecnologia.

Multicamadas, com foco na prevenção

A IA de ponta encontra a expertise humana.

Inteligência de ameaças reconhecida mundialmente.

Suporte hiperlocal e personalizado.

eset®
Digital Security
Progress. Protected.